UiO : Det juridiske fakultet

Grensene for en stats selvforsvarsrett etter FN-pakten artikkel 51 ved digitale angrep fra en annen stat

Kandidatnummer: 539

Leveringsfrist: 25.11.2018

Antall ord: 17760

Innholdsfortegnelse

1 INNLEDNING ... 1

1.1 Tema og problemstilling ... 1

1.2 Avgrensninger og presiseringer ... 2

1.3 Rettskildebildet ... 3

1.3.1 FN-pakten artikkel 2(4) og 51 anvendt på digitale operasjoner ... 3

1.3.2 Konvensjoner om digitale operasjoner ... 5

1.3.3 Tallinn Manual 2.0 ... 6

1.4 Fremstillingen videre ... 7

2 NÅR INNTRER SELVFORSVARSRETTEN ETTER ARTIKKEL 51 VED DIGITALE OPERASJONER? ... 9

2.1 Innledning ... 9

2.2 Grenseoverskridende digitale operasjoner ... 10

2.2.1 Når kan en stat pålegges ansvar for en digital operasjon? ... 10

2.2.2 Beviskrav og bevisbyrde ved tilskrivelse av statsansvar for digitale operasjoner ... 15

2.2.3 Kan digitale operasjoner utført av ikke-statlige aktører utløse retten til selvforsvar uavhengig av statsansvar jf. FN-pakten art. 51? ... 17

2.3 Når utgjør en digital operasjon et «væpnet angrep»? ... 19

2.3.1 Forholdet mellom maktforbudet etter FN-pakten artikkel 2(4) og selvforsvarsretten etter artikkel 51 ved digitale operasjoner ... 19

2.3.2 «Scale and effect»-kriteriet ... 20

2.3.3 Betydningen av målet for operasjonen ... 23

2.3.4 Betydningen av angripers intensjon ... 24

2.4 Samlede betraktninger ... 25

3 GRENSENE FOR SELVFORSVARSRETTEN ... 27

3.1 Innledning ... 27

3.2 Aktive digitale selvforsvarsresponser ... 27

3.3 «... inntil Sikkerhetsrådet har truffet de tiltak som er nødvendige ...» ... 29

3.4 Et pågående eller umiddelbart forestående væpnet angrep ... 30

3.4.1 Preventivt selvforsvar ... 31

3.4.2 «The last window of opportunity» ... 32
3.5 Umiddelbarhet ... 34
3.6 Nødvendighet ... 35
3.7 Proporsjonalitet ... 36
3.8 Hvem skal avgjøre om kriteriene for utøvelse av selvforsvar er oppfylt, og hva selvforsvaret nærmere skal bestå i? ... 39
3.9 Kollektivt selvforsvar ... 42
3.10 Samlede betraktninger ... 44

4 DIGITALE OPERASJONER ANALYSERT I LYS AV SELVFORSVARSRETTEN ... 46

4.1 Estland: De digitale operasjonene mot Estland 2007 ... 46
4.2 Iran: Stuxnet-operasjonen, 2010 ... 47
4.3 USA: Russisk innblanding i det amerikanske presidentvalget 2016 ... 49

5 AVSLUTTENDE BEMERKNINGER ... 53

6 KILDELISTE ... 55

1 Innledning

1.1 Tema og problemstilling

I denne masteroppgaven skal jeg behandle spørsmålet om hvor grensene for en stats selvforsvarsrett går etter FN-pakten artikkel 51 ved digitale angrep fra en annen stat. Dette er et utfordrende tema blant annet fordi de folkerettslige reglene på området er tilpasset konvensjonell, og ikke digital krigføring.[1]

Ettersom Internet er uten greografiske grenser og dets struktur i stor grad er bygd opp rundt anonymitet, vil digitale angrep medføre en rekke andre tekniske og rettslige komplikasjoner for en rammet stat enn det som er tilfellet ved tradisjonelle væpnede angrep.[2] Det er for eksempel ofte vanskeligere å beregne omfanget av samt å avgjøre hvem som står bak et digitalt angrep, sammenlignet med situasjonen ved tradisjonelle væpnede angrep.[3] Aktører som igangsetter digitale angrep drar dessuten ofte nytte av at visse stater har mindre gode relasjoner seg i mellom, og fører derfor angrep gjennom disse statenes nettverk for effektivt å kunne skjule egen identitet og lokasjon.[4]

Farten på utviklingen av det digitale området vil stadig utfordre gjeldende rett. Stater har ulike interesser og tilnærminger til digital sikkerhet samt ulik digital kapasitet. Dette påvirker statenes holdninger til folkeretten på det digitale området.[5]

Utenriksdepartementet la i september 2017 frem en internasjonal cyberstrategi for Norge. Som forordet til statsministeren påpeker, eksisterer det ingen konvensjoner i dag som spesifikt regulerer digitale operasjoner utført av stater. Det hersker på tross av dette en internasjonal konsensus om at folkeretten også får anvendelse på digitale operasjoner. Statsministeren påpeker at det likevel er behov for «en dialog om hvordan folkeretten kommer til anvendelse i cyberdomenet».[6]

Nasjonal sikkerhetsmyndighet (NSM) registrerte ifølge deres årsrapport for 2017 totalt 21 915 «uønskede hendelser» mot norske informasjonssystemer. Av disse ble 5232 prioritert for

1 Sklerov (2012) s. 45.
2 Mudrinich (2012) s. 195.
3 Sklerov (2012) s. 45.
4 Mudrinich (2012) s. 195.
5 Tsagourias (2017) s 37-38.
6 Utenriksdepartementet (2017) s. 3.

oppfølgning. Ifølge NSM er den generelle tendensen at antallet hendelser øker, og nettverksoperasjoner fra andre stater anses å utgjøre den høyeste IKT-risikoen for norsk offentlig forvaltning.[7]

Flere stater som Kina, Russland og USA anser det digitale rom som et fremtidig krigsområde. Samtlige har formulert egne digitale strategier og inkorporert cyberenheter i deres respektive militære enheter. Rapporter viser at stater har blitt utsatt for flere digitale angrep, selv om digital krigføring enda ikke har forekommet.[8] Den nederlandske forsvarsministeren uttalte imidlertid i oktober i år at hun anså Nederland for å være i cyberkrig med Russland etter et angivelig russisk forsøk på å igangsette digitale angrep mot organisasjonen OPCW i Nederland. Russland nekter imidlertid for ethvert forsøk på dataangrep.[9] Den nederlandske forsvarsministeren synes senere å ha moderert sitt utsagn.[10]

Eksempelet føyer seg imidlertid inn i rekken av digitale hendelser som vestlige stater mener kan tilbakeføres til Russland, og illustrerer den politiske spenningen som eksisterer mellom vestlige stater og Russland i dag.[11]

1.2 Avgrensninger og presiseringer

Første spørsmål oppgaven vil behandle er når selvforsvarsretten inntrer etter FN-pakten artikkel 51 ved digitale angrep (kapittel 2). Oppgavens andre spørsmål er hva selvforsvarsresponsene nærmere kan bestå i, og de folkerettslige begrensingene for utøvelsen av dem (kapittel 3).

Retten til selvforsvar etter art. 51 utgjør et unntak fra maktforbudet etter FN-pakten art. 2 (4) (punkt 1.3.1). Andre unntak fra maktforbudet som for eksempel samtykke, force majeure og nødrett, faller utenfor oppgavens tema og vil ikke bli behandlet.[12] Andre responser enn

---

7 Nasjonal sikkerhetsmyndighet (2017) s. 17.
8 Kondoch (2013) s. 460.
9 Aftenposten (2018).
10 Pieters (2018).
11 Reuters (2018).
12 Ruud (2011) s. 303.

selvforsvarsresponser som for eksempel mottiltak (på engelsk «countermeassures»), vil kun bli berørt der dette er relevant for å belyse selvforsvarsretten (punkt 2.2.1).[13]

Oppgaven vil bare behandle situasjoner der det første angrepet er et digitalt angrep. Fysiske angrep og andre ikke-digitale angrepsformer, faller utenfor problemstillingen.

Dette er en folkerettslig oppgave og det avgrenses derfor mot rene internrettslige spørsmål. For eksempel hersker det bred konsensus om at digital spionasje reguleres av det enkelte lands nasjonale straffelovgivning, og ikke av folkeretten.[14] Spørsmål tilknyttet digital spionasje vil derfor kun bli behandlet der dette er naturlig for å belyse selvforsvarsretten (punkt 3.7).

Ettersom oppgaven behandler selvforsvarsrettens inntreden og grensene for denne, er det reglene for jus ad bellum oppgaven primært vil behandle. Jus ad bellum utgjør de folkerettslige reglene for når en stat kan ty til militær makt. Dette må holdes atskilt fra jus in bello som omhandler reglene for opptreden under væpnet konflikt.[15] Reglene for jus in bello vil kun bli behandlet der disse reglene naturlig henger sammen med reglene for jus ad bellum (se særlig punkt 3.7).

1.3 Rettskildebildet

1.3.1 FN-pakten artikkel 2(4) og 51 anvendt på digitale operasjoner

FN-pakten artikkel 2(4) knesetter forbudet mot bruk av makt utført av stater. I Nicaragua-saken anerkjente ICJ maktforbudet slik det kommer til uttrykk i art. 2(4) som folkerettslig sedvanerett.[16] Maktforbudet avgrenses nedad mot ikke-intervensjonsprinsippet.[17]

---

[13] Mottiltak kan defineres som «i utgangspunktet folkerettsstridige handlinger som en stat iverksetter som svar på en forutgående folkerettskrenkelse fra en annen stat» (Ruud (2011) s. 308). Forskjellen på mottiltak og selvforsvarshandlinger er at førstnevnte er respons på handlinger som ikke utgjør «væpnede angrep», og det er derfor et absolutt forbud mot bruk av makt i strid med FN-pakten art. 2 (4) ved bruk av mottiltak. Selvforsvarsretten på sin side utgjør et unntak fra maktforbudet, slik at maktbruk er tillatt ved selvforsvarsutøvelse. (Ruud (2011) s. 308-309)

[14] Ohlin (2017) s. 1580. Se Melnitzky (2012) s. 564 som mener at digital spionasje likevel kan utgjøre «et væpneangrep» etter folkeretten.

[15] Larsen (2014a).

[16] ICJ, Nicaragua-saken (1986) avsnitt 190. Gray (2018) s. 603.

[17] Forbudet mot intervensjon i en annen stats anliggender kan utledes direkte av suverenitetsprinsippet, og er nærmere utdypet i Declaration on Friendly Relations, jf Generalforsamlingsresolusjon 2625 (1970). Forbudet går utpå at ingen stat har rett til å intervenere i en annen stats interne eller eksterne anliggender,

Selvforsvarsretten etter FN-pakten artikkel 51 utgjør hovedunntaket fra maktforbudet etter art. 2(4).[18]

Det følger av ordlyden i art. 51 at «[i]ntet 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 ...». Selvforsvarsretten utgjør folkerettslig sedvanerett, og utgjorde dette lenge før FN-pakten trådte i kraft, jf. også ordlyden «den naturlige rett» (på engelsk «the inherent right»).[19] Fastleggingen av den sedvanerettslige selvforsvarsretten kan spores tilbake til Caroline-saken fra 1837.[20]

Ettersom art. 51 suppleres av folkerettslig sedvanerett, vil også det sedvanerettslige grunnlaget for selvforsvarsretten bli behandlet.

Selvforsvarsretten etter art. 51 blir utløst ved et «væpnet angrep». ICJ fastslo i Atomvåpensaken (1996) at art. 2 (4) og art. 51 får anvendelse på «any use of force, regardless of the weapons employed».[21] Dette medfører at også digitale angrep som når opp til terskelen for et «væpnet angrep», er omfattet av art. 51.[22]

Ettersom digitale operasjoner ikke eksisterte i 1945 da FN-pakten ble satt i kraft og da sedvaneretten primært ble utviklet, kan det imidlertid hevdes at vilkårene etter både art. 51 og sedvaneretten på noen punkter må anvendes med en viss fleksibilitet sammenlignet med situasjonen ved konvensjonelle angrep (se for eksempel punkt 3.5).

Både stater og juridisk teori er svært splittet i spørsmålet om retten til selvforsvar etter art. 51 er sammenfallende med den sedvanerettslige selvforsvarsretten. Spørsmålet dreier seg nærmere bestemt om art. 51 uttømmende fastsetter innholdet av selvforsvarsretten, eller om det eksisterer en sedvanerettslig selvforsvarsrett som går lenger enn art. 51. De som støtter en

---

verken direkte eller indirekte. Dette omfatter blant annet enhver form for trusler mot eller innblanding i en stats politiske, økonomiske eller sosiale institusjoner. Oppfordring eller bruk av politiske, økonomiske eller andre virkemidler for å oppnå fordeler, eller for å tvinge en stat til underkastelse er forbudt. Stater er også forpliktet til å respektere andre staters valgfrihet med tanke på eget politisk, økonomisk og sosialt system. Intervensjonsforbudet omfatter langt mer enn bare bruk av makt. (Ruud (2011) s. 191) Kjernevilkåret for at det skal foreligge et brudd på ikke -intervensjonsprinsippet, er at det foreligger tvang, jf. ICJ, Nicaragua-saken (1986) avsnitt 205. Oppgaven vil kun behandle ikke-intervensjonsprinsippet der dette er relevant for å belyse grensene for selvforsvarsretten (se punkt 4.3).

18 Gray (2018) s. 611.

19 Ruud (2011) s. 194-195.

20 Jennings (1938).

21 ICJ, Atomvåpensaken (1996) s. 244 avsnitt 39.

22 Tallinn Manual 2.0 (2017) s. 328 avsnitt 1.

videre selvforsvarsrett mener dette kan utledes av ordlyden i art. 51, jf. «inherent right», og at denne omfatter handlinger som faller under terskelen for «væpnet angrep» etter art. 51. De argumenterer også blant annet for en rett til preventivt selvforsvar. Ettersom art. 51 setter begrensninger for selvforsvaret ved et «væpnet angrep», mener andre at en slik vid selvforsvarsrett vil gjøre art. 51 illusorisk. Ettersom selvforsvarsretten utgjør et unntak fra maktforbudet, er selvforsvarsretten etter deres syn også snever. De mener heller ikke at art. 51 viderefører en videre sedvanerettslig selvforsvarsrett som eksisterte før 1945.[23]

Jeg mener art. 51 og den sedvanerettslige selvforsvarsretten til dels er sammenfallende, slik at det er et absolutt vilkår om et «væpnet angrep» før en stat lovlig kan ty til selvforsvar både etter art. 51 og sedvaneretten. Begrunnelsen er den samme som over; dersom en stat kan iverksette selvforsvarsresponser mot enhver trussel som ikke når opp til terskelen for «væpnet angrep» etter art. 51, vil denne miste sin betydning. Dette vil også bli lagt til grunn som et vilkår for maktbruk i selvforsvar mot digitale operasjoner i denne oppgaven. Når det gjelder retten til preventivt selvforsvar hersker det bred konsensus om at det eksisterer en begrenset sedvanerettslig rett til dette selv om en slik rett ikke kan utledes direkte av ordlyden i art. 51, derav dels sammenfall (se punkt 3.4.1).

1.3.2 Konvensjoner om digitale operasjoner

Det eksisterer ingen konvensjon som spesifikt regulerer digitale operasjoner utført av stater i dag.[24] En sentral konvensjon på det digitale området er imidlertid Europarådets konvensjon om datakriminalitet (Convention on Cybercrime). Denne søker å harmonisere reglene for bekjempelse av datakriminalitet mellom traktatlandene samt å styrke det internasjonale samarbeidet på området. I tillegg ble det klart 12. november i år at mer enn 50 land og 150 teknologisselskaper samt organisasjoner har sluttet seg til en Paris-erklæring om tillit og sikkerhet i det digitale rom.[25] Dette er ingen bindende avtale, men en erklæring om tettere statlig samarbeid for bekjempelse av fiendtlige digitale operasjoner. Verken USA, Russland eller Kina har signert denne.[26] Ettersom verken denne eller Europarådets konvensjon om datakriminalitet angår digitale operasjoner utført av stater direkte, vil oppgaven kun berøre dem der det er relevant for oppgavens problemstilling (punkt 2.2.1 og 3.9).

---

23 Gray (2018) s. 611

24 Utenriksdepartementet (2017) s. 3.

25 Jørgenrud (2018).

26 Paris-erklæringen (2018).

1.3.3 Tallinn Manual 2.0

Tallinn-manualen er en ikke-bindende manual, utarbeidet av en rekke eksperter (kalt «International Group of Experts» eller «IGE») på det digitale området etter invitasjon fra NATO Cooperative Cyber Defence Centre of Excellence. Den representerer ingen ny konvensjon på det internasjonale digitalrettslige området, og den etablerer heller ingen ny folkerett. Manualen reflekterer heller ikke staters offisielle syn på egne digitale operasjoner. Den er ment å være en objektiv gjenspeilelse av folkeretten på det digitale området de lege lata, og den identifiserer samt kommenterer relevante folkerettslige regler som regulerer digitale operasjoner.[27] Reglene for jus ad bellum, herunder reglene om selvforsvar etter FN-pakten artikkel 51, er deler av folkeretten som manualen behandler.[28] Blant annet identifiserer og kommenterer den regler for statsansvar basert på FNs folkerettskommisjons arbeid med Articles on State Responsibility (heretter ASR), men anvendt på digitale operasjoner (se punkt 2.2.1).[29]

Etter statuttene for Den internasjonale domstol (ICJ) art. 38, vil Tallinn-manualen i utgangspunktet bare utgjøre juridisk teori, og dermed være en subsidiær rettskilde, jf. art. 38(1)(d). Roberts og Sivakumaran skriver imidlertid at selv om juridisk teori generelt sett synes å tillegges redusert vekt i folkerettsanvendelsen, utgjør Tallinn-manualen i sin første utgave et godt eksempel på at juridisk teori fortsatt tillegges stor vekt på visse områder av folkeretten. De nevner at på områder innen folkeretten hvor stater har vært tilbakeholdne med å formulere juridiske normer, eller hvor det eksisterer en fastlåst situasjon mellom ulike oppfatninger og hvor ingen domstoler har jurisdiksjon, vil slike akademiske verk kunne ha avgjørende rettskildemessig betydning. Juridisk litteratur som omhandler uavklarte rettsområder kan også gi opphav til nye rettslige ideer som siden anses å utgjøre gjeldende rett.[30]

Ettersom det ikke eksisterer en konvensjon som regulerer digitale operasjoner utført av stater, taler dette for at Tallinn-manualen veier tungt som et gjennomtenkt og omfattende juridisk

---

[27] Tallinn Manual 2.0 (2017) s. 1, 2.
[28] Tallinn Manual 2.0 (2017) s. 339-356.
[29] Tallinn Manual 2.0 (2017) s. 79-167.
[30] Roberts (2018) s. 107.

verk på området.[31] Dette underbygges av at mer enn femti land, inkludert de faste medlemmene av Sikkerhetsrådet kom med innspill i prosessen.[32]

Oppgaven vil derfor ofte ta utgangspunkt i Tallinn-manualen ved analyser.

Tallinn-manualen kan imidlertid virke noe overfladisk på visse punkter. Reglene slik de er identifisert samt kommentarene tilknyttet disse, er generelle og noen ganger også uklare.[33] Manualen fremhever de punktene der ekspertene var uenige, men Tsagourias påpeker at man kanskje hadde forventet at manualen skulle løse en del av tolkningsuenighetene istedenfor kun å fremheve dem.[34]

Manualen vil imidlertid kun være et utgangspunkt for de spørsmål oppgaven reiser. Andre rettskilder, herunder internasjonale konvensjoner, generalforsamlingsresolusjoner samt rettspraksis fra ICJ, vil bli anvendt både som supplement til manualen, men også på selvstendig grunnlag.

