CENTER FOR MILITÆRE STUDIER
KØBENHAVNS UNIVERSITET

Folkeretten og modreaktioner i cyberspace

Anders Henriksen

Februar 2014

Denne rapport er en del af Center for Militære Studiers forskningsbaserede myndighedsbetjening for Forsvarsministeriet. Formålet med rapporten er at give en fyldestgørende redegørelse for de beføjelser, som folkeretten giver en stat som Danmark, når denne gøres til genstand for cyberangreb fra udlandet.

Center for Militære Studier er et forskningscenter på Institut for Statskundskab på Københavns Universitet. På centret forskes der i sikkerheds- og forsvarspolitik samt militær strategi, og centrets arbejde danner grundlag for forskningsbaseret myndighedsbetjening af Forsvarsministeriet og de politiske partier bag forsvarsforliget.

Denne rapport er et analysearbejde baseret på forskningsmæssig metode. Rapportens konklusioner kan således ikke tolkes som udtryk for holdninger hos den danske regering, det danske forsvar eller andre myndigheder.

Læs mere om centret og dets aktiviteter på: http://cms.polsci.ku.dk/.

Forfatter:
Lektor, ph.d., Anders Henriksen, Centre for International Law and Justice

ISBN: 978-87-7393-728-0

This report is a part of Centre for Military Studies' policy research service for the Ministry of Defence. Its purpose is to elaborate on the options available under international law for a state like Denmark when it is subjected to cyber-attacks from abroad.

Centre for Military Studies is a research-based centre located at the Department of Political Science at the University of Copenhagen. The centre performs research in connection with security and defence policies and military strategies and this research constitutes the foundation for the policy research services that the centre provides for the Ministry of Defence and the political parties to the Defence Agreement.

This report is an analysis based on research methodology. Its conclusions should therefore not be understood as the reflection of the views and opinions of the Danish Government, the Danish Defence or any other authority.

Read more about the centre and its activities at http://cms.polsci.ku.dk/.

Author:
Associate Professor, ph.d., Anders Henriksen, Centre for International Law and Justice

ISBN: 978-87-7393-728-0

Abstract

The report follows a 2012 report published by the Centre for Military Studies on "Cyberwar, international law and computer network operations" and the purpose of the report is to elaborate on the options available under international law for a state like Denmark when it is subjected to cyber-attacks from abroad. To that end, the report lists the various legal 'tools' that are of relevance when determining if – and when – a state is allowed to operate in other states, including on the networks of other states. It is not always possible to identify the perpetrators of harmful cyber activities and it may also not be clear what the purpose of a given cyber-attack is. A proper response system therefore requires that a state is able to respond in an effective and lawful manner to harmful activities in cyberspace without any knowledge of the identity of the perpetrator or motive of the activities. The report initially provides an overview of the general principles of state sovereignty from which the more elaborate regulation springs. Subsequent to that, the report lists the principles that govern the lawful exercise of self-defense in response to an armed attack as well as the principles regulating the resort to lawful countermeasures. As a supplement, the report also provides an overview of necessity as a circumstance that precludes the wrongfulness of an act otherwise in violation of international law. The report concludes that, in theory at least, a consistent application of the listed 'tools' provide a state like Denmark with the necessary authority to counter harmful cyber activities from abroad. In the final part, the report recommends that Denmark works to make all states fulfil their international obligations with regard to bringing a stop to harmful cyber activities that emanate from their territories, that the relevant Danish authorities create clear guidelines on how Denmark acts in those instances where it is the target of major cyber-attacks from abroad, and finally, that the Danish politicians consider the extent to which Denmark will accept the disruptions that flow from cyber-attacks before the relevant authorities will counter the attacks by starting to violate the sovereignty of other states.