1.4 Fremstillingen videre

Kapittel 2 behandler spørsmålet om når selvforsvarsretten etter FN-pakten artikkel 51 inntrer ved digitale operasjoner.

Under deloverskriften «Grenseoverskridende digitale operasjoner» i punkt 2.2 vil spørsmålet om når en stat kan holdes ansvarlig for en digital operasjon samt beviskravet og bevisbyrden i den forbindelse bli behandlet (punkt. 2.2.1 og 2.2.2). Det samme vil spørsmålet om digitale operasjoner utført av ikke-statlige aktører uten statlig innblanding kan utgjøre et «væpnet angrep» jf. art. 51 (punkt. 2.2.3). Begrunnelsen for overskriften til punkt 2.2 er å få synliggjort det grunnleggende vilkåret om at det må foreligge et grenseoverskridende element for at art. 51 kommer til anvendelse.

Under deloverskriften «Når utgjør en digital operasjon et «væpnet angrep»» (punkt 2.3), vil forholdet mellom maktforbudet og selvforsvarsretten bli behandlet (punkt 2.3.1.). Deretter vil

---

31 Tallinn Manual 2.0 (2017) s. 1, 3. Schmitt (2017) s. 240. Jensen (2017) s. 737 -740. Banks (2017) s. 1513.

32 Jensen (2017) s. 740.

33 Banks (2017) s. 1494.

34 Tsagourias (2017) s 37.

kravet til operasjonens alvorlighetsgrad etter «scale and effect»-kriteriet, betydningen av målet samt betydningen av angripers intensjon bli behandlet (punkt 2.3.2 - 2.3.4).

Kapittel 3 analyserer grensene for selvforsvarsretten etter art. 51 og sedvaneretten når det først er fastslått at et digitalt angrep utløser en stats selvforsvarsrett.

Innledningsvis vil det bli redegjort for hva selve selvforsvarshandlingen kan bestå i, herunder aktive digitale selvforsvarsresponser (punkt 3.1 - 3.2). Deretter vil de nærmere grensene for selvforsvarsretten bli analysert (punkt. 3.3 - 3.7). Særlig spørsmålet om og når aktive digitale motangrep er i samsvar med begrensningene for selvforsvarutøvelse, vil gjennomgående bli behandlet. Hvem som skal avgjøre om kriteriene for selvforsvarsutøvelse er oppfylt og om aktive digitale motangrep skal iverksettes, vil bli diskutert nærmere i punkt 3.8. Kollektivt selvforsvar mot digitale angrep vil bli behandlet i punkt 3.9.

Kapittel 4 drøfter tre ulike hendelser hvor tre ulike stater ble rammet av fiendtlige digitale operasjoner i lys av selvforsvarsretten. Formålet med kapittelet er å anvende reglene for selvforsvarsretten etter art. 51 og sedvaneretten på virkelige digitale operasjoner, og derved belyse hvordan slike vurderinger kan forekomme i praksis. Drøftelsen foretas på tross av at ingen digital hendelse inkludert de oppgaven behandler, så langt har blitt offentlig karakterisert som et «væpnet angrep» av stater.[35] Digital sikkerhet er et område hvor det er grunn til å anta at mye informasjon er sikkerhetsgradert, herunder informasjon om faktisk forekommende digitale angrep samt staters selvforsvarsutøvelse i den forbindelse. Begrunnelsen for at akkurat disse tre tilfellene ble valgt er fordi sakene er interessante fra et folkerettslig ståsted, og fordi mye av faktum i disse sakene er offentlig tilgjengelig, noe som letter en rettslig analyse.

Både kapittel 2 og 3 avsluttes med samlede betraktninger for hvert sitt respektive kapittel, mens hele oppgaven avsluttes med noen konkluderende bemerkninger i kapittel 5.

[35] Hayward (2017) s. 410-411. Det kan imidlertid som nevnt muligens gjøres unntak for Nederland her.

2 Når inntrer selvforsvarsretten etter artikkel 51 ved digitale operasjoner?

2.1 Innledning

Selvforsvarsretten blir utløst ved et «væpnet angrep», jf. FN-pakten artikkel 51. Forutsetningen for at artikkel 51 kommer til anvendelse er imidlertid at det foreligger et grenseoverskridende element; rene interne stridigheter reguleres ikke av maktforbudet i FN-pakten artikkel 2 (4), og heller ikke av unntaket etter artikkel 51. Kjernen i selvforsvarsretten er som Ruud påpeker at en stat utøver selvforsvar mot angrep fra en annen stat.[36]

Kravet om et grenseoverskridende element er også fremholdt i Tallinn-manualen som påpeker at dette gjelder tilsvarende for digitale angrep.[37] Spørsmålet om når en stat kan holdes ansvarlig for et digitalt angrep mot en annen stat (punkt 2.2.1 og 2.2.2), samt spørsmålet om ikke-statlige aktører som opererer fra andre land kan utløse selvforsvarsretten selv uten statlig innblanding (punkt 2.2.3), hører naturlig inn under kravet om at det foreligger et grenseoverskridende element (punkt 2.2).

Artikkel 51 er taus om hvor omfattende og intenst et angrep må være før det er tale om et «væpnet angrep» (punkt 2.3). Isteden er definisjonen av «væpnet angrep» nærmere fastlagt i den internasjonale sedvaneretten. Det følger av sedvaneretten at terskelen for ulovlig maktbruk etter art. 2 (4) må være overskredet (punkt 2.3.1). Dette er imidlertid ikke tilstrekkelig da den nedre grense for et «væpnet angrep» ligger høyere enn grensen for maktforbudet.[38] Et kriterium som ble anvendt av ICJ i Nicaragua-saken var «the scale and effect» - kriteriet.[39]

Tallinn- manualen benytter i likhet med ICJ «the scale and effect»-kriteriet for å avgjøre om en digital operasjon utgjør et «væpnet angrep».[40] Dette kriteriet vil bli behandlet i punkt 2.3.2. Betydningen av den digitale operasjonens mål og angripers intensjon for spørsmålet om det foreligger et «væpnet angrep», vil bli behandlet avslutningsvis i punkt 2.3.3 og 2.3.4.

---

36 Gray (2018) s. 603. Ruud (2011) s. 195.

37 Tallinn Manual 2.0 (2017) s. 340 avsnitt 3.

38 ICJ Nicaragua-saken (1986), avsnitt 191. Ruud (2011) s. 195. Gray (2018) s. 612.

39 ICJ Nicaragua-saken (1986), avsnitt 195.

40 Tallinn Manual 2.0 (2017) s. 341 avsnitt 6 og 7.

2.2 Grenseoverskridende digitale operasjoner

For at en digital operasjon skal omfattes av FN-pakten artikkel 51, må det som nevnt foreligge et grenseoverskridende element.[41] For å avgjøre om det foreligger et grenseoverskridende element, må den rammede staten vite hvem som kan holdes ansvarlig for operasjonen.

Tilskrivelse av ansvar for det væpnede angrepet er et grunnleggende vilkår for selvforsvarsrettens inntreden selv om det hersker uenighet om dette innebærer tilskrivelse av statsansvar, eller om ikke-statlige aktørers angrep kan utløse selvforsvarsretten uten statlig innblanding.[42] Enkelte teoretikere mener imidlertid at folkeretten tillater aktive digitale selvforsvarsresponser uten kjennskap til angripers identitet dersom det digitale angrepet rammer statens kritiske infrastruktur.[43] Foruten å være iboende ulogisk (for hvor skal selvforsvarshandlingen rettes når man ikke vet hvem som står bak?), medfører dette også fare for feiltilskrivelse av ansvar, skade på uskyldige systemer og konflikteskalering i strid med både jus ad bellum og jus in bello (punkt 3.7).[44]

Nesten alle digitale operasjoner utført i dag kan spores tilbake til ikke-statlige aktører som opererer fra andre land. Spørsmålet blir dermed for det første om og når en stat kan holdes ansvarlig for ikke-statlige aktørers handlinger (punkt 2.2.1 og 2.2.2).[45] For det andre oppstår det et spørsmål om ikke-statlige aktører kan utløse en stats selvforsvarsrett uavhengig av statsansvar (punkt 2.2.3).[46]

2.2.1 Når kan en stat pålegges ansvar for en digital operasjon?

Tallinn-manualen baserer sin analyse av statsansvar på FNs folkerettskommisjons arbeid med Articles on State Responsibility fra 2001 (heretter ASR) slik de ble tatt til etterretning av FNs generalforsamling i resolusjon av 56/83 av 28. januar 2002.[47] Som manualen påpeker er ikke

---

41 Gray (2018) s. 603. Ruud (2011) s. 195.

42 Gray (2018) s. 615. Roscini (2010) s. 119. Graham (2010) s. 92. Banks (2017) s. 1497. Mudrinich (2012) s. 193, 197.

43 Se feks. Jensen (2002) s. 234.

44 Roscini (2010) s. 119.

45 Graham (2010) s. 93.

46 Tallinn Manual 2.0 (2017) s. 345, avsnitt 18.

47 Tallinn Manual 2.0 (2017) s. 79 fotnote 112. Generalforsamlingsresolusjon 56/83 (2002).

utkastet folkerettslig bindende, men flere av reglene anses å utgjøre folkerettslig sedvanerett.[48] Dette ble fastslått blant annet av ICJ i Folkemord-saken (2007).[49]

Tallinn-manualen fastslår at statsansvar basert på folkerettslig sedvanerett også omfatter digitale handlinger.[50] Vilkårene for å pålegge statsansvar for digitale operasjoner fastslås i manualens regel 14 til 18.[51] Ettersom nesten alle digitale operasjoner utført i dag kan spores tilbake til ikke-statlige aktører, er det regel 14 og 17 som er mest aktuelle, og kun disse som vil omtales her.[52]

Regel 14 uttrykker at en stat kan holdes folkerettslig ansvarlig for en cyberrelatert handling som innebærer et brudd på en folkerettslig forpliktelse, og som kan tilskrives denne staten, jf. ASR art. 1 som utgjør folkerettslig sedvanerett.[53]

Utgangspunktet er at digitale kriminelle operasjoner utført av ikke-statlige aktører ikke kan tilskrives staten disse opererer fra.[54] Det følger imidlertid av Tallinn-manualen regel 17 jf. ASR art. 8, at en digital operasjon utført av en ikke-statlig aktør kan tilskrives en stat når den ikke-statlige aktøren er engasjert i henhold til statens instruksjoner, under dets overoppsyn («direction») eller kontroll, eller når staten anerkjenner og vedtar operasjonene som dets egne.[55]

Begrepene «direction» og «control» refererer til «effective control» jf. Nicaragua-saken (1986) og Folkemordsaken (2007).[56] ICJ avviste i Folkemordsaken «the overall control test» som ble lagt til grunn av ICTY i Tadić-saken (1999).[57] Årsaken var blant annet at denne testen ble ansett å innebære en for vid adgang til å pålegge statsansvar. Domstolen uttalte at en stat kun er ansvarlig for egne handlinger, herunder handlinger begått av andre aktører på statens vegne.[58]

---

48 Tallinn Manual 2.0 (2017) s. 79 fotnote 112. Roberts (2018) s. 105. Ruud (2011) s. 302.

49 ICJ, Folkemordsaken (2007) avsnitt 385, 398, 401, 420.

50 Tallinn Manual 2.0 (2017) s. 80 avsnitt 4.

51 Tallinn Manual 2.0 (2017) s. 87-104.

52 Graham (2010) s. 93.

53 Tallinn Manual 2.0 (2017) s. 84, avsnitt 1 fotnote 124.

54 Tallinn Manual 2.0 (2017) s. 95 avsnitt 1.

55 Tallinn Manual 2.0 (2017) s. 94.

56 ICJ Nicaragua-saken (1986) avsnitt 115. ICJ Folkemordsaken (2007) avsnitt 400. Tallinn Manual 2.0 (2017) s. 96 avsnitt 5.

57 ICTY, Tadić-saken (1999) avsnitt 145

58 ICJ, Folkemordsaken (2007) avsnitt 406. Tallinn Manual 2.0 (2017) s. 96 avsnitt 6.

Ifølge Tallinn-manualen har en stat «effective control» over en digital operasjon utført av en ikke-statlig aktør, når den digitale operasjonen er en integrert del av en operasjon som staten bestemmer utførelsen og retningen av.[59] En stat utøver ikke «effective control» dersom den kun supplerer eller gir generell støtte til ikke-statlige digitale operasjoner, eller bare tar ansvar for en spesifikk del av disse.[60]

Det hersker imidlertid uenighet om innholdet i «effective control» - standarden.[61]

Flere teoretikere mener at sedvaneretten i etterkant av terrorangrepene 11. september 2001 har forandret innholdet i denne standarden til en standard for indirekte ansvar.[62] Bakgrunnen er at Afghanistan ble holdt indirekte ansvarlig for terrorangrepene utført av Al-Qaeda på tross av at Afghanistans Taliban-regime verken utøvde «effective» eller «overall control» over Al-Qaedas handlinger.[63]

Stater har etter disse teoretikernes syn uavhengig av konkret statlig innblanding, en generell folkerettslig forpliktelse til å forhindre at eget territorium blir brukt av ikke-statlige aktører for å igangsette væpnede angrep mot andre stater.[64] Indirekte ansvar kan etter dette pålegges ved såkalt tilskrevet ansvar («imputed responsibility») ved brudd på denne forpliktelsen, fremfor at angrepet direkte og endelig må kunne tilbakeføres til staten («conclusive attribution»).[65]

Dette utleder de av det generelle aktsomhetskravet som innebærer en statlig forpliktelse til å forhindre handlinger som krenker andre staters rettigheter igangsatt fra eget territorium, og som har kommet til uttrykk i flere generalforsamlingsresolusjoner, folkerettslige avgjørelser samt i anerkjent juridisk teori.[66]

Når det gjelder det konkrete spørsmålet om det foreligger en plikt til å forhindre digitale angrep igangsatt fra eget territorium, kan en slik plikt utledes av Europarådets konvensjon om

---

59 Tallinn Manual 2.0 (2017) s. 96 avsnitt 6. Kommentar til ASR art. 8, s. 70 avsnitt 3.

60 Tallinn Manual 2.0 (2017) s. 97 avsnitt 8.

61 Kondoch (2013) s. 472.

62 Sklerov (2012) s. 54. Graham (2010) s. 96.

63 Sklerov (2012) s. 55-56.

64 Graham (2010) s. 93, 101. Mudrinich (2012) s. 193.

65 Graham (2010) s. 93. Mudrinich (2012) s. 193. Sklerov (2012) s. 62.

66 Se Generalforsamlingsresolusjon 2625 (1970) og 49/60 (1994). ICJ, Corfu Channel-saken (1949) s. 22. ICJ, Gisselsaken (1980) s 32-33. Sklerov (2012) s. 54 fotnote 5, 6, 7, s. 62-63. Schmitt (2003) s. 540-541. Graham (2010) s. 94.

datakriminalitet.[67] Tre av statene som har ratifisert den er permanente medlemmer av Sikkerhetsrådet, og fem er blant statene med flest internettbrukere i verden.[68] Selv om konvensjonen i utgangspunktet er en regional avtale, har konvensjonen derfor likevel stor betydning for utvikling av sedvaneretten på området.[69]

I tillegg anerkjenner FNs Generalforsamling digitale angrep som en fare mot internasjonal fred og sikkerhet, og har bedt stater om å forhindre at eget territorium blir brukt for igangsettelse av digitale angrep.[70] Flere stater har erklært digitale angrep som en trussel mot den internasjonale fred og sikkerhet, og mange har kriminalisert digitale angrep etter egen intern straffelovgivning.[71] Stater synes på bakgrunn av dette å anerkjenne en slik spesifikk forpliktelse.[72]

Den nevnte Paris-erklæringen er også et eksempel på et initiativ hvor villigheten til å samarbeide internasjonalt for å forhindre digitale angrep utført av ikke-statlige aktører, er i fokus selv om denne ikke pålegger partene konkrete forpliktelser.[73]

Tallinn-manualen mener også at stater er pålagt et aktsomhetskrav ved digitale angrep igangsatt fra eget territorium, men behandler dette etter andre regler enn reglene for statsansvar, jf. manualens regel 6 og 7. Aktsomhetskravet etter manualen innebærer konkret at stater er forpliktet til å iverksette de tiltak som er gjennomførbare etter forholdene for å stanse digitale operasjoner som påvirker rettighetene til, og medfører alvorlige konsekvenser for, andre stater.[74] Ekspertene mener imidlertid at dette aktsomhetskravet ikke innebærer et krav om å ty til preventive, materielle tiltak, og at statene selv kan velge hvordan de vil stanse digitale angrep fra eget territorium.[75] Kunnskap om slike operasjoner er et vilkår for aktsomhetskravets anvendelse etter manualen.[76]

---

67 Se særlig Europarådets konvensjon om datakriminalitet art. 2-11, 22, 23-25. Sklerov (2012) s. 63 fotnote 19, fotnote 21.

68 Sklerov (2012) s. 63 fotnote 20. Graham (2010) s. 94.

69 Sklerov (2012) s. 63 fotnote 20.

70 Generalforsamlingsresolusjon 53/70 (1999), 54/49 (1999), 55/63 (2001), Sklerov (2012) s. 66.

71 Graham (2010) s. 94. Sklerov (2012) s. 64, 66.

72 Graham (2010) s. 94. Sklerov (2012) s. 66.

73 Jørgenrud (2018).

74 Tallinn Manual 2.0 (2017) s. 30, 31 avsnitt 4, 43.

75 Tallinn Manual 2.0 (2017) s. 32 avsnitt 5, s. 44 avsnitt 6, 7.

76 Tallinn Manual 2.0 (2017) s. 45 avsnitt 9.

Manualen påpeker at selv om en stat ikke kan holdes ansvarlig for hele operasjonen etter regel 17, hindrer ikke det at en stats medvirkning i seg selv kan utgjøre et brudd på folkeretten som for eksempel intervensjons- og maktforbudet.[77] Et brudd på aktsomhetskravet vil i følge manualen gi grunnlag for iverksettelse av mottiltak.[78]

Graham og Sklerov argumenterer for et strengere aktsomhetskrav enn Tallinn-manualen. Etter deres syn består aktsomhetskravet av en plikt til å vedta streng nasjonal straffelovgivning som rammer fiendtlige digitale grenseoverskridende operasjoner, gjennomføre grundig etterforskning ved digitale angrep, straffeforfølge de involverte samt samarbeide med den rammede staten og yte bistand til dennes etterforskning.[79]

Dersom staten konsekvent unnlater å ta grep for å forhindre at digitale angrep blir igangsatt fra eget territorium, kan denne staten etter deres syn anses som en tilfluktsstat. I slike tilfeller kan statsansvar pålegges uten å måtte påvise en direkte forbindelse mellom den som utøver angrepet og tilfluktsstaten, og selvforsvarsretten inntrer så fremt de øvrige vilkårene er oppfylt.[80] En svikt hos staten i å forhindre slike angrep er nok.[81]

Basert på dette synes det å herske bred konsensus om at stater er pålagt et generelt aktsomhetskrav som går ut på å forhindre digitale angrep igangsatt fra eget territorium mot andre stater, men at det er uenighet om det nærmere innholdet i denne forpliktelsen. Dersom denne forpliktelsen blir brutt, er det også uenighet om konsekvensene av dette. Sklerov og Graham er blant dem som argumenterer for at brudd utløser en stats selvforsvarsrett, mens Tallinn-manualen derimot kun taler om mottiltak.