Dansk resumé

Rapporten bygger videre på en rapport fra Center for Militære Studier fra 2012 om "Cyberkrig, folkeretten og computer network operations" og den redegør mere fyldestgørende for de beføjelser, som folkeretten giver en stat som Danmark, når denne gøres til genstand for cyberangreb fra udlandet. Rapporten opstiller de forskellige folkeretlige 'figurer', der er af betydning i forhold til at vurdere, om – og i givet fald hvornår – en stat må operere i andre stater, herunder på andre staters netværk, for at imødegå cyberangreb. Det er ikke altid klart, hvem der står bag konkrete skadevoldende aktiviteter i cyberspace og det er heller ikke altid muligt at vide, hvad formålet med de givne aktiviteter er. Et egnet beredskab forudsætter derfor, at en stat kan reagere effektivt og lovligt mod skadevoldende aktiviteter i cyberspace uden kendskab til bagmændenes identitet eller motiver. Rapporten gennemgår indledningsvis de almindelige folkeretlige principper om suverænitet, der danner baggrund for den mere detaljerede folkeretlige regulering på området. Dernæst uddybes de folkeretlige principper for henholdsvis udøvelse af selvforsvar mod væbnede angreb og iværksættelsen af modforanstaltninger. Som et supplement hertil redegøres der også for nødretten som en folkeretlig ansvarsfrihedsgrund. Det konkluderes, at en velovervejet anvendelse af de opregnede folkeretlige 'figurer' i teorien giver en stat som Danmark de fornødne folkeretlige beføjelser til at foretage sig de handlinger, der er nødvendige for at standse de skadevoldende aktiviteter i cyberspace, der måtte udgå fra udlandet. Det anbefales afslutningsvis, at Danmark arbejder for, at alle stater lever op til deres folkeretlige forpligtelse til at standse de skadevoldende cyberaktiviteter, der udgår fra deres territorier, at de relevante danske myndigheder udarbejder klare retningslinjer for, hvorledes man fra dansk side håndterer de situationer, hvor Danmark gøres til genstand for større cyberangreb fra udlandet, og endelig at de danske politikere overvejer, hvor voldsomme cyberangreb, vi fra dansk side er parate til at acceptere inden de relevante danske myndigheder påbegynder cyberangreb, der krænker andre staters suverænitet.

Anbefalinger

Som andre stater er også Danmark udfordret folkeretligt i forhold til at udarbejde de fornødne retningslinjer for, hvorledes vi fra dansk side må imødegå skadevoldende cyberaktiviteter, der udgår fra udlandet. I lyset heraf indeholder denne rapport følgende anbefalinger.

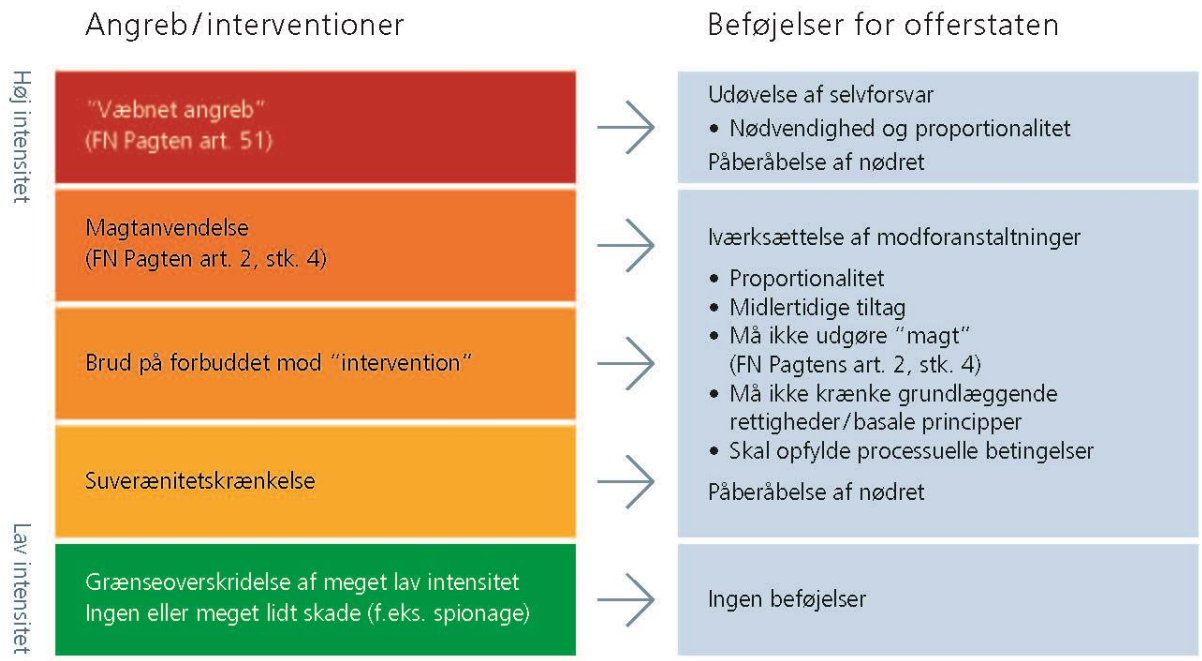
1) Danmark bør arbejde for, at stater lever op til deres folkeretlige forpligtelse til at standse de skadevoldende cyberaktiviteter, der udgår fra deres territorier.