Selv om reglene for statsansvar er på det rene og det er påvist at det foreligger et brudd på maktforbudet jf. art. 2(4) i form av en digital operasjon som når opp til terskelen for et «væpnet angrep» jf. art. 51 (punkt 2.3), må den angrepne staten uansett i det konkrete tilfellet kunne bevise hvilken stat som står bak angrepet før denne lovlig kan ty til selvforsvarsresponser. Spørsmålet om beviskrav og bevisbyrde ved tilskrivelse av ansvar for digitale operasjoner, behandles under.

---

77 Tallinn Manual 2.0 (2017) s. 100 avsnitt 19.

78 Tallinn Manual 2.0 (2017) s. 50 avsnitt 28.

79 Graham (2010) s. 93, 94. Sklerov (2012) s. 67.

80 Graham (2010) s. 93. Mudrinich (2012) s. 193.

81 Sklerov (2012) s. 56. Forhold som prekluderer ansvar for digitale operasjoner er etter regel 19 i Tallinn-manualen samtykke, selvforsvar, lovlige mottiltak («countermeassures»), nødrett, force majeure eller nødverge. (Tallinn Manual 2.0 (2017) s. 104) Disse ansvarsfrihetsgrunnene vil ikke forfølges videre her.

2.2.2 Beviskrav og bevisbyrde ved tilskrivelse av statsansvar for digitale operasjoner

Digitale angrep medfører betydelige vanskeligheter når det gjelder etablering av bevis for statsansvar.[82]

Tradisjonelt har det vært vanlig å anse bruken av statlige ressurser som en ubestridelig indikasjon på statlig innblanding. Dersom en digital operasjon stammer fra statlig digital infrastruktur, kan imidlertid en ikke-statlig aktør ha tilegnet seg kontroll over denne. Ikke-statlige aktører kan også forfalske egen identitet ved såkalt «spoofing», og digitale angrep ledes ofte gjennom uskyldige tredjelands nettverk, slik at det synes som om en uskyldig stat står bak operasjonen.[83] I noen tilfeller kan det være tvil om staten i det hele tatt er angrepet eller om skaden skyldes teknisk svikt.[84]

Det finnes ingen folkerettslig regel med tanke på beviskravet for etablering av statsansvar for digitale operasjoner.[85]

Tallinn-manualen anser beviskravet for å være avhengig av en konkret rimelighetsvurdering der faktorer som alvorligheten av folkerettsbruddet, omstendighetene rundt, den tilgjengelige informasjonens mengde, presisjon samt pålitelighet, inngår. Tidlige beslutninger basert på lite informasjon er generelt mindre troverdige enn senere beslutninger basert på mer informasjon. Jo mer skadelig eventuelle selvforsvarsresponser vil være, desto høyere krav stilles til informasjonens pålitelighet. Samtidig forventes en stat som er rammet av småskala digitale operasjoner å tilveiebringe mer bevis for statsansvar, enn en stat som opplever totalødeleggende digitale operasjoner som krever en umiddelbar respons. Manualen anerkjenner slik den bevismessige usikkerheten tilknyttet etablering av statsansvar for digitale operasjoner.[86]

Kondoch påstår at det kreves høy grad av sikkerhet før en stat kan ty til selvforsvarshandlinger. Dette utleder han av ICJs bevisvurdering i Oljeplattform-saken

---

82 Kondoch (2013) s. 473.

83 Banks (2017) s. 1492. Graham (2010) s. 92. Carlin (2016) s. 409. Dinniss (2012) s. 105. Tallinn Manual 2.0 (2017) s. 91 avsnitt 13, 15.

84 Kondoch (2013) s. 473.

85 Banks (2017) s. 1503, s. 1504. Kondoch (2013) s. 473.

86 Tallinn Manual 2.0 (2017) s. 81-82 avsnitt 10, 11. Banks (2017) s. 1499, 1503-1504, 1505-1506.

(2003).[87] I tillegg mener han at bevisbyrden for at det foreligger et «væpnet angrep» ligger på den angrepne staten, jf. uttalelser i Oljeplattform-saken (2003) og Nicaragua-saken (1986).[88]

Banks påstår på sin side at beviskravet for statsansvar er satt lavt ettersom det ikke finnes en sedvanerettslig eller traktatbasert regel om dette. Etter hans mening utgjør det ikke et folkerettsbrudd dersom en stat mislykkes i å tilveiebringe overbevisende bevis for statsansvar, og det eksisterer etter hans syn heller ingen bevisbyrderegel.[89]

Som Sklerov påpeker kan ikke stater holdes ansvarlige for ethvert grenseoverskridende angrep igangsatt innenfor dets grenser. Den rammede staten må derfor ved vurdering av statsansvar for ikke-statlige aktørers angrep, i det minste undersøke den andre statens straffelovgivning som omhandler digitale angrep, dets håndhevelse av loven og tidligere samarbeidsvilje med andre stater som har blitt rammet av digitale angrep fra dets territorium.[90]

Sklerov anser imidlertid en stat for å ha oppfylt sin bevisbyrde dersom den i god tro og etter beste tekniske evne tilskriver statsansvar for et digitalt angrep på bakgrunn av den tilgjengelige informasjonen som den besitter.[91]

Jeg er enig i Kondochs rettslige vurderinger på dette punktet, og leser de nevnte avgjørelsene på samme måte som ham. Hensynet til å motvirke feiltilskrivelse av ansvar, skade på uskyldige systemer i strid med folkeretten samt generell konflikteskalering, tilsier også at beviskravet for statsansvar settes høyt og at bevisbyrden påligger den rammede staten. Banks innrømmer at en stat som tar feil angående hvem som står bak et digitalt angrep og som igangsetter mottiltak basert på dette, har begått et folkerettsbrudd.[92] Dette tilsier at beviskravet for statsansvar ved selvforsvarsresponser er strengere enn det han selv skal ha det til. Samtidig er jeg også enig med Sklerov i at en stat som i god tro og etter beste tekniske evne tilskriver ansvar for en digital operasjon, har oppfylt sin bevisbyrde. Begrunnelsen er de nevnte tekniske bevisvanskelighetene ved tilskrivelse av ansvar for digitale operasjoner. For å motvirke at stater i realiteten mister sin selvforsvarsrett ved digitale angrep, er det derfor viktig at beviskravet heller ikke settes for høyt.

---

87 ICJ, Oljeplattform-saken (2003) avsnitt 61. Kondoch (2013) s. 473.

88 Kondoch (2013) s. 473. ICJ, Oljeplattform-saken (2003) avsnitt 57, Nicaragua-saken (1986) avsnitt 155.

89 Banks (2017) s. 1504, 1505.

90 Sklerov (2012) s. 54, 68. Graham (2010) s. 94.

91 Sklerov (2012) s. 71.

92 Banks (2017) s. 1503.

2.2.3 Kan digitale operasjoner utført av ikke-statlige aktører utløse retten til selvforsvar uavhengig av statsansvar jf. FN-pakten art. 51?

Det er omstridt om en digital operasjon igangsatt av ikke-statlige aktører fra en stat mot en annen stat kan utløse retten til selvforsvar etter art. 51 forutsatt at terskelen for «væpnet angrep» er overskredet, når disse handlingene verken direkte eller indirekte kan tilskrives staten de ikke-statlige aktørene opererer fra.[93] Dette spørsmålet skiller seg fra spørsmålet behandlet i punkt 2.2.1 ved at situasjonen som behandles her er når stater ikke engang indirekte kan holdes ansvarlig for de ikke-statlige aktørenes handlinger. Spørsmålet er altså om selvforsvarsretten kan utløses helt uavhengig av statsansvar.

Opprinnelig omfattet selvforsvarsretten kun angrep fra stater. Angrepene utført av den ikke-statlige terrorgruppen Al Qaeda 11. september 2001, ble imidlertid ansett som et «væpnet angrep» etter FN-pakten art. 51 av en rekke stater, Sikkerhetsrådet vedtok flere resolusjoner som anerkjente anvendelsen av selvforsvarsretten og NATO støttet også denne tilnærmingen.[94]

Enkelte teoretikere anser dette som et uttrykk for en utvikling av sedvaneretten der angrep fra ikke-statlige aktører kan utløse selvforsvarsretten uavhengig av statsansvar. De mener dette også kan utledes av ordlyden etter art. 51 ettersom art. 2 (4) kun omfatter staters handlinger, mens art. 51 ikke har en slik begrensning.[95]

Flertallet av ekspertene bak Tallinn-manualen støtter dette, og mener selvforsvarsretten utløses ved digitale angrep utført av ikke-statlige aktører uavhengig av statsansvar.[96]

I Mursaken (2004) uttalte ICJ at art. 51 anerkjenner retten til selvforsvar ved et «væpnet angrep» utført av en stat mot en annen stat. Truslene mot Israel ble imidlertid ansett å komme innenfra. Det forelå dermed ikke et grenseoverskridende element, og ICJ fastslo at Sikkerhetsrådets resolusjoner om terrorangrepene 11. september ikke kunne påberopes av Israel. ICJ tok heller ikke stilling til om angrep fra ikke-statlige aktører i andre land kan

---

93 Tallinn Manual 2.0 (2017) s. 345 avsnitt 18. Kondoch (2013) s. 472.

94 Sikkerhetsrådsresolusjon 1368 (2001), 1373 (2001), NATO (2001), OAS (2001).

95 Ruud (2011) s. 197. Tallinn Manual 2.0 (2017) s. 345 avsnitt 18, 19. Sklerov (2012) s. 53. Kesan (2012) s. 525. Graham (2010) s. 93.

96 Tallinn Manual 2.0 (2017) s. 345 avsnitt 19.

utgjøre et «væpnet angrep» jf. art. 51. I Democratic Republic of the Congo v. Uganda (2005) fastslo domstolen derimot at selvforsvarsretten ikke fikk anvendelse ettersom angrepene ikke kunne tilskrives en stat. Den sistnevnte saken tilsier at ICJ ikke støtter en tilnærming der selvforsvarsretten får anvendelse uavhengig av statsansvar for væpnede angrep, på tross av de nevnte statserklæringene og Sikkerhetsrådsresolusjonene etter terrorangrepene 11. september.[97]

Sklerov mener at statsansvar er et vilkår for igangsettelse av aktive digitale selvforsvarsresponser. Som han påpeker kan en stat i motsatt fall ha gjort alt i sin makt for å forhindre digitale angrep igangsatt fra eget territorium, men likevel bli utsatt for grenseoverskridende selvforsvarsresponser.[98]

Etter mitt syn vil en vid adgang til selvforsvarsresponser uavhengig av bevis for statsansvar, i tillegg gjøre reglene for statsansvar illusoriske og overflødige.

Rettspraksis er imidlertid etter statuttene for ICJ jf. art. 38 (1) (d) kun en subsidiær rettskilde, mens folkerettslig sedvanerett er en primær rettskilde jf. art. 38 (1) (b). I utgangspunktet veier derfor folkerettslig sedvanerett tyngre enn rettspraksis. Dersom statspraksis og opinio juris tilsier at det eksisterer en sedvanerettslig adgang til selvforsvar ved grenseoverskridende væpnede angrep fra ikke-statlige aktører uavhengig av statsansvar, trekker dette i så fall i retning av at en slik rett eksisterer til tross for uttalelser fra ICJ.

På den andre siden må både kravene etter jus ad bellum samt jus in bello være oppfylt for at en selvforsvarsrespons skal anses lovlig (se punkt 3.7). Kravet om distinksjon etter jus in bello innebærer at stater er forpliktet til å skille mellom sivile og militære mål i en væpnet konflikt. Proporsjonalitetskravet under jus in bello innebærer at et lovlig angrep anses ulovlig dersom det forårsaker for omfattede skader på sivile personer og gjenstander. Prinsippene har sedvanerettslig status, og kommer til uttrykk i art. 48 og 51 nr. 5 b i første tilleggsprotokoll av 1977 til de fire Genève-konvensjonene av 1949.[99]

Selv om en eventuell selvforsvarsrespons rettes direkte mot de ikke-statlige aktørene, tilsier kravene til distinksjon og proporsjonalitet under jus in bello varsomhet med igangsettelse av

---

97 ICJ, Mursaken (2004) avsnitt 139, Democratic Republic of the Congo v. Uganda (2005) avsnitt 146-147. Tallinn Manual 2.0 (2017) s. 345 avsnitt 18.

98 Sklerov (2012) s. 59-60 fotnote 16.

99 Genève-konvensjonene, Larsen (2014b), Larsen (2015).

grenseoverskridende selvforsvarsresponser der staten ikke kan holdes ansvarlig for det digitale angrepet. Ikke minst gjelder dette der selvforsvarsresponsen består av fysiske motangrep. Ved aktive digitale selvforsvarsresponser (punkt 3.2) innebærer internetts sammenkobling også større risiko for skade på uskyldige datasystemer (i verste fall essensielle statlige datasystemer) dersom det ikke er nødvendig å holde en stat ansvarlig, enn dersom det foreligger et slikt krav.

2.3 Når utgjør en digital operasjon et «væpnet angrep»?

2.3.1 Forholdet mellom maktforbudet etter FN-pakten artikkel 2(4) og selvforsvarsretten etter artikkel 51 ved digitale operasjoner

ICJ fastslo som nevnt i Atomvåpensaken (1996) at FN-pakten artikkel 2(4) og artikkel 51 får anvendelse på «any use of force, regardless of the weapons employed».[100] Dette medfører at også digitale operasjoner som når opp til terskelen for et «væpnet angrep» er omfattet av artikkel 51.[101] Spørsmålet er imidlertid når en digital operasjon utgjør et «væpnet angrep».[102]

Art. 51 er taus om hvor omfattende og intens en operasjon må være, før det er tale om et «væpnet angrep». Isteden er definisjonen av «væpnet angrep» nærmere fastlagt i sedvaneretten.[103] For at en hendelse skal utgjøre et «væpnet angrep» etter art. 51, må imidlertid terskelen for ulovlig maktbruk etter art. 2 (4) være overskredet. Dette følger av Nicaragua-saken (1986) hvor et «væpnet angrep» karakteriseres som den mest alvorlige formen for maktbruk.[104] Maktforbudet etter art. 2 (4) utgjør sedvanerett, men det nærmere innholdet er imidlertid noe uklart.[105] Saken omhandlet amerikansk støtte til opprørsbevegelsen contras i Nicaragua.[106] Flere av USAs aksjoner ble av ICJ bedømt som ulovlig maktbruk i strid med art. 2 (4). Den rene økonomiske støtten var imidlertid kun i strid med ikke-intervensjonsprinsippet (punkt 1.3.1).[107]

---

[100] ICJ, Atomvåpensaken (1996) s. 244 avsnitt 39.
[101] Tallinn Manual 2.0 (2017) s. 328 avsnitt 1.
[102] Graham (2010) s. 90.
[103] Ruud (2011) s. 195. Gray (2018) s. 612.
[104] ICJ Nicaragua-saken (1986), avsnitt 191.
[105] ICJ Nicaragua-saken (1986) avsnitt 190. Gray (2018) s. 603.
[106] Ruud (2011) s. 191.
[107] ICJ Nicaragua-saken (1986) avsnitt 228.

Terskelen for «væpnet angrep» etter art. 51 ligger imidlertid høyere enn terskelen for maktforbudet etter art. 2(4).[108] ICJ benyttet i Nicaragua-saken «the scale and effect»-kriteriet som et kriterium for å avgjøre om en hendelse utgjør et «væpnet angrep».[109]

Tallinn-manualen støtter seg til dette, og benytter «the scale and effect»-kriteriet både for å avgjøre om en digital operasjon utgjør ulovlig maktbruk og et «væpnet angrep».[110] Manualen påpeker at «scale and effect»-kriteriet reflekterer de kvantitative og kvalitative omstendighetene som må tas i betraktning ved vurderingen av om en digital operasjon utgjør ulovlig maktbruk.[111] Man kan gå utfra at det samme gjelder ved vurderingen av om terskelen for «væpnet angrep» etter art. 51 er overskredet.

2.3.2 «Scale and effect»-kriteriet

ICJ var i Nicaragua-saken taus om det nærmere innholdet av «scale and effect»-kriteriet.[112] Det følger imidlertid implisitt av generalforsamlingsresolusjonen «the Definition of Aggression» at et angrep må være tilstrekkelig alvorlig før det er tale om et «væpnet angrep» etter art. 51.[113]

Ifølge Tallinn-manualen er digitale operasjoner som medfører tap av liv, alvorlig skade eller betydelige ødeleggelser, klare tilfeller som vil utgjøre et «væpnet angrep» etter «scale and effect» - kriteriet. Tilfeller som klart faller utenfor er digital informasjonsinnhenting i etterretningsøyemed samt digitale operasjoner som medfører korte eller periodiske forstyrrelser på uviktige digitale tjenester. Folkeretten er imidlertid uklar når det gjelder den presise terskelen for når konsekvensene av en operasjon gjør denne til et «væpnet angrep». ICJ indikerte i Oljeplattform-saken at en skadelig operasjon rettet mot en enkelt militærinstallasjon kunne utgjøre et «væpnet angrep» etter art.51.[114]

---

108 Ruud (2011) s. 195.

109 ICJ Nicaragua-saken (1986), avsnitt 195.

110 Tallinn Manual 2.0 (2017) s. 330-331 avsnitt 1, 341 avsnitt 6 og 7.

111 Tallinn Manual 2.0 (2017) s. 330-331 avsnitt 1.

112 ICJ Nicaragua-saken (1986), avsnitt 195.

113 Generalforsamlingsresolusjon 29/3314 (1974). Sklerov (2012) s. 58. Faga (2017) s. 14.

114 ICJ, Oljeplattform-saken (2003) avsnitt 57, 61.Tallinn Manual 2.0 (2017) s. 341 avsnitt 8, 9.

Manualen påpeker at en serie av digitale operasjoner der hver enkelt operasjon faller under terskelen for et «væpnet angrep» kumulert kan utgjøre et «væpnet angrep», men fremhever at operasjonene må være utført av samme aktør, være relatert til hverandre og samlet oppfylle «scale and effect»-kriteriet. Kondoch påpeker at «the accumulation of events theory» er kontroversiell og ikke har oppnådd bred støtte verken av Sikkerhetsrådet eller av andre stater.[115]

I folkerettslig teori er det utviklet tre konkrete tilnærminger for å avgjøre om en digital operasjon utgjør et «væpnet angrep».[116]

Etter en instrumentbasert tilnærming vil skader forårsaket av et digitalt angrep bare utgjøre et «væpnet angrep» dersom skaden også kan oppnås ved et fysisk angrep. Et eksempel er en digital operasjon som ødelegger et kraftnett da dette vanligvis krever fysisk maktbruk.[117]

Etter en effektbasert tilnærming vurderes de totale effektene av den digitale operasjonen, særlig innvirkningen på statens økonomiske, politiske eller sosiale infrastruktur.[118] Et eksempel er digitale operasjoner som innebærer informasjonsmanipulasjon i en stats bank- og finansvesens slik at statens næringsvirksomhet blir alvorlig forstyrret. Skaden dette medfører på statens totale økonomi gjør at dette anses som et «væpnet angrep».[119]

Etter en objektiv ansvarstilnærming vil ethvert digitalt angrep mot en stats kritiske infrastruktur automatisk bli ansett som et «væpnet angrep» etter art. 51, som også etter enkelte teoretikeres syn legitimerer bruk av aktive digitale selvforsvarsresponser.[120]

Sklerov mener den effektbaserte tilnærmingen er mest hensiktsmessig da den dekker alle tilfellene etter den instrumentbaserte tilnærmingen, men samtidig åpner for at digitale operasjoner som ikke er sammenlignbare med fysiske angrep, kan utgjøre væpnede angrep. Den objektive ansvarstilnærmingen kan etter Sklerovs syn medføre brudd på folkeretten.

---

115 Tallinn Manual 2.0 (2017) s. 342 avsnitt 11. Kondoch (2013) s. 470.
116 Sklerov (2012) s. 59. Faga (2017) s. 14.
117 Sklerov (2012) s. 59, fotnote 12. Faga (2017) s. 14.
118 Sklerov (2012) s. 59. Faga (2017) s. 14.
119 Sklerov (2012) s. 59 fotnote 13.
120 Sklerov (2012) s. 59. Faga (2017) s. 14-15.

Årsaken er at ved automatisk igangsettelse av aktive selvforsvarsresponser risikerer staten å ramme en stat som er helt uten ansvar for operasjonen.[121]

Jeg er enig i dette, men vil tilføye at dersom spørsmålet om statsansvar og spørsmålet om terskelen for «væpnet angrep» holdes fra hverandre, er det fortsatt mulig for en stat etter en objektiv tilnærming å anse ethvert digitalt angrep på den kritiske infrastrukturen som et «væpnet angrep» jf. «the scale and effect»-kriteriet. Men den rammede staten må som nevnt uansett etablere statsansvar for angrepet før igangsettelse av aktive selvforsvarsresponser kan anses legitime etter folkeretten (se punkt 2.2.3).

Ekspertene bak Tallinn-manualen var delte i spørsmålet om skade på personer eller eiendom var et vilkår for å anse en digital operasjon som et «væpnet angrep». Noen mente for eksempel at rene finansielle tap ikke utgjorde et «væpnet angrep». Andre var av motsatt oppfatning. Andre igjen betraktet enhver digital operasjon mot en stats kritiske infrastruktur med alvorlige konsekvenser som et «væpnet angrep».[122]

Ekspertene synes dermed å støtte seg til forskjellige teoretiske modeller ved vurderingen av når et digitalt angrep utgjør et «væpnet angrep». Dette forklarer også hvorfor manualen bruker konkrete eksempler for å utdype «scale and effect»-kriteriet istedenfor generelle rettslige vurderinger. Manualen illustrerer slik den rettslige usikkerheten og den teoretiske uenigheten som hersker med tanke på klassifisering av digitale angrep. Selv om manualen ikke skal leses som uttrykk for staters offisielle syn, indikerer den at det eksisterer svært ulik statspraksis for kategorisering av digitale angrep.

Schmitt anser «scale and effects»-kriteriet for å være korrekt rettslig sett, men til liten praktisk nytte. Det rettslige innholdet i terskelen for «væpnet angrep» vil etter hans syn heller bli fastlagt av statene gjennom en utvikling av sedvaneretten. Han antar at stater vil behandle digitale operasjoner som væpnede angrep etter art. 51 dersom disse medfører alvorlige konsekvenser etter en effektbasert tilnærming. Nederlandske myndigheter har for eksempel uttalt at en digital operasjon som rammer vesentlige myndighetsfunksjoner kan bli kvalifisert som et «væpnet angrep» uavhengig av fysisk skade gitt at operasjonen kan medføre alvorlig forstyrrelse i myndighetsfunksjonen eller alvorlige og langvarige konsekvenser for statens

[121] Sklerov (2012) s. 59-60, fotnote 16.
[122] Tallinn Manual 2.0 (2017) s. 343 avsnitt 12, 13.

stabilitet. Schmitt påpeker imidlertid at staters holdninger til dette spørsmålet vil forbli uavklart frem til slike operasjoner inntreffer med tilstrekkelig grad av tetthet.[123]

Etter mitt syn kan man legge til at utviklingen av sedvaneretten til en viss grad er avhengig av at stater offentliggjør deres vurderinger og klassifiseringer av fiendtlige digitale operasjoner som de blir rammet av. Per i dag er det grunn til å anta at mye av denne informasjonen er sikkerhetsgradert. Dette svekker utviklingen av sedvaneretten på området, og medfører betydelig rettslig usikkerhet når det gjelder den nærmere terskelen for når en digital operasjon utgjør et «væpnet angrep». Etter mitt syn kan en rettslig avklaring på dette punktet forhindre selvforsvarsresponser i strid med folkeretten, men også medvirke til internasjonal konsensus om når selvforsvarsresponser er i samsvar med folkeretten. Dette vil igjen bidra til mindre politiske spenninger på det digitale området internasjonalt.

2.3.3 Betydningen av målet for operasjonen

Utgangspunktet er at digitale operasjoner rettet mot personer eller eiendom innen den rammede statens territorium, som er grenseoverskridende og tilstrekkelig alvorlig jf. «scale and effect»-kriteriet, utgjør et «væpnet angrep» etter art. 51, jf. Tallinn-manualen.[124]

Hvorvidt digitale operasjoner rettet mot eiendom eller personer utenfor statens territorium, kan utgjøre væpnede angrep mot denne staten, er ifølge manualen noe uklart. Gitt at de øvrige vilkårene er oppfylt, er ekspertene enige om at en operasjon mot en stats myndighetspersoner eller ikke-kommersielle fasiliteter, utgjør et «væpnet angrep». Som eksempel nevner manualen at en statsleder blir drept i utlandet forårsaket av en digital operasjon. Ellers eksisterer det ifølge manualen ingen klar regel. Avgjørelsen vil da blant annet avhenge av om objektet er statseid, skadeomfanget, de rammede individenes status og om operasjonen er politisk motivert, altså gjennomført ut i fra objektets eller individets nasjonale tilhørighet.[125]

---

[123] Schmitt (2017) s. 246. Advisory Council on International Affairs No 77, AIV/No 22 (2011), s. 20.

[124] Tallinn Manual 2.0 (2017) s. 346 avsnitt 21

[125] Tallinn Manual 2.0 (2017) s. 346 avsnitt 22.

2.3.4 Betydningen av angripers intensjon

Det hersker uenighet blant Tallinn-manualens eksperter om angripers intensjon er av betydning for bedømmelsen av om en digital operasjon utgjør et «væpnet angrep».[126]

Flertallet mener at intensjon er irrelevant og at det kun er «scale and effect»-kriteriet som har betydning. Mindretallet mener at staten må ha hatt en intensjon om å igangsette et «væpnet angrep». Manualen begrunner ikke uenigheten nærmere.[127] Roscini mener det følger av nødvendighetskriteriet (punkt 3.6) at staten som et minimum blant annet må fastslå at den skadelige digitale operasjonen ikke var et uhell, før selvforsvarsretten kan inntre.[128]

ICJ undersøkte i Oljeplattform-saken om flere fiendtlige operasjoner som USA mente kunne tilbakeføres til Iran, utgjorde et «væpnet angrep» etter art. 51 samlet sett, herunder om disse spesifikt var rettet mot USA. Irans manglende intensjon om å ramme USA synes her å bli brukt som et rettslig argument for at det ikke forelå et «væpnet angrep». Avgjørelsen taler dermed for at intensjon har betydning ved vurderingen av om en operasjon utgjør et «væpnet angrep».[129]

Både rettsavgjørelser og juridisk teori er etter statuttene for ICJ subsidiære rettskilder jf. art. 38 (1)(d). Det er dermed vanskelig å avgjøre på generelt grunnlag hvilken av disse rettskildene som har størst vekt. ICJs avgjørelser er imidlertid kun bindende mellom partene jf. art. 59 jf. art. 38 (1) (d). Oljeplattform-saken gjaldt ikke digitale operasjoner, og som nevnt tidligere er ikke alle reglene på dette området tilpasset digital krigføring. Dette tilsier at Tallinn-manualen som et gjennomtenkt akademisk verk på cyberområdet utarbeidet av eksperter fra mange stater, veier tyngre på dette punktet, og at intensjonen ikke har betydning ved bedømmelsen av om en digital operasjon utgjør et «væpnet angrep».

Ettersom hastigheten på digitale angrep gjør det tilnærmet umulig for den rammede staten å undersøke angripers intensjon før den tyr til selvforsvarsresponser, bør heller ikke intensjonen de lege ferenda etter mitt syn ha betydning ved digitale angrep. Ellers kan selvforsvarsretten bli illusorisk.

---

126 Tallinn Manual 2.0 (2017) s. 343-344 avsnitt 14.

127 Tallinn Manual 2.0 (2017) s. 343-344 avsnitt 14, 15.

128 Roscini (2010) s. 119.

129 ICJ, Oljeplattform-saken (2003) avsnitt 64. Kondoch (2013) s. 469.

Selvforsvarsresponsen må som manualen påpeker uansett oppfylle kravene til blant annet nødvendighet og proporsjonalitet.[130]

2.4 Samlede betraktninger

Som kapittelet har vist eksisterer det en rett til selvforsvar etter FN-pakten artikkel 51 og folkerettslig sedvanerett ved digitale angrep. Når denne retten inntrer er imidlertid omdiskutert.

Et grunnleggende krav er at det foreligger et grenseoverskridende element. Tilskrivelse av ansvar for en digital operasjon bedømmes etter reglene for statsansvar (punkt 2.2.1). Hvorvidt det er et krav om at angrepet kan tilbakeføres til en stat, hersker det uenighet om i teorien (se punkt 2.2.3). Etter mitt syn vil en selvforsvarsrett uten krav til etablering av statsansvar, innebære en for vid adgang til selvforsvar, og gjøre reglene for statsansvar illusoriske. Risikoen for utilsiktet skade vil også bli større, noe som særlig kan stride imot jus in bello. Jeg mener at en stat i det minste må kunne holdes indirekte ansvarlig for et digitalt angrep før dette utløser selvforsvarsretten.

Hvor stor grad av statlig kontroll som kreves for å fastslå statsansvar der operasjonen utføres av ikke-statlige aktører, er kontroversielt (punkt 2.2.1). Tallinn-manualen benytter «effective control»-kriteriet slik dette er fastslått i ICJs rettspraksis. Det synes imidlertid å herske bred konsensus blant teoretikere og stater om at dette kriteriet har utviklet seg til en standard for indirekte ansvar. Dette baserer de på det generelle aktsomhetskravet som påligger alle stater til å forhindre at eget territorium blir brukt til igangsettelse av angrep mot andre stater. Enkelte teoretikere mener brudd på aktsomhetsnormen utløser en stats selvforsvarsrett forutsatt at de andre vilkårene for selvforsvarsutøvelse er oppfylt, mens Tallinn-manualen kun taler om mottiltak.

For at selvforsvarsretten skal inntre må den angrepne staten kunne bevise hvilken stat som står bak det digitale angrepet. Det finnes som nevnt ingen folkerettslig regel med tanke på beviskravet for etablering av statsansvar for digitale operasjoner (punkt 2.2.2). Rettspraksis trekker imidlertid i retning av et høyt beviskrav og at bevisbyrden påligger den angrepne staten. Dette underbygges av hensynet til å motvirke feiltilskrivelse av ansvar og skade på uskyldige systemer i strid med både jus ad bellum og jus in bello. Tallinn-manualen anser en konkret rimelighetsvurdering for avgjørende. Enkelte teoretikere mener en stat har oppfylt sin

[130] Tallinn Manual 2.0 (2017) s. 344 avsnitt 14.

bevisbyrde dersom den i god tro og etter beste tekniske evne pålegger statsansvar for et digitalt angrep. Jeg er som nevnt enig i dette. For å motvirke at stater i realiteten mister sin selvforsvarsrett ved digitale angrep, er det viktig at beviskravet ikke settes for høyt.

Selvforsvarsretten inntrer ved et «væpnet angrep» (punkt 2.3). Kapittelet har drøftet når en digital operasjon anses som et «væpnet angrep», herunder «scale and effect»-kriteriet (punkt 2.3.2). Dette kriteriet gir imidlertid i seg selv liten veiledning, og ulike tilnærminger til terskelen for «væpnet angrep» ved digitale operasjoner er utviklet i folkerettslig teori.

Når det gjelder spørsmålet om angripers intensjon har betydning for om en digital operasjon utgjør et «væpnet angrep» (punkt 2.3.4), mener som nevnt flertallet bak Tallinn-manualen at angripers intensjon er irrelevant. Oljeplattform-saken trekker imidlertid i motsatt retning. Tallinn-manualen veier etter mitt syn tyngre som et saksspesifikt, gjennomtenkt og akademisk verk på området. Etter mitt syn burde heller ikke intensjonen ha betydning ved vurderingen av om en digital operasjon utgjør et «væpnet angrep» de lege ferenda. Begrunnelsen er at farten på digitale angrep gjør at en stat i mange tilfeller ikke rekker å foreta en slik vurdering, og at selvforsvarsretten i motsatt fall kan miste sin betydning. Selvforsvarsresponsen må uansett oppfylle kravene til blant annet nødvendighet og proporsjonalitet (punkt 3.6 og 3.7).

Det rettslige innholdet i terskelen for «væpnet angrep» ved digitale operasjoner, vil ifølge enkelte teoretikere bli fastlagt av statene gjennom en utvikling av sedvaneretten. En slik utvikling avhenger imidlertid etter mitt syn til en viss grad av offentliggjøring av staters vurderinger og klassifiseringer av digitale operasjoner. Mangelen på slik åpenhet svekker utviklingen av sedvaneretten på området, og medfører rettslig usikkerhet.

3 Grensene for selvforsvarsretten

3.1 Innledning

Når det først er fastslått at et digitalt angrep utløser en stats selvforsvarsrett, blir spørsmålet hvor grensene for selve selvforsvaret går. FN-pakten art. 51 sier lite om dette, og suppleres her av folkerettslig sedvanerett.[131]

Selve selvforsvarshandlingen kan bestå av enten fysisk eller ikke-fysisk maktbruk, herunder digital maktbruk. Det finnes tre former for digitale selvforsvarstiltak; passive selvforsvarsmetoder, aktive selvforsvarsresponser og en blanding av disse.[132] Det er de fysiske og aktive digitale selvforsvarsresponser som er interessante å analysere i lys av grensene for selvforsvarsretten. Rene passive digitale selvforsvarsresponser som brannmurer, kryptering, automatiske varslingssystemer og lignende, vil en stat alltids lovlig kunne iverksette da disse ikke innebærer bruk av makt, jf. FN-pakten art. 2 (4).[133] Kapittelet vil derfor ikke behandle slike selvforsvarstiltak.

3.2 Aktive digitale selvforsvarsresponser

Et aktivt digitalt selvforsvar består av tre stadier; Intrusion Detection Systems («IDS»), sporingsteknologi («traceback») samt aktive motangrep i form av tilbakesending av data for å avbryte eller forstyrre et digitalt angrep.[134]

Hovedargumentet for bruk av aktive digitale selvforsvarsresponser er at passive selvforsvarsmetoder ikke har vist seg tilstrekkelige for å forhindre nye metoder for og en økende grad av digitale angrep, i tillegg til deres manglende avskrekkende effekt på potensielle angripere.[135]

---

131 Ruud (2011) s. 199.

132 Et eksempel er såkalte «honeypots» som er feller skapt for å lokke til seg hackere i håp om å avsløre deres identitet og angrepsteknikker. Kesan (2012) s. 471-472. Sandvik (2012) s. 42.

133 Mudrinich (2012) s. 182. Kesan (2012) s. 471, 475.

134 Mudrinich (2012) s. 182. Kesan (2012) s. 471, 475.

135 Mudrinich (2012) s. 181. Kesan (2012) s. 432-434, 474. Hadji-Janev (2016) s. 53. Graham (2010) s. 92. Flowers (2014) s. 305.

Et annet argument er at dersom myndighetene unnlater å iverksette aktive digitale selvforsvarsresponser kan man risikere at private aktører selv benytter seg av slike metoder for å beskytte egen virksomhet.[136] Problemet med dette er den manglende offentlige kontrollen dette innebærer, samt risikoen for at staten der virksomheten har sete holdes ansvarlig for virksomhetens motangrep. Slike privatinitierte motangrep kan dermed bli bedømt som igangsettelse av selvforsvarsresponser etter art. 51, noe som vil stride mot distinksjonsprinsippet etter jus i bello da de som beslutter dette må være av militær rang (punkt 3.8). Dette medfører fare for konflikt mellom stater på feilaktig grunnlag, og dermed skade på uskyldige datasystemer i strid med folkeretten. Ved at staten selv iverksetter aktive selvforsvarsresponser sender den dermed et signal til nasjonale private aktører om et velfungerende statlig digitalt forsvar. Risikoen for at private virksomheter tyr til egne aktive motangrep vil dermed bli redusert. Alternativt kan stater ved deres respektive militære enheter og private aktører samarbeide om oppdagelse og sporing av digitale angrep. Et slikt samarbeid er særlig aktuelt der den private aktøren er eier av samfunnskritisk, nasjonal infrastruktur. I Norge samarbeider Telenor med både Cyberforsvaret og Nasjonal sikkerhetsmyndighet om dette.[137]

Selv om aktive digitale selvforsvarsresponser ikke innebærer fysisk maktbruk, er det omdiskutert hvorvidt de er i samsvar med folkerettens begrensninger for selvforsvarsutøvelse. Aktive digitale selvforsvarsresponser innebærer som nevnt en fare for skade på uskyldige datasystemer.[138] Dette skyldes blant annet at angrepene ofte ledes gjennom tredjelands nettverk som øker risikoen for at feil aktør holdes ansvarlig. I tillegg er kirurgisk presisjon tilnærmet umulig.[139]

Dersom feil stat holdes ansvarlig og denne utsettes for aktive digitale selvforsvarsresponser kan dette også utløse denne statens selvforsvarsrett som igjen kan medføre vekslende responshandlinger i en konfliktspiral det er vanskelig å komme ut av.[140]

Faren for utilsiktet skade gjør at Kesan og Hayes mener aktive digitale selvforsvarsresponser ikke bør brukes i for stort omfang. De anser imidlertid bruken av begrensede aktive

---

136 Rosenzewig (2014) s. 103-104.

137 Telenor (udatert)

138 Flowers (2014) s. 303, 306. Sandvik (2012) s. 42. Kesan (2012) s. 434, 527.

139 Graham (2010) s. 102. Mudrinich (2012) s. 193.

140 Flowers (2014) s. 305.

motangrep («mitigative counter-striking») for å være i samsvar med folkeretten. Dette er aktive selvforsvarsresponser som begrenser skader på rammede datasystemer, og som kun respoderer med den maktbruk som er strengt nødvendig for å beskytte systemet fra ytterligere skade.[141]

Kesan og Hayes påpeker forøvrig at aktive forsvarsmetoder allerede har foregått i flere år både fra myndigheter og private aktører, selv om man kan stille spørsmål ved lovligheten av måten de er blitt utøvd på.[142]

Nedenfor vil de folkerettslige begrensingene for både fysiske og aktive digitale selvforsvarsresponser mot digitale angrep, analyseres nærmere.

3.3 «... inntil Sikkerhetsrådet har truffet de tiltak som er nødvendige ...»

En tidsmessig begrensning for selvforsvarsutøvelsen følger allerede av ordlyden etter FN-pakten artikkel 51. Selvforsvarsretten gjelder kun «... inntil Sikkerhetsrådet har truffet de tiltak som er nødvendige for å opprettholde internasjonal fred og sikkerhet ...». Av art. 51 følger også en umiddelbar rapporteringsplikt til Sikkerhetsrådet ved utøvelse av selvforsvarsretten.

Halberstam er av den oppfatning at Sikkerhetsrådet eksplisitt må frata statens rett til ytterligere selvforsvarshandlinger for at staten skal miste denne retten. Tallinn-manualen er av samme oppfatning ved selvforsvar mot digitale angrep. Sikkerhetsrådets tiltak må dessuten være effektive.[143]

Sikkerhetsrådet har så langt ikke gitt en resolusjon som gjelder digitale operasjoner. Det er likevel ingen grunn til at organet ikke skal kunne behandle digitale operasjoner som en trussel mot freden etter kapittel VII i FN-pakten. Kina, Russland og USA er ifølge Kondoch svært uenige i hvordan digital sikkerhet skal håndteres. President Obama forsøkte å adressere cyberretalerte problemer med Kina i juni 2013, men mislyktes. Når medlemmer av

[141] Kesan (2012) s. 435, 475, 527.
[142] Kesan (2012) s. 475.
[143] Halberstam (1996) s. 231. Tallinn Manual 2.0 (2017) s. 356 avsnitt 2. Ruud (2011) s. 199.