2) De relevante danske myndigheder bør udarbejde klare retningslinjer for, hvorledes man fra dansk side håndterer de situationer, hvor Danmark gøres til genstand for større cyberangreb fra udlandet, og hvor det må forventes, at de lokale myndigheder i værtsstaten hverken selv foretager sig det fornødne for at bringe angrebene til ophør eller giver samtykke til, at de danske myndigheder kan forsøge at standse angrebene. Det anbefales i den forbindelse, at de danske myndigheder gør brug af de folkeretlige 'figurer', der opstilles i rapporten (se figur 1 nedenfor), og skaber den fornødne grad af operationel klarhed over, hvornår danske modreaktioner, der krænker andre staters suverænitet, kan undtages i henhold til henholdsvis principperne om udøvelse af ret til selvforsvar, modforanstaltninger og nødret. Den nødvendige operationelle klarhed vil eventuelt kunne skabes i forbindelse med afholdelsen af diverse former for scenariebaserede øvelser.

3) De danske politikere bør overveje, hvor voldsomme cyberangreb, vi fra dansk side er parate til at acceptere inden de relevante danske myndigheder påbegynder cyberangreb, der krænker andre staters suverænitet. Resultatet af disse overvejelser bør kommunikeres klart til de relevante danske myndigheder.

4) Eventuelle danske modreaktioner mod skadevoldende cyberaktiviteter bør så vidt muligt have samme karakter som de pågældende aktiviteter.

Figur 1: Folkeretlige beføjelser ('figurer') ved forskellige angrebstyper.



Indholdsfortegnelse

1. BAGGRUND 1

2. UDFORDRINGERNE I CYBERSPACE 5

3. SUVERÆNITET I CYBERSPACE – RETTIGHEDER OG PLIGTER 7

3.1. Baggrund 7

3.2. Principperne om territoriel ukrænkelighed 7

3.3. Principperne om udøvelse af suverænitet 8

3.4. Pligten til at beskytte andre stater mod skadevoldende handlinger 9

3.5. Brud på pligten til at beskytte andre stater 10

4. UDØVELSE AF SELVFORSVAR MOD CYBERANGREB 12

5. MODFORANSTALTNINGER 15

5.1. Baggrund 15

5.2. Særligt om proportionaliteten af modforanstaltninger 17

5.3. Processuelle krav til iværksættelsen af modforanstaltninger 18

6. NØDRET 20

7. KONKLUSION – OG ANBEFALINGER 22

8. NOTER 25

9. LITTERATUR 31

1. Baggrund

Forsvarsministeriet har med afsæt i det seneste forsvarsforlig oprettet en cyberkapacitet – det såkaldte Center for Cybersikkerhed – der bl.a. skal 'forsvare egen brug af og forhindre modstanderes udnyttelse af cyberspace'.[1]