Sikkerhetsrådet ikke klarer å løse dette på et bilateralt nivå, mener Kondoch det er vanskelig å se hvordan de skal oppnå enighet i Sikkerhetsrådet.[144]

Jeg er ikke enig i dette. Uenighet på bilateralt nivå om visse punkter trenger ikke innebære uenighet i Sikkerhetsrådet om andre punkter. Selv om Kina og USA er uenige om visse cyberrelaterte problemer på bilateralt nivå, betyr ikke dette at de ikke kan oppnå enighet når det gjelder andre cyberrelaterte problemer i Sikkerhetsrådet.

3.4 Et pågående eller umiddelbart forestående væpnet angrep

Av ordlyden i artikkel 51 følger det at et væpnet angrep «occurs». Dette tilsier at angrepet må være påbegynt eller inntruffet. Et omstridt tema er om det eksisterer en rett til preventivt selvforsvar før et angrep faktisk er påbegynt.[145]

Det er bred enighet blant stater og teoretikere om en rett til preventivt selvforsvar ved et umiddelbart forestående «væpnet angrep» («an imminent attack»).[146] Begrunnelsen er at man ikke kan forvente at stater skal forholde seg passive og vente på et angrep før de handler.[147] Dette synet baserer seg på den nevnte Caroline-saken.[148]

Saken omhandlet ikke preventivt selvforsvar direkte, men Websters formulering om at selvforsvarsretten inntrer når nødvendigheten av selvforsvar er «instant, overwhelming, leaving no choice of means, and no moment for deliberation»[149], anses som det klassiske uttrykket for en slik rett.[150] Det er bred enighet om at preventivt selvforsvar er lovlig dersom disse kriteriene er oppfylt.[151]

Ekspertene bak Tallinn-manualen er også av den oppfatning at det eksisterer en rett til preventivt selvforsvar ved digitale operasjoner.[152]

---

144 Kondoch (2013) s. 474.
145 Gray (2018) s. 614. Ruud (2011) s. 197.
146 Ruud (2011) s. 198. Schmitt (2017) s. 246-247. Sklerov (2012) s. 51.
147 Roscini (2010) s. 122.
148 Jennings (1938). Tallinn Manual 2.0 (2017) s. 350-351 avsnitt 2.
149 Jennings (1938) s. 89.
150 Jennings (1938) s. 89. Ruud (2011) s. 195.
151 Tsagourias (2017) s 34.
152 Tallinn Manual 2.0 (2017) s. 350 avsnitt 2.

Tidspunktet for når et «væpnet angrep» anses som umiddelbart forestående, er det imidlertid uenighet om.[153] Et annet kontroversielt spørsmål er om det eksisterer en rett til selvforsvar når angrepet ikke er umiddelbart forestående i form av såkalte forkjøpsangrep («pre-emptive self-defence»).[154] Dette vil omtales nærmere under.

3.4.1 Preventivt selvforsvar

Vilkåret for utøvelse av preventivt selvforsvar er at det foreligger et umiddelbart forestående væpnet angrep («an imminent attack»).

Et spørsmål er om det eksisterer en selvforsvarsrett når angrepet ikke er umiddelbart forestående ved såkalte forkjøpsangrep («pre-emptive self-defence»). Dette er svært kontroversielt da det ifølge Kondoch innebærer en rett til selvforsvar ved en oppfattet, men fjern trussel, som igjen medfører en betydelig risiko for statlig konflikteskalering. I tillegg kan slike forkjøpsangrep brukes som skalkeskjul for andre motiver enn selvforsvar, og dermed åpne for misbruk.[155] Jeg er enig i dette, og tilføyer at disse betrakningene også får anvendelse på digitale angrep.

Det tradisjonelle utgangspunktet for vurderingen av om det foreligger et umiddelbart forestående «væpnet angrep», er den tidsmessige nærheten til angrepet slik det kommer til uttrykk i Caroline-kriteriene.[156]

Disse kriteriene gir imidlertid ikke stater tilstrekkelig tid til å forsvare seg mot digitale angrep ettersom slike angrep kan utføres uten advarsel, i løpet av millisekunder og med totalødeleggende effekt.[157] Farten på digitale operasjoner tilsier at selvforsvar er umulig når det digitale angrepet først er igangsatt.[158] Preventivt selvforsvar er derfor eneste mulighet ved digitale angrep.[159]

---

153 Schmitt (2017) s. 247. Tsagourias (2017) s 34.
154 Gray (2018) s. 614.
155 Kondoch (2013) s. 471, fotnote 73.
156 Jennings (1938) s. 89. Schmitt (2017) s. 247. Sklerov (2012) s. 51.
157 Schmitt (2017) s. 247. Tsagourias (2017) s 34.
158 Tallinn Manual 2.0 (2017) s. 351 avsnitt 3
159 Tsagourias (2017) s 34

Spørsmålet er imidlertid på hvilket tidspunkt en stat lovlig kan utøve selvforsvar før et digitalt angrep blir igangsatt.[160]

Ifølge Schmitt må den digitale operasjonen være en del av en overordnet operasjon som kuliminerer i et «væpnet angrep». Operasjonen må utgjøre et utgjenkallelig steg på veien til et umiddelbart forestående og sannsynligvis uunngåelig angrep, og selvforsvaret må utføres i forkant av angrepet under det han kaller «the last possible window of opportunity».[161] Roscini anser dette som en fornuftig anvendelse av kriteriene fra Caroline-saken.[162]

Kesan og Hayes mener Schmitts kriterier setter en for høy terskel for utførelse av preventive selvforsvarshandlinger. De mener at preventivt selvforsvar lovlig kan igangsettes også etter et avsluttet angrep, dersom bevis tilsier at dette er en del av et pågående angrep. De fremtidige angrepene er da umiddelbart forestående («imminent») etter deres syn.[163] Sklerov er av samme oppfatning.[164]

Tallinn-manualen hevder at retten til preventivt selvforsvar inntrer når angriper klart har forpliktet seg til å igangsette et angrep, og den potensielt rammede staten vil miste dets mulighet til effektivt å forsvare seg med mindre den handler. Ekspertene mener som Schmitt at utøvelse av preventivt selvforsvar må foretas under «the last window of opportunity» forut for angrepet. Angrepet trenger imidlertid ikke etter deres syn være i ferd med å igangsettes; dette setter en for streng tidsmessig grense for selvforsvaret.[165]

3.4.2 «The last window of opportunity»

Etter «the last window of opportunity»-standarden kan en stat utøve selvforsvar mot digitale angrep når angriper har en klar intensjon om å igangsette et væpnet angrep, og den angrepne staten ellers vil miste muligheten til effektiv å forsvare seg selv. Det avgjørende er ikke den tidsmessige nærheten til angrepet, men tidspunktet for når unnlatelse av å handle vil medføre at staten ikke blir i stand til å forsvare seg selv på en effektiv måte. Dette vinduet kan vise seg lenge før angrepet faktisk inntreffer. Tallinn-manualen påpeker imidlertid at jo lenger tid det

[160] Tsagourias (2017) s 34
[161] Schmitt (1999) s. 932-933
[162] Roscini (2010) s. 122
[163] Kesan (2012) s. 528-529
[164] Sklerov (2012) s. 51
[165] Tallinn Manual 2.0 (2017) s. 351 avsnitt 4

gjenstår til det forventede angrepet, desto mindre sannsynlig vil det være at preventivt selvforsvar er eneste mulige løsning, altså at det er i samsvar med nødvendighetskravet.[166]

Man må ifølge manualen avgrense mot rene forberedelseshandlinger og startfasen av et angrep. Plassering av for eksempel en «logic bomb»[167] kvalifiserer som et umiddelbart forestående angrep dersom programvarens aktiveringsvilkår sannsynligvis vil bli oppfylt. Plassering av fjernstyrt ondartet programvare vil derimot ikke utgjøre et umiddelbart forestående angrep når dette kun innebærer at angriper skaffer seg en mulighet til å angripe en gang i fremtiden. Et angrep anses i slike tilfeller umiddelbart forestående først når angriper har en klar intensjon om å aktivere den, og staten ellers mister muligheten til effektivt å forsvare seg selv. Manualen påpeker at det i praksis er vanskelig å trekke dette skillet. Det avgjørende blir derfor en rimelighetsvurdering av statens tilnærming til situasjonen samt om de andre vilkårene for selvforsvarsutøvelse er oppfylt.[168]

Et mindretall av ekspertene mener «the last window of opportunity»-standarden ikke utgjør gjeldende rett. De mener selvforsvar må være siste mulighet, og at angrepet må være i ferd med å bli igangsatt. Standarden er etter deres syn for åpen for tolkning, og dermed også misbruk.[169] Ekspertgruppen er enige om at staten må ha konkludert med at angriper har besluttet å angripe.[170]

Tsagourias påpeker at vurderingen av om et digitalt angrep er umiddelbart forestående er utfordrende på grunn av hemmeligholdet rundt digitale operasjoner.[171] Han anser imidlertid «the last window of opportunity-standard» oppstilt i Tallinn-manualen for å være mye videre enn de snevre Caroline-kriteriene nevnt tidligere. Dersom kravet om et umiddelbart forestående angrep skal vurderes etter denne, kan en stat slik han ser det lovlig benytte seg av selvforsvarshandlinger lenge før et væpnet angrep faktisk inntreffer. En slik vid adgang til preventivt selvforsvar vil etter hans syn tillate forkjøpsangrep som er svært omstridt etter

166 Tallinn Manual 2.0 (2017) s. 352 avsnitt 4, 5.

167 Wikipedia (2018): «A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.».

168 Tallinn Manual 2.0 (2017) s. 352 avsnitt 7, 8.

169 Tallinn Manual 2.0 (2017) s. 353 avsnitt 9.

170 Tallinn Manual 2.0 (2017) s. 353 avsnitt 10, 11.

171 Tsagourias (2017) s 35. Gardam (2004) s. 179.

folkeretten. Kondoch er også skeptisk til at Tallinn-manualen synes å støtte forkjøpsangrep, og peker på faren for eskalering og misbruk.[172]

Jeg er enig i dette og vil tilføye at selv om manualen synes å påstå at nødvendighetskriteriet uansett vil kunne fungere som en barriere for preventive selvforsvarshandlinger, vil brudd på både nødvendighetskriteriet i seg selv samt proporsjonalitetskriteriet kunne unngås ved en strengere tidsmessig begrensning. Om denne standarden faktisk er et uttrykk for gjeldende rett de lege lata er usikkert.

3.5 Umiddelbarhet

Kravene til umiddelbarhet, nødvendighet og forholdsmessighet kan utledes indirekte av begrepet «selvforsvar», men utgjør også folkerettslig sedvanerett, jf. Caroline-saken.[173]

Kravet til umiddelbarhet innebærer et forbud mot rene gjengjeldelseshandlinger. Selvforsvarshandlingen må foretas innen rimelig tid etter et inntruffet væpnet angrep, og må følge som et direkte svar på det.[174]

Vurderingen av om umiddelbarhetskravet er oppfylt ved selvforsvar mot digitale angrep avhenger av momenter som den tidsmessige nærheten mellom angrepet og selvforsvarshandlingen, tiden det tar å identifisere angriperen samt den nødvendige perioden for å forberede selvforsvaret. Manualen påpeker at en konkret rimelighetsvurdering blir avgjørende.[175]

Jo lenger tid det tar å spore opp aktøren bak et digitalt angrep, desto mindre sannsynlig er det imidlertid at umiddelbarhetskravet er tilfredsstilt. Som Flowers påpeker kan selvforsvarsresponser etter at et angrep virker avsluttet fort fremstå som ulovlig gjengjeldelse. Dersom angrepet derimot anses som del av en serie av pågående angrep, vil bruken av aktive digitale selvforsvarsresponser ifølge Sklerov kunne forsvares med tanke på å stanse fremtidige angrep.[176] Tallinn-manualen anser en rimelighetsvurdering som avgjørende; dersom det er rimelig å anta at ytterligere digitale operasjoner vil følge, kan staten fortsette å

---

172 Tsagourias (2017) s 35. Kondoch (2013) s. 471.
173 Ruud (2011) s. 200. Jennings (1938).
174 Ruud (2011) s. 200. Roscini (2010) s. 120. Kondoch (2013) s. 472.
175 Tallinn Manual 2.0 (2017) s. 353-354 avsnitt 12, 13.
176 Sklerov (2012) s. 70, Flowers (2014) s. 305.

handle i selvforsvar. Er konklusjonen motsatt vil ytterligere maktbruk anses som gjengjeldelseshandlinger i strid med umiddelbarhetskravet.[177]

Farten, uforutsigbarheten samt hemmeligholdet rundt de fleste digitale operasjoner gjør det vanskelig for stater å respondere raskt på digitale angrep.[178] En stats militære nettverk kan for eksempel ha blitt satt ut av drift av angrepet, slik at en umiddelbar respons er umulig.[179] I tillegg kan et digitalt angrep ligge usynlig i statens datasystemer og gjøre at skaden ikke oppdages før etter lang tid. Et eksempel på et slikt usynlig digitalt angrep er som manualen påpeker, bruk av en «worm» slik som Stuxnet (se punkt 4.2). Som Roscini nevner kan også bruken av «logic bombs» eller «time bombs» gjøre at selve skaden oppstår lenge etter angrepet ble igangsatt. Slike usynlige eller forsinkede digitale angrep vil også forsinke selvforsvarsreaksjonen, og må etter Roscinis mening gi en viss tidsmessig fleksibilitet ved bedømmelsen av om kravet til umiddelbarhet er oppfylt.[180] Jeg er enig i at disse faktorene taler for at umiddelbarhetskravet anvendes med fleksibilitet, men for at responsen ikke skal bli bedømt som ulovlig gjengjeldelse krever dette etter mitt syn at kravene til nødvendighet og proporsjonalitet er klart oppfylt.

3.6 Nødvendighet

Nødvendighetskravet samt proporsjonalitetskravet utgjør veletablerte sedvanerettslige krav til selvforsvarsutøvelsen under jus ad bellum. ICJ har stadfestet og bekreftet dette mange ganger.[181]

Kravet til nødvendighet innebærer at handlinger utført i selvforsvar må være nødvendige for selvforsvarets formål som er å forhindre, stanse eller slå tilbake angrepet. Tiltak som ikke innebærer maktbruk må ha vist seg unyttige.[182] Staten må videre ha tilskrevet angrepet til

---

177 Tallinn Manual 2.0 (2017) s. 353-354 avsnitt 13.

178 Melzer (2011) s. 18.

179 Roscini (2010) s. 120.

180 Tallinn Manual 2.0 (2017) s. 354 avsnitt 14. Roscini (2010) s. 120.

181 ICJ, Nicaragua-saken (1986) avsnitt 176, 194, Atomvåpen-saken (1996) avsnitt 41, Oljeplattform-saken (2003) avsnitt 74, Democratic Republic of the Congo v. Uganda (2005) s. 223, avsnitt 147. Dinniss (2012) s. 102.

182 Ago (1980) s. 69. Kondoch (2013) s. 472. Dinniss (2012) s. 102.

riktig aktør (punkt 2.2).[183] I tillegg til dette må maktbruken begrenses til det som er strengt nødvendig for å forhindre, stanse eller slå tilbake angrepet.[184]

Selvforsvarshandlinger er ikke nødvendig når formålet med selvforsvaret er oppnådd, og ytterligere selvforsvarshandlinger vil da være ulovlige.[185] Selvforsvar skal derfor ikke brukes som et påskudd for utvidelse av selvforsvarsaksjonen til andre mål enn det som er nødvendig for å oppnå formålet med selvforsvaret.[186]

Kravet til nødvendighet er strengt, og gir ikke rom for skjønn.[187]

Ved digitale angrep innebærer dette at dersom et passivt digitalt forsvar er tilstrekkelig for å forhindre, stanse eller slå tilbake et digitalt angrep, vil både fysiske samt aktive digitale motangrep som innebærer bruk av makt, være unødvendige og dermed ulovlige etter jus ad bellum.[188] Dersom bruken av fysiske eller aktive digitale motangrep er nødvendig, må maktbruken uansett begrenses til det som er nødvendig for å oppnå formålet med selvforsvaret.[189]

Hovedargumentet i teorien for bruk av aktive digitale selvforsvarsresponser er som nevnt at passive selvforsvarsmetoder ikke anses å utgjøre tilstrekkelig selvforsvar mot digitale angrep.[190]

3.7 Proporsjonalitet

Proporsjonalitetskravet under jus ad bellum innebærer at selvforsvarsaksjonen må stå i et rimelig forhold til formålet med selvforsvaret som er å forhindre, stanse eller slå tilbake et «væpnet angrep».[191] Selvforsvarshandlingen skal ikke fremstå som gjengjeldelse eller straff, og må derfor begrenses i omfang, varighet og intensitet til det som er nødvendig for å sikre

---

183 Roscini (2010) s. 119.

184 Ruud (2011) s. 200. Gray (2018) s. 612.

185 Melzer (2011) s. 17.

186 Ruud (2011) s. 200.

187 ICJ, Oljeplattform-saken (2003) avsnitt 73.

188 Tallinn Manual 2.0 (2017) s. 349 avsnitt 3, 4. Schmitt (2017) s. 248-249.

189 Ruud (2011) s. 200. Gray (2018) s. 612.

190 Mudrinich (2012) s. 181. Kesan (2012) s. 432-434, 474. Hadji-Janev (2016) s. 53. Graham (2010) s. 92. Flowers (2014) s. 305.

191 Ago (1980) s. 69. Gray (2018) s. 612. Sklerov (2012) s. 50.

formålet.[192] I Nicaragua-saken ble det klart at dersom det tar lang tid å oppnå formålet med selvforsvaret, kan selvforsvaret bedømmes som uproporsjonalt.[193] Det trenger ikke være proporsjonalitet mellom det væpnede angrepets maktbruk og selvforsvarets maktbruk. Maktbruken trenger heller ikke være av samme art.[194] ICJ har stadfestet at arten av målet for selvforsvarsaksjonen har betydning.[195] Selvforsvaret må også begrenses til det området hvor angrepet som skal slås tilbake vil inntreffe eller har inntruffet.[196]

Vurderingen av om såkalte aktive digitale selvforsvarsresponser er i samsvar med proporsjonalitetskravet må vurderes utfra om responsene står i et rimelig forhold til formålet med selvforsvaret i den konkrete saken. En aktiv digital selvforsvarsrespons som brukes for å ramme andre deler av en digital infrastruktur enn der angrepet stammer fra, vil ikke utgjøre en forholdsmessig selvforsvarsrespons etter jus ad bellum. Som Schmitt påpeker vil for eksempel et motangrep mot hele den digitale infrastrukturen til angriperstaten være uforholdsmessig dersom angrepet kan overvinnes ved begrensede motangrep mot den digitale infrastrukturen hvor angrepet stammer fra.[197]

Heller ikke ved digitale angrep trenger maktbruken være av samme art og omfang for at proporsjonalitetskravet under jus ad bellum skal være oppfylt. Fysisk maktbruk kan derfor utgjøre svar på et digitalt angrep. Som eksempel nevner Tallinn-manualen at angriperstaten kan være usårbar for digitale motangrep, slik at en fysisk respons er eneste mulighet for å oppnå formålet med selvforsvaret.[198]

I prinsippet er som nevnt jus ad bellum og jus in bello to distinkte systemer der jus ad bellum består av de folkerettslige reglene for når en stat kan ty til militær makt, mens jus in bello omhandler reglene for opptreden under væpnet konflikt når dette først har oppstått.[199] Disse har to ulike proporsjonalitetsvurderinger. Maktbruk i selvforsvar etter art. 51 som er i samsvar med proporsjonalitetskravet etter jus ad bellum, kan dermed likevel stride mot proporsjonalitetskravet etter jus in bello.[200] ICJ har i Atomvåpen-saken uttalt at selv om

---

192 Ago (1980) s. 69. Dinniss (2012) s. 104. Gardam (2004) s. 156. Ruud (2011) s. 200.
193 ICJ, Nicaragua-saken (1986) avsnitt 237.
194 Ago (1980) s. 69. Gardam (2004) s. 161. Sklerov (2012) s. 51.
195 ICJ, Oljeplattform-saken (2003) avsnitt 74.
196 Gardam (2004) s. 163.
197 Schmitt (2017) s. 249.
198 Tallinn Manual 2.0 (2017) s. 349-350 avsnitt 5, 6.
199 Larsen (2014a).
200 Moussa (2014) s. 62-63, 65.

proporsjonalitetskravet er oppfylt etter jus ad bellum, må også kravene etter jus in bello være oppfylt for at maktbruk utført i selvforsvar skal anses lovlig.[201] Uttalelsen har blitt tolket forskjellig i folkerettslig teori. Noen mener den uttrykker at en selvforsvarshandling bare kan bedømmes som proporsjonal dersom den respekterer jus in bello-kriteriene. Moussa er blant dem som mener at ICJ heller mente å fastslå at maktbruk i selvforsvar kun er lovlig dersom proporsjonalitetskravet etter både jus ad bellum og jus in bello er oppfylt.[202]

Selv om proporsjonalitetskravet er oppfylt etter de nevnte jus ad bellum-kriteriene, avhenger dermed lovligheten av selvforsvaret også av at kriteriene for jus in bello er oppfylt. Særlig momenter som selvforsvarets utilsiktede konsekvenser, varigheten, midlene, metodene og målene for det, i tillegg til det geografiske og destruktive omfanget vil være relevante her.[203]

Dersom fysiske responser benyttes mot et digitalt angrep og dette innebærer omfattende sivile skader eller tap av liv, vil dette kunne stride i mot jus in bello og dermed gjøre selvforsvarshandlingen ulovlig, jf. uttalelsen i Atomvåpen-saken. Flere teoretikere mener at aktive digitale selvforsvarsresponser samsvarer bedre med prinsippene etter jus in bello enn fysiske responser, ved digitale væpnede angrep. Dette gjelder uavhengig av om slik maktbruk er i samsvar med proprosjonalitetskravet etter jus ad bellum.[204]

Det er usikkert om en stat i vurderingen av forholdsmessigheten av en selvforsvarsaksjon, kan betrakte en serie av mindre digitale angrep i ett.[205] Doktrinen om kumulasjon av hendelser («the doctrine of the accumulation of events») er ifølge Roscini kontroversiell.[206] I Oljeplattformsaken verken avviste eller bekreftet ICJ denne doktrinen.[207]

Et eget spørsmål er om såkalt Computer Network Exploitation (CNE) eller uthenting av sensitiv informasjon om angriperstatens datanettverk i sammenheng med utførelse av begrensede digitale motangrep, er i samsvar både med nødvendighetskravet og proporsjonalitetskravet.[208]

---

201 ICJ, Atomvåpensaken (1996) avsnitt 42, 43. Gardam (2004) s. 169.
202 Moussa (2014) s. 69.
203 Gardam (2004) s. 162.
204 Graham (2010) s. 98-99. Sklerov (2012) s. 71-72.
205 Roscini (2010) s. 120.
206 Roscini (2010) s. 120.
207 ICJ, Oljeplattform-saken (2003) avsnitt 64.
208 Wormdal (2018).

For eksempel er det blitt dokumentert at norsk og amerikansk etterretning samarbeider om å hente ut sensitiv informasjon om russiske datanettverk. Dette kan bli brukt både til å igangsette digitale angrep, eller for å finne ut av Russlands planer med tanke på å forhindre eventuelle fremtidige angrep.[209] Etterretning og spionasje reguleres som nevnt i utgangspunktet av statenes interne lovgivning, og ikke av folkeretten.[210] Det kan imidlertid argumenteres for at dersom slik spionasje benyttes i sammenheng med en selvforsvarsrespons, kan selvforsvarsresponsens maktbruk anses å være mer inngripende enn dersom slik informasjonsinnhenting ikke ble foretatt på samme tid.

Etter mitt syn er ikke innhenting av sensitiv informasjon i forbindelse med et begrenset motangrep ved et påført digitalt angrep verken i strid med nødvendighetskravet eller proporsjonalitetskravet så lenge formålet er å forhindre fremtidige dataangrep. Man kan se det slik at angriperstaten ved å igangsette digitale angrep eller la eget territorium bli benyttet til slike angrep, også har akseptert en risiko for å bli rammet av aktive digitale selvforsvarsresponser, og dermed også av spionasje som i utgangspunktet er mindre inngripende enn en aktiv selvforsvarsrespons.[211]

Det problematiske er imidlertid at slik informasjonsuthenting innebærer fare for misbruk og igangsettelse av aktive selvforsvarsresponser lenge etter at det digitale angrepet er utført. En konkret vurdering vil i så fall avgjøre om et slik aktivt motangrep basert på CNE kan forsvares utfra kravene til både umiddelbarhet, nødvendighet samt proporsjonalitet. Utover dette kan CNE medføre fare for ytterligere politiske spenninger og konflikteskalering, noe som etter mitt syn tilsier statlig varsomhet med bruken av dette.[212]

3.8 Hvem skal avgjøre om kriteriene for utøvelse av selvforsvar er oppfylt, og hva selvforsvaret nærmere skal bestå i?

Spørsmålet om hvem som i det konkrete tilfellet skal avgjøre om eventuelle aktive digitale motangrep skal iverksettes, har betydning for om kravene til jus ad bellum og jus in bello overholdes i praksis.

---

209 Wormdal (2018).
210 Ohlin (2017) s. 1580.
211 Sklerov (2012) s. 71.
212 Wormdal (2018).

Noen mener at systemadministratorer må avgjøre dette fordi responsen på et digitalt angrep må komme relativt raskt for å ha effekt.[213] Andre mener at systemadministratorer i såfall må ha autorisasjon.[214] Andre igjen mener at vedkommende må være av militær rang grunnet distinksjonsprinsipet; personen som igangsetter angrepet må kunne anses som en stridende etter prinsippene for jus in bello.[215] Som regel vil slike beslutninger baseres på retningslinjer gitt i forkant.[216]

Selve sporingen av angrepet tilbake til opprinnelsespunktet blir ofte utført ved bruk av automatiske sporingsprogrammer, og er relativt uproblematisk folkerettslig sett.[217] Samtidig er det viktig at denne prosessen ikke er helautomatisert ettersom det ikke er gitt at enheten angrepet spores tilbake til er enheten angrepet opprinnelig ble igangsatt fra, eller at eieren er den ansvarlige aktøren for angrepet.

Mer problematisk er staters eventuelle bruk av programvarer som responderer automatisk med aktive selvforsvarsresponser ved digitale angrep.

Snowden avslørte i et intervju med WIRED at NSA har utviklet en datamaskin som analyserer mengder av metadata, oppdager, sporer opp og responderer på digitale angrep automatisk. Dersom dette stemmer medfører dette en rekke folkerettslige implikasjoner. For det første medfører det økt risiko for at feil aktør holdes ansvarlig for et digitalt angrep, og for det andre medfører det fare for utilsiktet skade og skade på nøytrale tredjeland i strid med både jus ad bellum og jus in bello. Disse folkerettsbruddene kan igjen føre til økte politiske spenninger og konflikteskalering.[218]

Den konkrete vurderingen av selvforsvarsresponsers legitimitet etter kriteriene under jus ad bellum og jus in bello, krever per i dag stor grad av skjønnsutøvelse, det vil si menneskelig vurdering og analyse. Dette tilsier etter mitt syn at helautomatiserte prosesser for oppdagelse, analysering og respondering på digitale angrep ikke er i samsvar med folkeretten, og at

---

213 Graham (2010) s. 97.
214 Kesan (2012) s. 525.
215 Graham (2010) s. 97.
216 Sklerov (2012) s. 70 fotnote 33.
217 Graham (2010) s. 97.
218 WIRED (2014).

menneskelig skjønnsutøvelse i det minste må komme inn som et tillegg til de automatiserte prosessene.[219]

Når det gjelder hvem som spesifikt skal avgjøre om kriteriene for selvforsvarsutøvelse er oppfylt og hva det nærmere skal bestå i, er det etter min mening klart at en sivil systemadministrator ikke kan beslutte iverksettelsen av aktive digitale motangrep da dette vil stride imot distinksjonsprinsippet etter jus in bello. Systemadministrator må således være av militær rang. Mange land har også inkorporert cyberforsvar i deres respektive militære enheter.[220] Det er imidlertid ingenting i veien for at sivile systemadministratorer varsler om og koordinerer alvorlige dataangrep. En rekke stater har for eksempel opprettet såkalte CERT (Computer Emergency Response Team), som består av sivile eksperter på området. I Norge ledes NorCERT av Nasjonal sikkerhetsmyndighet (NSM). NSM er et sivilt direktorat underlagt Forsvarsdepartementet som rapporterer både til sivil og militær sektor.[221] Det er heller ingenting i veien for iverksettelse av andre sivil-militære samarbeidsprosjekter som for eksempel den nevnte mellom Telenor og Cyberforsvaret (punkt 3.2), så lenge de folkerettslige avgjørelsene tas av en aktør med militær rang.

Uansett er det verdt å påpeke at de folkerettslige vurderingene rundt bruken av aktive selvforsvarsresponser er krevende grunnet hastigheten til dataangrep. I tillegg er tilgjengelig informasjon ofte svært spekulativ.[222] Avgjørelsene er også skjønnsmessige, og fulle av politiske vurderinger.[223]

Jeg mener derfor at det foreligger en reell fare for feilvurderinger og konflikteskalering mellom stater dersom systemadministratorer av lavere militær rang gis for vide fullmakter på dette punktet. For å unngå dette bør aktører med høyere militær rang de lege ferenda være beslutningstakere når det gjelder avgjørelser om å benytte aktive digitale motangrep etter mitt syn. Som Graham påpeker bør avgjørelsene tas av noen som forstår den fulle politiske og rettslige risikoen av å benytte dette.[224] Selv om det ikke er direkte folkerettslig relevant taler demokratihensyn samt hensynet til offentlig kontroll etter min mening for at folkevalgte for

---

219 Melzer (2011) s. 18.
220 Kondoch (2013) s. 460.
221 Nasjonal sikkerhetsmyndighet (2014)
222 Sklerov (2012) s. 70.
223 Graham (2010) s. 97-98.
224 Graham (2010) s. 97-98, 101. Kesan (2012) s. 525-526.

eksempel representert ved en stats forsvarsminister, til en viss grad også deltar i beslutningsprosessen.

3.9 Kollektivt selvforsvar

Retten til kollektivt selvforsvar er eksplisitt nevnt i FN-pakten artikkel 51, og utgjør folkerettslig sedvanerett.[225] For at retten skal inntre må en stat være utsatt for et «væpnet angrep», staten må erklære at den har blitt utsatt for et slikt angrep og det må foreligge en forespørsel om assistanse fra denne staten overfor andre stater. Selvforsvaret må utføres innenfor rammene av den andre statens forespørsel og samtykke.[226] Begrensningene for utøvelse av individuelt selvforsvar som for eksempel nødvendighet og proporsjonalitet, gjelder også ved utøvelse av kollektivt selvforsvar.[227]

Tallinn-manualen påpeker at retten til kollektivt selvforsvar etter artikkel 51 også kan benyttes ved digitale angrep. De nevnte begrensningene for utøvelse av selvforsvaret får også anvendelse ved kollektivt selvforsvar mot digitale angrep. Manualen nevner som eksempel at den rammede staten kan begrense forespørselen om assistanse til utøvelse av digitale fremfor fysiske responser, og for eksempel begrense målet for den digitale selvforsvarsresponsen.[228]

Artikkel 51 i FN-pakten er ansett som rettslig grunnlag for regionale forsvarsallianser. NATO-pakten artikkel 5 henviser uttrykkelig til artikkel 51, og stadfester at et angrep mot ett av medlemsstatene skal regnes som et angrep mot alle.[229] NATO har de siste årene hatt økt fokus på digitale trusler, og var for eksempel en av de første internasjonale aktørene som erklærte en digital selvforsvarspolicy som et svar på de digitale angrepene mot Estland i 2007.[230] Forsvar mot digitale angrep er per i dag en del av NATOs kjerneområder, og alliansen har bekreftet at folkeretten også får anvendelse i det digitale rom.[231] NATOs generalsekretær uttalte i et intervju med Der Spiegel at et digitalt angrep mot en av medlemsstatene kan bli ansett som et «væpnet angrep» som utløser retten til kollektivt

[225] ICJ, Nicaragua-saken (1986) avsnitt 176, 193. Gray (2018) s. 618.
[226] ICJ, Nicaragua-saken (1986) avsnitt 195, 199.
[227] ICJ, Nicaragua-saken (1986) avsnitt 176.
[228] Tallinn Manual 2.0 (2017) s. 354, 355 avsnitt 3.
[229] Ruud (2011) s. 196.
[230] Hadji-Janev (2016) s. 46.
[231] NATO (2018a).

selvforsvar etter NATO-pakten art. 5.[232] Foreløpig har ikke dette skjedd, men NATO har fordømt flere digitale angrep og forsøk på dette som Russland angivelig skal ha stått bak, for eksempel forsøket på å gjennomføre et digitalt angrep mot organisasjonen OPCW i Nederland i april i år.[233] NATO-landene har også blitt enige om å opprette et nytt digitalt operasjonssenter i 2018 for å styrke NATO's kommandostruktur, og NATO har fått tillatelse fra medlemsstatene til å benytte nasjonale cyberressurser for gjennomføring av oppdrag og operasjoner.[234]

EU har også de senere årene hatt fokus på digitale trusler, og lanserte i 2013 en cyberstratgi.[235] I 2016 kom et direktiv om sikring av nettverk og informasjonssystemer (NIS-direktivet). Dette direktivet representerte EUs første lovgivning på cybersikkerhetsområdet. Samarbeid mellom medlemsstatene er en viktig del av direktivet. For eksempel ble det opprettet en samarbeidsgruppe for å støtte og forenkle strategisk samarbeid og informasjonsutveklsing mellom medlemsstatene. Medlemstatene er pålagt å implementere direktivet innen 9. mai 2018, samt å utpeke operatører for essensielle digitalrelaterte tjenester innen 9. november i år.[236]

Selv om EU-samarbeidet i seg selv ikke utgjør en forsvarsallianse slik som NATO, er det en generell tendens til digital opprustning i takt med flere digitale angrep rettet mot europeiske stater, og en kollektiv tilnærming til dette. Den nevnte Paris-erklæringen er et eksempel på dette. Både NATO og EU rapporterer om at de digitale angrepene og effekten av disse tiltar både i mengde og styrke, og peker på en eskalering i så måte.[237] Flere stater anser digitale angrep som en overhengende trussel, og flere innser at samarbeid er et essensielt virkemiddel for avskrekking og bekjempelse av digitale angrep. Den norske regjering la for eksempel frem en internasjonal cyberstrategi for Norge i fjor, hvor internasjonalt samarbeid var en viktig del.[238] Også USA anerkjenner viktigheten av slikt samarbeid.[239]

---

232 Der Spiegel (2016).
233 NATO (2018b).
234 NATO (2018a).
235 EU-kommisjonen (2013).
236 EU-kommisjonen (2018).
237 Fortalen til Dir 2016/1148 EU. NATO (2018a).
238 Utenriksdepartementet (2017).
239 US Department of Defense (2018).

Hadji-Janev og Bogdanoski mener at en måte å redusere den digitale trusselen på er å benytte såkalt «swarming-based» digitalt selvforsvar innenfor rammene av kollektivt selvforsvar. Dette innebærer sentralisert planlegging, men desentralisert utøvelse av selvforsvaret. Etter deres oppfatning vil NATO være en perfekt organisasjon for å utprøvelse av en slik teknikk med dets kollektive sikkerhets- og forsvarssystemer.[240]

Hadji-Janev og Bogdanoski mener NATO mest sannsynlig bare vil respondere med kollektivt selvforsvar ved angrep som har konsekvenser som kan sammenlignes med fysiske angrep, slik som tap av liv og fysiske skader. Årsaken er medlemslandenes ulike syn på terskelen for hva som utgjør et «væpnet angrep».[241]

Etter mitt syn viser både den folkerettslige, men også den politiske utviklingen på dette området en sterk tendens til harmonisering av regelverk, økt samarbeid og digital opprustning internasjonalt. Dette innebærer at staters ulike oppfatninger av hva som utgjør et «væpnet angrep» etter hvert vil bli mindre. NATOs økte fokus på digitale angrep som en trussel mot forsvarsalliansen samt dets offisielle uttalelser i så måte, tilsier derfor etter mitt syn at man ikke skal se bort fra en kollektiv selvforsvarsrespons på et digitalt angrep mot et medlemssland i fremtiden.

3.10 Samlede betraktninger

Kapittel 3 har analysert grensene for en stats selvforsvarsutøvelse ved digitale angrep fra andre stater etter FN-pakten artikkel 51 og folkerettslig sedvanerett, når det er på det rene at selvforsvarsretten først er inntrådt (kapittel 2).

Selv om folkeretten er tilpasset konvensjonell og ikke digital krigføring, viser dette kapittelet at de tradisjonelle reglene også får anvendelse på selvforsvar mot digitale angrep. På grunn av særegenhetene tilknyttet digitale angrep, må imidlertid de enkelte begrensningene som følger av den alminnelige folkeretten på enkelte punkter anvendes med en viss fleksibilitet. Dette gjelder for eksempel kravet til umiddelbarhet (punkt 3.5).

---

240 Hadji-Janev (2016) s. 39, 44, 45.

241 Hadji-Janev (2016) s. 50.

På den annen side kan ikke alle de tradisjonelle folkerettslige begrensningene anvendes med fleksibilitet. For eksempel innebærer Tallinn-manualens kriterier i form av standarden for «the last window of opportunity» en videre adgang til selvforsvar ved digitale angrep enn tidligere anerkjent i folkeretten (punkt 3.4.2). Flere teoretikere kritiserer manualens standard for å være for vid ved at den åpner for forkjøpsangrep. Jeg er enig og mener brudd på nødvendighets - samt proporsjonalitetskriteriet kan unngås ved en strengere tidsmessig begrensning i forkant av et digitalt angrep. Om denne standarden faktisk er et uttrykk for gjeldende rett, er usikkert.

Et annet eksempel er at Tallinn-manualen hevder at fysiske motangrep mot digitale angrep er i samsvar med proporsjonalitetskravet etter jus ad bellum (punkt 3.7). Dette stemmer forsåvidt med anerkjent generell folkerettslig teori. Ifølge ICJ må imidlertid kravene etter både jus ad bellum og jus in bello være tilfredsstilt for at en selvforsvarsaksjon skal bedømmes som lovlig. Fysiske selvforsvarsresponser mot digitale angrep som innebærer omfattende sivile skader og/eller tap av liv, vil mest sannsynlig stride imot kravene til jus in bello, og dermed gjøre selvforsvarsresponsen ulovlig etter folkeretten.