Som led i forberedelserne til implementeringen af denne cyberkapacitet offentliggjorde Center for Militære Studier efter ønske fra forsvarsministeriet i april 2012 en rapport om "Cyberkrig, folkeretten og computer network operations" – i det følgende benævnt "2012-rapporten" – der analyserede cyberoperationers forenelighed med de dele af folkeretten, der regulerer, hvornår stater er berettiget til at gøre brug af magt i deres internationale relationer – også betegnet *jus ad bellum*. Rapporten indeholdt endvidere en række anbefalinger til de relevante danske myndigheder, herunder en anbefaling om, at der etableres nogle "klare retningslinjer for, hvordan vi fra dansk side reagerer, hvis Danmark rammes af større cyberangreb", og at det overvejes, "hvornår cyberangreb anses for at være så alvorlige, at de bør udløse danske modforanstaltninger, herunder egentlige selvforsvarshandlinger".[2] Det blev også anbefalet, at forsvaret udarbejder "klare operationelle retningslinjer for, hvordan Danmark reagerer på konkrete cyberangreb", eventuelt i form af en art 'cyberforholdsordre', der "kan tjene som grundlag for en indledende dansk reaktion på igangværende cyberangreb på Danmark."[3]

Formålet med nærværende rapport om "Modreaktioner i cyberspace" er at følge op og bygge videre på 2012-rapporten, herunder at redegøre mere fyldestgørende for de beføjelser, som folkeretten giver en stat som Danmark, når denne gøres til genstand for cyberangreb fra udlandet. Sigtet er bl.a. at kaste lys over, hvorledes en stat som Danmark kan imødegå de cyberangreb, der ikke er tilstrækkeligt alvorlige til at udgøre et 'væbnet angreb', der i henhold til artikel 51 udløser en ret til selvforsvar.

Det er i den forbindelse værd at bemærke, at der til dato kun har været meget få tilfælde, hvor det har været relevant at diskutere, om et cyberangreb har udgjort et væbnet angreb, der har udløst en ret til selvforsvar.[4] Selvom det ikke skorter på dommedagsprofetier om cyberrelaterede børskrak, flyvemaskiner, der falder ned fra himlen, og nedsmeltede atomkraftværker, så har cyberangreb indtil videre (heldigvis) været af et helt andet og langt mindre alvorligt omfang. Der er eksempelvis (så vidt vides) endnu ikke nogen, der er kommet til skade i cyberangreb, og selvom der som berørt i rapporten fra 2012 er flere eksempler på, at stater har udført omfattende cyberoperationer mod andre stater som led i forberedelsen af

konventionelle angreb[5] eller som et supplement til konventionelle militære operationer[6], så har vi også endnu til gode at se den første egentlige cyberkrig, der udelukkende føres i cyberspace. I sin seneste trusselsvurdering konkluderer Center for Cybersikkerhed da også, at det ikke er sandsynligt, at "statslige aktører vil udføre et målrettet angreb på dansk kritisk infrastruktur på kort til mellemlang sigt", og at ikke-statslige aktører ikke for nuværende har "de fornødne tekniske kapaciteter til at udføre avancerede angreb."[7] De for tiden mest presserende folkeretlige spørgsmål for en stat som Danmark knytter sig derfor heller ikke så meget til rammerne for cyberkrig, men derimod i stedet om at finde ud af, hvorledes danske myndigheder skal forholde sig folkeretligt i forhold til de cyberangreb, der, trods ikke ubetydelige gener og forstyrrelser, er af væsentligt mindre omfang.