Et tredje eksempel er såkalte automatiske sporings- og responssystemer der det blir respondert automatisk med aktive digitale motangrep ved digitale angrep. Flere av kriteriene etter jus ad bellum og jus in bello beror på skjønn. Dette tilsier etter mitt syn at helautomatiserte prosesser for oppdagelse, analysering og respondering på digitale angrep ikke er i samsvar med folkeretten, og at de tradisjonelle folkerettslige begrensningene for selvforsvarsutøvelse heller ikke på dette punktet kan anvendes med fleksibilitet. Hvor utbredt bruken av slike systemer er i praksis er imidlertid usikkert.

4 Digitale operasjoner analysert i lys av selvforsvarsretten

4.1 Estland: De digitale operasjonene mot Estland 2007

I 2007 ble Estland rammet av et omfattende distribuert tjenestenektangrep (DDoS-angrep) der nærmere 80 000 datamaskiner fra 170 land ble brukt for på samme tid å oversvømme estlandske datasystemer med datanettverkstrafikk.[242] Aksjonen ble igangsatt gjennom oppfordringer på nettet og styrt derfra.[243] Dette medførte at myndighetenes samt bankvesenets kritiske elektroniske systemer opplevde nettverksbrudd for en periode på nesten tre uker.[244] Angrepet resulterte ikke i omfattende fysiske skader.[245] Hvem som egentlig stod bak angrepene er uklart. Russland ble anklaget for å stå bak i starten, men Dinniss påpeker at angrepene av flere er ansett å kunne spores tilbake til uavhengige patriotiske hackere.[246]

Hayward sammenligner et DDoS-angrep med en konvensjonell bombe; selv om man ved et slikt angrep utnytter en del av den unike sårbarheten til det spesifikke målet, er den generelle metoden mulig å anvende på nytt. Han påstår imidlertid at DDoS-angrep mest sannsynlig aldri vil anses å utgjøre et «væpnet angrep» etter artikkel 51 på grunn av arten av DDoS-angreps konsekvenser. Det hersker ifølge ham en generell konsensus om dette i den fremherskende teorien på området.[247]

Han karakteriserer likevel de digitale operasjonene mot Estland i 2007 som et av de mest velkjente tilfellene av det som mest sannsynlig vil bli «a long line of cyber warfare operations».[248] Rettslig sett er imidlertid det fremherskende synet at operasjonene mot Estland ikke kan karakteriseres som et «væpnet angrep» jf. art. 51. Årsaken er mangelen på betydelige og langvarige skadelige konsekvenser, samt at ingen fysisk, væpnet makt ble brukt.[249] Ingen internasjonal digital hendelse har ifølge Hayward så langt blitt karakterisert

---

242 Tsagourias (2017) s 36. Hayward (2017) s. 423.
243 Hayward (2017) s. 423.
244 Hayward (2017) s. 412. Tsagourias (2017) s 29.
245 Hayward (2017) s. 412.
246 Kondoch (2013) s. 461. Dinniss (2012) s. 105.
247 Hayward (2017) s. 412.
248 Hayward (2017) s. 400.
249 Hayward (2017) s. 411. Tsagourias (2017) s 29.

som et «væpnet angrep» av stater. Dette inkluderer både operasjonene mot Estland i 2007, Iran i 2010 samt USA i 2016 som omtales under.[250]

Når det gjelder operasjonene mot Estland påstår Hayward at både Estland og dets allierte hadde sterke politiske grunner for ikke å anerkjenne disse som væpnede angrep. En slik anerkjennelse ville ifølge ham kunne utløse NATO-pakten art. 5 om kollektivt selvforsvar. Dette ville igjen kunne ha ført til en eskalering mellom NATO og Russland. Han påstår at estlandske myndigheter kan ha ment at en slik eskalering ville være uforholdsmessig i forhold til konsekvensene de digitale operasjonene medførte.[251]

4.2 Iran: Stuxnet-operasjonen, 2010

Mellom juni 2009 og mai 2010 rammet en skadelig programvare kalt Stuxnet datasystemene til fem fasiliteter i Iran, herunder et kjernekraftverk i Natanz.[252] Programvaren rammet såkalte SCADA-systemer (Supervisory Control and Data Acquisition systems); en type industrielle kontrollsystemer som bruker en spesifikk programvare for å håndtere storskala industrisystemer.[253] Stuxnet endret koden til disse systemene for deretter å forandre sentrifugene i kjernekraftverkets fysiske operasjoner. Sentrifugenes motorer ble manipulert til med jevne mellomrom å øke eller senke hastigheten uten at dette ble oppdaget av operatørene som håndterte de aktuelle kontrollenhetene på kraftverket.[254]

Ekspertene bak Tallinn-manualen er delte i spørsmålet om hendelsen utgjorde et «væpnet angrep» eller ikke. Uenigheten består nærmere i om operasjonens alvorlighetsgrad jf. «the scale and effects»-kriteriet, medførte at denne utgjorde et «væpnet angrep». Noen av ekspertene mener at den digitale operasjonen utgjorde et «væpnet angrep» med tanke på de omfattende skadene operasjonen påførte de iranske sentrifugene. Andre eksperter mener at dette ikke utgjorde et «væpnet angrep». Samtlige er enige om at det uansett var tale om ulovlig maktbruk i strid med FN-pakten art. 2(4).[255] Det synes som om manualen legger til grunn at skadene påført sentrifugene faktisk skyldtes Stuxnet-operasjonen.

---

250 Hayward (2017) s. 410-411.
251 Hayward (2017) s. 411.
252 Ziolkowski (2012) s. 3.
253 Ziolkowski (2012) s. 3.
254 Ziolkowski (2012) s. 3-4.
255 Tallinn Manual 2.0 (2017) s. 342 avsnitt 10.

På grunn av mangelen på detaljert og pålitelig informasjon når det gjelder Stuxnets opphav og mulige påførte skader utenfor selve SCADA-systemene, er det ifølge Ziolkowski krevende å drøfte dette rettslig sett. Hun påstår at de rettslige analysene rundt hendelsen må utføres på grunnlag av antakelser, og at de kun vil berøre folkerettslige implikasjoner.[256]

Ziolkowski fremhever at man ikke har klare bevis på hvem som stod bak Stuxnet-operasjonen. Selv om mange aktører kan ha en interesse i å ramme Irans atomvåpenprogram, påpeker hun at dette ikke i seg selv utgjør tilstrekkelige rettslige bevis for å kunne plassere ansvaret for operasjonen.[257]

Hun mener det også er uklart om sentrifugene faktisk ble ødelagt av Stuxnet ettersom iranske myndigheter aldri har bekreftet dette. Videre påpeker hun at selv om rapporter viser at svært mange sentrifuger ble erstattet, utgjør ikke dette et rettslig bevis på at utbyttingen skyldtes Stuxnet. Iranske myndigheter har ifølge rapporter hatt en rekke tekniske problemer med sine sentrifuger særlig grunnet bruk av en gammel sentrifugemodell, og Ziolkowski påpeker at utbyttingen like gjerne kan skyldes dette.[258]

Når det gjelder målet for operasjonen mener hun altså at det ikke foreligger tilstrekkelige bevis på at objektet som ble rammet av Stuxnet også omfattet sentrifugene, og ikke kun SCADA-systemene. Dette har betydning for om angrepet kan klassifiseres som et «væpnet angrep». Gitt at det kun var SCADA-systemene som faktisk ble ødelagt av Stuxnet, kan målet for operasjonen tilsi at det ikke er tale om et «væpnet angrep». Det samme kan sies om konsekvensene av operasjonen, jf. «the scale and effect»-kriteriet; dersom kun SCADA-systemene ble rammet av Stuxnet tilsier det at konsekvensene av operasjonen var langt mindre omfattende enn dersom skaden på sentrifugene også skyldtes Stuxnet. Operasjonens alvorlighetsgrad blir altså betraktelig redusert dersom utbyttingen av sentrifugene ikke skyldes Stuxnet.

Forutsatt at sentrifugene faktisk ble ødelagt som følge av den digitale operasjonen, er det uklart om angripers intensjon var å ramme sentrifugene eller kun SCADA-systemene. Dersom

---

256 Ziolkowski (2012) s. 4, 6.
257 Ziolkowski (2012) s. 5.
258 Ziolkowski (2012) s. 5.

intensjonen kun var å ramme SCADA-systemene, blir spørsmålet om de utilsiktede skadene på sentrifugene gjør at operasjonen kan regnes som et «væpnet angrep» som beskrevet i punkt 2.2.5. ICJs vurdering av intensjonens betydning i Oljeplattformsaken (2003) tilsier at de utilsiktede skadene på sentrifugene i så fall ikke gjør den digitale operasjonen til et «væpnet angrep».[259] Flertallet av ekspertene bak Tallinn-manualen ville derimot ikke ha gitt angripers intensjon noen relevans i så måte.[260] Jeg er som nevnt enig med flertallet bak manualen på dette punktet.

Tsagourias legger i motsetning til Ziolkowski til grunn at de iranske sentrifugene ble ødelagt og byttet ut på grunn av Stuxnet-angrepet. Han påpeker at i løpet av tiden Stuxnet var virksom ble nærmere 1000 sentrifuger erstattet ifølge en rapport utført av IAEA (International Atomic Energy Association). [261] Dersom man anser alvorlighetsgraden for å være det avgjørende for om en digital operasjon utgjør et «væpnet angrep», vil det ifølge ham være vanskelig å fastslå hvor ødeleggelsen av disse 1000 sentrifugene skal plasseres på en slik skala. Han påpeker at andre konsekvenser også bør tas i betraktning; for eksempel at operasjonen forsinket Irans atomvåpenprogram med fire år.[262]

4.3 USA: Russisk innblanding i det amerikanske presidentvalget 2016

22. juli 2016 publiserte WikiLeaks mer enn 18 000 e-poster fra Det demokratiske partis nasjonale komité (DNC). E-postene viste at DNC som formelt skulle være objektive, egentlig støttet Hillary Clintons kampanje fremfor Bernie Sanders´. I oktober samme år ble tusenvis av e-poster fra og til Clintons kampanjeleder i tillegg publisert nærmest på daglig basis. Dette medførte en omfattende mediedekning både nasjonalt og internasjonalt der spenninger innen Clinton-kampanjen stod sentralt; blant annet ble det hevdet av flere på innsiden av kampanjen mente Clinton var en mindre sterk kandidat. Kun to dager før presidentvalget ble ytterligere en rekke e-poster fra DNC publisert.[263] Hillary Clinton tapte presidentvalget.

---

[259] ICJ, Oljeplattform-saken (2003) avsnitt 64.

[260] Tallinn Manual 2.0 (2017) s. 343-344 avsnitt 14.

[261] Tsagourias (2017) s 29.

[262] Tsagourias (2017) s 33.

[263] Banks (2017) s. 1487.

Det viste seg etterhvert at Russland stod bak hackerangrepet.[264] Spørsmålet er om Russlands innblanding i det amerikanske presidentvalget, kan anses som et «væpnet angrep», jf. FN-pakten artikkel 51, eller som ulovlig bruk av makt, jf. artikkel 2 (4).

Banks hevder at Russlands hacking av DNC verken utgjorde et «væpnet angrep» eller ulovlig maktbruk. Han går ikke nærmere inn på begrunnelsen for dette, men viser til Tallinn-manualens redegjørelse av kriteriene for dette.[265]

Når det gjelder spørsmålet om hackingen utgjorde ulovlig bruk av makt, jf. art. 2 (4), følger det av forarbeidene til FN-pakten at ulovlig maktbruk etter art. 2 (4) ikke inkluderer økonomisk eller politisk press som truer den territorielle integriteten eller politiske selvstendigheten til en stat.[266] Etterfølgende erklæringer bekrefter også at art. 2(4) kun refererer til væpnet makt («armed force»), og at andre former for tvang omfattes av ikke-intervensjonsprinsippet (punkt 1.3.1).[267] Tallinn-manualen fastslår på bakgrunn av dette at digitale operasjoner som kun er rettet mot å undergrave tilliten til en stats myndigheter, ikke utgjør ulovlig maktbruk.[268] Formålet med hackingen syntes nettopp å være undergravelse av tilliten til Hillary Clinton som presidentkandidat. Dette tilsier at hackingen ikke stred imot maktforbudet.

Dersom man likevel legger til grunn at hackingen utgjorde ulovlig maktbruk, kan man spørre om hackingen dermed også utgjorde et «væpnet angrep» etter art. 51. Det er på det rene at Russland stod bak operasjonene. Kravene til både statsansvar og et grenseoverskridende element er dermed oppfylt. Etter «scale and effect»-kriteriet (punkt 2.3.2), herunder en instrumentbasert tilnærming, er det imidlertid klart at inngrepet ikke utgjorde et «væpnet angrep»; hackingen medførte ingen fysiske skader. Heller ikke etter en effektbasert tilnærming kan hackingen sies å utgjøre et «væpnet angrep». Den resulterte ikke i omfattende skader på USAs nasjonale infrastruktur, og det er uansett vanskelig å påvise en direkte årsakssammenheng mellom hackingen og Clintons tap av valgkampen. Etter en objektiv ansvarstilnærming kunne imidlertid enkelte ha argumentert for at hackingen representerte en innblanding i det amerikanske valget som utgjorde et «væpnet angrep» på landets «politiske

---

264 Banks (2017) s. 1489.

265 Banks (2017) s. 1500.

266 United Nations (1945) s. 559, 720-721.

267 Generalforsamlingsresolusjon 2625 (1970), 42/22 (1987). Roscini (2010) s. 105-106.

268 Tallinn Manual 2.0 (2017) s. 331 avsnitt 3.

infrastruktur». Den objektive ansvarstilnærmingen er kontroversiell, og en slik konklusjon er uansett klart uholdbar.[269]

Ettersom hackingen verken kan sies å stride mot maktforbudet etter art. 2 (4) eller utgjøre et «væpnet angrep» etter art. 51, blir spørsmålet om hackingen stred mot ikke-intervensjonsprinsippet (punkt 1.3.1).

Banks er av den oppfatning at den russiske hackingen ikke utgjorde en ulovlig intervensjon. Årsaken er mangelen på et tvangselement.[270] Han viser til Tallinn-manualen hvor tvangsbegrepet blir ansett å omfatte både fysisk tvang, men også handlinger som skal frarøve andre staters valgfrihet, eller tvinge dem til å handle eller avstå fra å handle på en ufrivillig måte.[271] Tallinn-manualen påpeker at det å endre elektroniske stemmesedler for å manipulere valgresultater utgjør en ulovlig intervensjon.[272] Brian Egan, Department of State Legal Adviser, har ifølge Banks også hevdet at en digital operasjon som påvirker en annen stats mulighet til å holde valg eller som manipulerer dennes valgresultater, innebærer et klart brudd på ikke-intervensjonsprinsippet.[273]

Ettersom russerne verken manipulerte stemmemaskinene eller forandret på stemmesedlene mener Banks at den russiske hackingen ikke utgjorde en ulovlig intervensjon. Det eneste russerne gjorde var ifølge ham å innhente og spre privat informasjon. Dette er ikke å anse som tvang etter hans syn.[274]

På den andre siden fremhever Banks at sedvaneretten er basert på tradisjonelle væpnede konflikter. Det er derfor ikke sikkert at disse kriteriene kan anvendes analogisk på digitale operasjoner. Den russiske hackingen synes mer tvangsmessig ifølge ham dersom man ser det slik at russerne effektivt «weaponized the information» for å svekke tilliten til det amerikanske demokratiske systemet.[275]

---

[269] Sklerov (2012) s. 59. Faga (2017) s. 14-15.
[270] Banks (2017) s. 1500.
[271] Banks (2017) s. 1501. Tallinn Manual 2.0 (2017) s. 317 avsnitt 18.
[272] Tallinn Manual 2.0 (2017) s. 313 avsnitt 2.
[273] Banks (2017) s. 1500.
[274] Banks (2017) s. 1501.
[275] Banks (2017) s. 1501.

Det er som nevnt vanskelig å påvise en direkte årsakssammenheng mellom publiseringen av e-postene, og det faktum at Clinton tapte valget. Dette har imidlertid etter mitt syn ikke nevneverdig betydning ettersom enhver innblanding i det politiske systemet til en annen stat, anses å være i strid med intervensjonsforbudet jf. Declaration on Friendly Relations (1970). Etter min oppfatning legger Banks for mye vekt på det manglende tvangselementet i saken, og jeg mener man uansett som han selv skriver kan argumentere for at russerne «weaponized the information».[276] Selv om publiseringen ikke nødvendigvis medførte at presidentvalget direkte ble tvunget i en viss retning, kan man argumentere for at e-postene ble brukt som et slags informasjonsvåpen for å mobilisere velgerne til å stemme på Clintons motkandidat. Dette tilsier at Russland i det minste indirekte forsøkte å påvirke det amerikanske valget i strid med intervensjonsforbudet. Hensynet til å unngå både direkte og indireke intervensjon i en annen stats politiske systemer, tilsier også at hackingen etter mitt syn bør bedømmes for å stride mot intervensjonsforbudet de lege ferenda. Begrunnelsen er å motvirke at andre stater på tilsvarende måte omgår folkerettens begrensninger ved å ty til indirekte og kreative løsninger for å blande seg inn i andre staters politiske systemer.

Banks mener imidlertid at Russlands hacking kan anses som et brudd på suverenitetsprinsippet. Tallinn-manualen fastslår at suverenitetsprinsippet også får anvendelse på utførelsen av digitale operasjoner mot en stats vilje rettet mot denne statens digitale infrastruktur.[277] Imidlertid mener han at USAs milde reaksjoner på hackingen tilsier at staten heller anså dette som et tilfelle av spionasje som ikke reguleres av folkeretten.[278] Jeg mener at Russlands hacking i det minste må anses som et brudd på suverenitetsprinsippet dersom det ikke kan anses som et brudd på intervensjonsforbudet.

[276] Banks (2017) s. 1501. Generalforsamlingsresolusjon 2625 (1970).

[277] Tallinn Manual 2.0 (2017) s. 11 avsnitt 1. Banks (2017) s. 1512.

[278] Banks (2017) s. 1512.

5 Avsluttende bemerkninger

Problemstillingen oppgaven har behandlet er grensene for en stats selvforsvarsrett ved digitale angrep fra en annen stat etter FN-pakten artikkel 51 og folkerettslig sedvanerett. Den har vist at selv om de folkerettslige reglene på området er tilpasset konvensjonell og ikke digital krigføring, får de folkerettslige reglene i stor grad også anvendelse på digitale angrep. Tallinn-manualen spiller i den forbindelse en betydelig rolle ved at den har forenklet anvendelsen av de folkerettslige reglene på det digitale området. Imidlertid utgjør ikke alle reglene Tallinn-manualen oppstiller gjeldende rett de lege lata (se for eksempel punkt 3.4.2 om standarden for «the last window of opportunity»).

Det eksisterer også særlige rettslige utfordringer når det gjelder digitale angrep som Tallinn-manualen heller ikke løser. Som påpekt i kapittel 2 finnes det for eksempel ingen folkerettslig regel med tanke på beviskravet for etablering av statsansvar for digitale operasjoner, og det foreligger på dette punktet svært delte meninger i teorien (punkt 2.2.2). Et annet omstridt spørsmål er som nevnt om digitale operasjoner utført av ikke-statlige aktører uten statlig innblanding, kan utløse selvforsvarsretten (punkt 2.2.3). Digitale operasjoner er også vanskeligere å klassifisere som væpnede angrep enn fysiske operasjoner, og selv om Tallinn-manualen benytter det generelle «scale and effect»-kriteriet, er det nærmere innholdet i dette kriteriet preget av ulike teoretiske tilnærminger (punkt 2.3.2).

Den mest aktuelle formen for selvforsvar ved digitale angrep foruten passive selvforsvarsmetoder som brannmurer, varslingssystemer og lignende, er aktive digitale motangrep. Det er imidlertid omdiskutert hvor grensene for slik selvforsvarsutøvelse går (se punkt 3.2, 3.6 og 3.7). Aktive digitale selvforsvarsresponser medfører fare for skade på uskyldige datasystemer som igjen kan innebære brudd på jus in bello, og dermed gjøre selvforsvarsresponsen ulovlig etter folkeretten på tross av at denne er i samsvar med jus ad bellum (punkt 3.7).

Oppgaven har analysert tre hendelser der digitale operasjoner ble igangsatt mot tre forskjellige stater; operasjonene mot Estland i 2007, Iran i 2010 og USA i 2016. Som nevnt innledningsvis har ingen stater (muligens med unntak av Nederland) så langt offisielt karakterisert en digital operasjon som et «væpnet angrep» etter art. 51 (punkt 1.1). Sklerov mener dette skyldes de folkerettslige uklarhetene som hersker rundt selvforsvarsretten ved

digitale angrep. Stater er etter hans syn tilbakeholdne med å karakterisere digitale operasjoner som væpnede angrep og igangsette selvforsvarsresponser, av frykt for selv å bryte folkeretten.[279] En annen årsak kan være at stater ønsker å igangsette lignende operasjoner selv, og at en offentlig klassifisering av digitale operasjoner som væpnede angrep vil forhindre dem fra dette.[280] Utfordringen er som Graham påpeker å utvikle anvendelige prosedyrer som gir myndigheter mulighet til å handle raskt, men samtidig innenfor folkerettens grenser ved digitale angrep.[281] Enkelte teoretikere mener løsningen ligger i en regulering og standardisering av aktive selvforsvarsresponser for å gjøre aktivitetene mer transparente og for å bidra til at slike selvforsvarsmetoder blir utøvd i samsvar med folkeretten.[282]

Det er behov for en nærmere folkerettslig avklaring når det gjelder grensene for en stats selvforsvarsrett ved digitale angrep fra andre stater. Per i dag er det folkerettslig teori som dominerer rettskildebildet på dette området. Fra et rettskildemessig ståsted er dette mindre heldig med tanke på at juridisk teori i utgangspunktet bare utgjør en subsidiær rettskilde folkerettslig sett, jf. statuttene for ICJ art. 38 (1)(d). Utviklingen av sedvaneretten på området er imidlertid avhengig av at stater til en viss grad offentliggjør både deres rettslige vurderinger av digitale angrep som de selv rammes av, men også av deres egne selvforsvarsresponser i så måte. Utstrakt hemmelighold svekker utviklingen av sedvaneretten på området, og medfører betydelig rettslig usikkerhet. En rettslig avklaring gjennom traktatfesting, statspraksis og opinio juris kan etter mitt syn medvirke til mindre politiske spenninger samt konflikteskalering på det digitale området, og dermed også i internasjonale relasjoner generelt.

[279] Sklerov (2012) s. 46.
[280] Hayward (2017) s. 412-413.
[281] Graham (2010) s. 102.
[282] Hadji-Janev (2016) s. 55.

6 Kildeliste

Traktater og direktiver

FN-pakten	Charter of the United Nations, 26. juni 1945
NATO-pakten	North Atlantic Treaty, 4. april 1949
Genève-konvensjonene	Protocol additional to the Geneva Conventions of 12-08-1949, and relating to the protection of victims of international armed conflicts (Protocol I), 8. juni 1977
Europarådets konvensjon om datakriminalitet	Convention on Cybercrime ETS nr. 185, Budapest 23. november 2001
Dir 2016/1148 EU	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Resolusjoner og erklæringer

Generalforsamlingsresolusjon 2625 (1970)	Generalforsamlingsresolusjon. Resolution 2625 (1970) Adopted by the General Assembly 24 October 1970. Declaration on Principles of International Law

concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations. [http://www.un-documents.net/a25r2625.htm] [Sitert 16.11.2018]

Generalforsamlingsresolusjon 29/3314 (1974)

Generalforsamlingsresolusjon. Resolution adopted by the General Assembly 14 December 1974. 29/3314. Definition of Aggression [http://www.un-documents.net/a29r3314.htm] [Sitert 31.10.2018]

Generalforsamlingsresolusjon 42/22 (1987)

Generalforsamlingsresolusjon. Resolution 42/22 (1987). Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations. 18 November 1987. [http://www.un.org/documents/ga/res/42/a42r022.htm] [Sitert 01.11.2018]

Generalforsamlingsresolusjon 49/60 (1994)

Generalforsamlingsresolusjon. Resolution 49/60 (1994). Measures to Eliminate Terrorism. 9 December 1994. [http://www.un.org/documents/ga/res/49/a49r060.htm] [Sitert 16.11.2018]

Generalforsamlingsresolusjon 53/70 (1999)

Generalforsamlingsresolusjon. Resolution adopted by the General Assembly 4 January 1999. 53/70. Developments in the field of information and telecommunications in the context of international security. [http://undocs.org/A/RES/53/70] [Sitert 29.10.2018]

Generalforsamlingsresolusjon 54/49 (1999)

Generalforsamlingsresolusjon. Resolution adopted by the General Assembly 23 December 1999. 54/49. Developments in the field of information and telecommunications in the context of international security. [http://undocs.org/A/RES/54/49] [Sitert 29.10.2018]

Generalforsamlingsresolusjon 55/63 (2001)

Generalforsamlingsresolusjon. Resolution adopted by the General Assembly 22 January 2001. 55/63. Combating the criminal misuse of information technologies. [https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf] [Sitert 27.10.2018]

Generalforsamlingsresolusjon 56/83 (2002)

Generalforsamlingsresolusjon. Resolution adopted by the General Assembly 28 January 2002. 56/83. Responsibility of States for

internationally wrongful acts. [http://undocs.org/A/RES/56/83] [Sitert 18.09.2018]

Sikkerhetsrådsresolusjon 1368 (2001)

Sikkerhetsrådsresolusjon. Resolution 1368 (2001) Adopted by the Security Council at its 4370th meeting, on 12 September 2001. [https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement] [Sitert 12.11.2018]

Sikkerhetsrådsresolusjon 1373 (2001)

Sikkerhetsrådsresolusjon. Resolution 1373 (2001) Adopted by the Security Council at its 4385th meeting, on 28 September 2001. [https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement] [Sitert 12.11.2018]

Paris-erklæringen (2018)

Paris-erklæringen. Paris Call for Trust and Security in Cyberspace, 12. november 2018 https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf [Sitert 16.11.2018]

Rettspraksis

ICJ, Corfu Channel-saken

Corfic Channel case, Judgment of

(1949)	*April 9th, 1949: ICJ Reports 1949,* p. 4.
ICJ, Gisselsaken (1980)	*United States Diplomatic and Consular Staff in Tehran, Judgment, ICJ Reports 1980*, p. 3.
ICJ, Nicaragua-saken (1986)	*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment, ICJ Reports 1986*, p. 14.
ICJ, Atomvåpensaken (1996)	*Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, ICJ Reports 1996*, p. 226
ICTY, Tadić-saken (1999)	*Prosecutor v Tadić, ICTY, Judgment, Case No IT-94-1-A, Appeals Chamber, 15 July 1999*
ICJ, Oljeplattform-saken (2003)	*Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, ICJ Reports 2003*, p. 161
ICJ, Mursaken (2004)	*Legal Consequences cf the Construction of a Wa11 in the Occupied Palestinian Territory, Advisory Opinion, ICJ Reports 2004,* p. 136
ICJ, Democratic Republic of the Congo v. Uganda (2005)	*Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, ICJ Reports 2005,* p. 168

ICJ, Folkemordsaken (2007) — *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), Judgement, ICJ Reports 2007*, p. 43

Litteratur

Advisory Council on International Affairs No 77, AIV/No 22 (2011) — Advisory Council on International Affairs. Cyber Warfare, No 77, AIV/No 22, CAVV, desember 2011. [https://aiv-advies.nl/download/da5c7827-87f5-451a-a7fe-0aacb8d302c3.pdf] [Sitert 24.09.2018]

Aftenposten (2018) — Aftenposten. *Nederlandsk minister mener landet er i cyberkrig med Russland.* (2018), https://www.aftenposten.no/verden/i/BJ93L7/Nederlandsk-minister-mener-landet-er-i-cyberkrig-med-Russland [Sitert 25.10.2018]

Ago (1980) — Ago, Roberto. «Addendum to the eighth report on State responsibility», *Yearbook of the International Law Commission*, vol. II (1), (1980), s. 13-70

Banks (2017) — Banks, William. «State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0»,

Texas Law Review, volum 95, 1487 (2017), s. 1487-1513

Carlin (2016) — Carlin, John P. «Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats», *Harvard National Security Journal*, volum 7, 391 (2016), s. 391-436

Der Spiegel (2016) — Der Spiegel. *We Don't Want a New Cold War.* (2016), http://www.spiegel.de/international/world/interview-with-nato-secretary-general-jens-stoltenberg-a-1095799.html [Sitert 24.10.2018]

Dinniss (2012) — Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War,* 1. utg., New York: Cambridge University Press, 2012.

EU-kommisjonen (2013) — EU-kommisjonen. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* (2013) https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [Sitert 24.10.2018]

EU-kommisjonen (2018) — EU-kommisjonen. *The Directive on security of network and information systems (NIS Directive).* (2018), https://ec.europa.eu/digital-single-

market/en/network-and-information-security-nis-directive [Sitert 24.10.2018]

Faga (2017) — Faga, Hemen Philip. «The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century», *Baltic Journal of Law & Politics* vol. 10 (2017) s. 1–34

Flowers (2014) — Flowers, Angelyn, Sherali Zeadally. «US Policy on Active Cyber Defense», *Journal of Homeland Security and Emergency Management*, vol. 11, (2014) s. 289-308

Gardam (2004) — Gardam, Judith. *Necessity, Proportionality and the Use of Force by States,* 1. utg., New York: Cambridge University Press, 2004.

Graham (2010) — Graham, David E. «Cyber Threats and the Law of War», *Journal of National Security Law & Policy*, vol. 4, (2010), s. 87-102

Gray (2018) — Gray, Christine. «The Use of Force and the International Legal Order», i *International Law*, Malcolm D. Evans, 5. utg., New York: Oxford

University Press, 2018, s. 601-635

Hadji-Janev (2016) — Hadji-Janev, Metodi, Mitko Bogdanoski. «Swarming-based cyber defence under the framework of collective security», *Security Journal*, vol. 30 (2016), s. 39-59

Halberstam (1996) — Halberstam, Malvina. "The Right to Self-Defense Once the Security Council Takes Action," *Michigan Journal of International Law* vol. 17, no. 2 (1996) s. 229-248

Hayward (2017) — Hayward, Ryan J. «Evaluating the "Imminence" of a Cyber Attack for Purposes of Anticipatory Self-Defense", *Columbia Law Review*, vol. 117, no. 2 (2017), s. 399-434

Jennings (1938) — Jennings, R.Y. «The Caroline and McLeod Case», *American Journal of International Law*, volum 32, nr. 1, (1938), s. 82-100

Jensen (2002) — Jensen, Eric Talbot. «Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense», *Stanford Journal of International Law,* vol. 38 (2002), s. 207-240

Jensen (2017) — Jensen, Eric Talbot. «The Tallinn Manual 2.0: Highlights and

Insights». *48 Georgetown Journal of International Law 735*, BYU Law Research Paper No. 17-10 (2017), s. 735-778

Jørgenrud (2018) — Jørgenrud. *Paris-erklæring 50 land enige om å bekjempe datakrim. USA, Russland og Kina sa nei takk*. (2018), https://www.digi.no/artikler/50-land-enige-om-a-bekjempe-datakrim-usa-russland-og-kina-sa-nei-takk/451028 [Sitert 16.12.2018]

Kesan (2012) — Kesan, Jay P, Carol Mullins Hayes. «Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace», *Harvard Journal of Law and Technology*, vol. 25, no. 2, (2012), s. 429-543

Kommentar til ASR — Kommentar til ASR, «Materials on the Responsibility of States for Internationally Wrongful Acts", i *United Nations Legislative Series,* UN Doc. ST/LEG/SER B/25 (2012) [sitert 18.09.2018]

Kondoch (2013) — Kondoch, Boris. «Jus ad Bellum and Cyber Warfare in Northeast Asia», *Journal of East Asia & International Law*, vol. 6, no. 1 (2013), s. 459-478

Larsen (2014a) — Mujezinovic Larsen, Kjetil.

Internasjonal humanitærrett. (2014), https://snl.no/internasjonal_humanit%C3%A6rrett [Sitert 27.10.2018]

Larsen (2014b) — Mujezinovic Larsen, Kjetil. *Distinksjonsprinsippet.* (2014), https://snl.no/distinksjonsprinsippet [Sitert 27.10.2018]

Larsen (2015) — Mujezinovic Larsen, Kjetil. *Distinksjonsprinsippet.* (2015), https://snl.no/proporsjonalitetsprinsippet [Sitert 12.11.2018]

Melnitzky (2012) — Melnitzky, Alexander. "Defending America against Chinese Cyber Espionage through the Use of Active Defenses," *Cardozo Journal of International and Comparative Law*, vol. 20, no. 2 (2012), s. 537-570.

Melzer (2011) — Melzer, Nils. «Cyberwarfare and international law», *United Nations Institute for Disarmament Research*, 2011.

Moussa (2014) — Moussa, Jasmine «Nuclear weapons and the separation of jus ad bellum and jus in bello», i *Nuclear Weapons under International Law,* Gro Nystuen, Stuart Casey-Maslen, Annie

Golden Bersagel, Cambridge: Cambridge University Press, 2014, s. 59-88

Mudrinich (2012) — Mudrinich, Erik M. «Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem», *The Air Force Law Review*, vol. 68 (2012), s. 167-206

Nasjonal sikkerhetsmyndighet (2014) — Nasjonal sikkerhetsmyndighet. *Organisasjon.* (2014), https://nsm.stat.no/om-nsm/organisasjon/ [Sitert 24.11.2018]

Nasjonal sikkerhetsmyndighet (2017) — Nasjonal sikkerhetsmyndighet. (2017). *Nasjonalt tryggingsorgan — Årsrapport 2017. Ei borg vi kan forsvare*, 2017 [https://nsm.stat.no/globalassets/rapporter/arsrapporter/nsm-arsrapport-2017_web_enkeltsider.pdf] [Sitert 25.09.2018]

NATO (2001) — NATO. *Statement by the North Atlantic Council.* (2001), https://www.nato.int/docu/pr/2001/p01-124e.htm [Sitert 12.11.2018]

NATO (2018a) — NATO. *Cyber defence.* (2018), https://www.nato.int/cps/en/natohq/topics_78170.htm? [Sitert

24.10.2018]

NATO (2018b) NATO. *Statement by NATO Secretary General Jens Stoltenberg on Russian cyber attacks.* (2018), https://www.nato.int/cps/en/natohq/news_158911.htm?selectedLocale=en [Sitert 24.10.2018]

OAS (2001) OAS. *Meeting of Consultation of Ministers of Foreign Affairs.* (2001), http://www.oas.org/oaspage/crisis/rc.24e.htm [Sitert 12.11.2018]

Ohlin (2017) Ohlin, Jens David. «Did Russian Cyber Interference in the 2016 Election Violate International Law?», *Texas Law Review*, volum 95, 1579 (2017), s. 1579-1598

Pieters (2018) Pieters, Janene. (2018) «Deal With Cyber Attackers More Publicly: Ministry of Defense», *NLTimes.nl*, 13. november 2018 [https://nltimes.nl/2018/11/13/deal-cyber-attackers-publicly-ministry-defense]

Reuters (2018) Reuters. *West accuses 'pariah state' Russia of global hacking campaign*. (2018), https://www.reuters.com/article/us-britain-russia-cyber/west-accuses-pariah-state-russia-of-global-

hacking-campaign-idUSKCN1ME1HE [Sitert 25.10.2018]

Roberts (2018) — Roberts, Anthea og Sandesh Sivakumarani. «The Theory and Reality of the Sources of International Law», i *International Law*, Malcolm D. Evans, 5. utg., New York: Oxford University Press, 2018, s. 89-119

Roscini (2010) — Roscini, Marco. «World Wide Warfare - Jus ad Bellum and the Use of Cyber Force», *Max Planck Yearbook of United Nations Law*, vol. 14, (2010), s. 85-130

Rosenzewig (2014) — Rosenzewig, Paul. "International Law and Private Actor Active Cyber Defensive Measures," *Stanford Journal of International Law*, vol. 50, no. 1 (2014) s. 103-118.

Ruud (2011) — Ruud, Morten og Geir Ulfstein. *Innføring i folkerett,* 4. utg., Oslo: Universitetsforlaget, 2011.

Sandvik (2012) — Sandvik, Kristin Bergtora. «Towards a Militarization of Cyberspace?
Cyberwar as an Issue of International Law», *Peace Research Institute Oslo (PRIO)*

Paper, (2012), s. 1-58

Schmitt (1999) — Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", *Columbia Journal of Transnational Law*, vol. 37 (1998-1999) s. 885-937

Schmitt (2003) — Schmitt, Michael N. "Preemptive Strategies in International Law," *Michigan Journal of International Law* vol. 24, no. 2 (2003) s. 513-548

Schmitt (2017) — Schmitt, Michael N. «Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical *Vade Mecum», Harvard National Security Journal,* vol. 8, (2017) s. 239-282

Sklerov (2012) — Sklerov, Matthew J. «Responding to International Cyber Attacks as Acts of War», i *Inside Cyber Warfare,* Jeffrey Carr, 2. utg., USA: O´Reilly, 2012, s. 45-75

Tallinn Manual 2.0 (2017) — Schmitt, Michael N. og Liis Vihul.

Tallinn manual 2.0 on the international law applicable to cyber operations, 1. utg., Storbritannia: Cambridge University Press, 2017.

Telenor (udatert)

Telenor. *Digitale trusler krever mer enn dugnadsinnsats* (udatert), https://www.telenor.no/om/digital-sikkerhet/digitale-trusler-krever-mer-enn-dugnadsinnsats.jsp [Sitert 24.11.2018]

Tsagourias (2017)

Tsagourias, Nicholas. «The Law of Cyber Warfare: Restrictions, Opportunities and Loopholes», *Canadian Journal of Law and Technology,* vol. 15, no. 1 (2017) s. 27-40

United Nations (1945)

United Nations. (1945) *Documents of the United Nations Conference on International Organization*, vol. VI. [http://digitallibrary.un.org/record/1300969/files/UNIO-Volume-6-E-F.pdf?version=1] [Sitert 01.12.2018]

US Department of Defense (2018)

US Department of Defense. *Summary. Department of Defense. Cyber Strategy.* (2018) https://media.defense.gov/2018/Sep

/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [Sitert 24.10.2018]

Utenriksdepartementet (2017) — Utenriksdepartementet. (2017) *Internasjonal cyberstrategi for Norge 2017,* 27.09.2017. [https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategi_web.pdf] [Sitert 28.08.2018]

Wikipedia (2018) — Wikipedia. *Logic bomb.* (2018), https://en.wikipedia.org/wiki/Logic_bomb [Sitert 05.10.2018]

WIRED (2014) — WIRED. (2014) «Edward Snowden: The Untold Story» 22. august 2014 [https://www.wired.com/2014/08/edward-snowden/]

Wormdal (2018) — Wormdal, Bård. (2018) "Norge og USA hacker russiske datanettverk», *NRK,* 22. mars 2018

Ziolkowski (2012) — Ziolkowski, Katharina. «Stuxnet-Legal Considerations», *NATO Cooperative Cyber Defence Centre of Excellence*, (2012) s. 1-25