Der er flere grunde til, at det ikke har været helt ligetil at udarbejde denne rapport. Der er for det første meget lidt relevant folkeretlig litteratur på området. De eksisterende artikler, bøger og rapporter fokuserer stort set udelukkende på cyberkrig, og de mest voldsomme former for cyberangreb[8], og det måske bedste eksempel er den meget omtalte "Tallinn-manual", som en international ekspertgruppe offentliggjorde i foråret 2013.[9] Manualen får givetvis central betydning for den folkeretlige debat, og der henvises da også med mellemrum til manualen i denne rapport, men den forholder sig primært til den del af folkeretten, der regulerer staters brug af væbnet magt og væbnede konflikter.[10] En ny ekspertgruppe indledte ganske vist i starten af 2014 arbejdet med at skrive en såkaldt "Tallinn Manual 2.0", der skal kigge nærmere på staters reaktioner på mindre alvorlige cyberangreb, men resultatet af dette arbejde forventet først at ligge klar i 2016.[11] Det hører herudover også med til historien om manualen, at den kun blev udarbejdet *på opfordring fra* NATOs Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) i Tallinn, Estland, og at dets indhold alene udtrykker ekspertgruppens opfattelse af gældende folkeret – og ikke NATOs.[12]

Det har for det andet været endog særdeles vanskeligt at identificere folkeretseksperter, der har haft en kvalificeret holdning til de spørgsmål, der er genstand for analyse i rapporten. Den stort set samstemmende tilbagemelding fra de folkeretseksperter, som er blevet kontaktet i forbindelse med udarbejdelsen af rapporten har faktisk været, at der – indtil videre – stort set ingen specifik viden er på området. De almindelige folkeretlige principper, der kan tænkes at have relevans, er velkendte, men kun meget få har undersøgt, hvorledes de mere konkret skal finde anvendelse i cyberspace. Som professor Michael N. Schmitt, der var formand for den ekspertgruppe, der udarbejdede Tallinn-manualen, bemærkede, så er området ganske enkelt uopdyrket.[13]

Der er som led i udarbejdelsen af rapporten ikke desto mindre blevet afholdt møder med repræsentanter for forsvarsministeriets departement og med Center for Cybersikkerhed i Danmark, ligesom der har været gennemført en række møder med relevante forskere i Sverige og med repræsentanter for det svenske forsvarsministerium. Endelig har forfatteren afholdt et besøg i Washington D.C., USA, hvor der var lejlighed til at drøfte centrale problemstillinger med relevante ressourcepersoner.

Cyberspace udfordrer på en række områder de stater, der, som Danmark, ønsker at imødegå skadevoldende cyberaktiviteter, der udgår fra andre stater, og en af primære folkeretlige udfordringer består i at skabe et system, der effektivt og lovligt gør det muligt at imødegå skadevoldende aktiviteter i cyberspace uden kendskab til bagmændenes identitet eller motiver. Formålet med rapporten er at forsøge at bidrage til etableringen af et sådant system ved at give en række folkeretlige svar på, hvorledes en stat som Danmark må imødegå cyberangreb fra udlandet. Det sker i praksis ved at redegøre for de forskellige folkeretlige 'figurer', der kan være af relevans i forhold til at vurdere, om – og i givet fald hvornår – danske myndigheder er berettiget til at operere i andre stater, herunder på andre staters netværk.

To ting skal i den forbindelse understreges.

Det første er, at rapporten ikke berører de strafferetlige aspekter af internationale skadevoldende aktiviteter i cyberspace, og at det i sagens natur betyder, at der meget vel kan være en række forhold af potentiel relevans for etableringen af et egnet folkeretligt beredskab mod skadevoldende cyberaktiviteter, såsom spørgsmål om etableringen af et velegnet strafferetligt værn mod cyberkriminalitet og forbedringen af det internationale samarbejde om efterforskning og udlevering, der ikke behandles.

Den anden ting, der skal understreges er, at rapportens formål som berørt er begrænset til at opstille de relevante *folkeretlige* rammer for Danmarks eventuelle politik for modreaktioner i cyberspace. Svarene på, hvordan den konkrete politik skal se ud, og hvorledes denne i praksis skal føres ud i livet, må findes andetsteds. Rapporten forholder sig med andre ord *ikke* til, om det altid vil være opportunt – endsige praktisk muligt – for de relevante danske myndigheder at gøre brug af de beføjelser til at reagere på diverse former for cyberangreb, som folkeretten giver Danmark.

Rapporten er struktureret på den måde, at den indledes umiddelbart neden for med et par ord om de folkeretlige udfordringer, der er forbundet med det forhold, at det ofte volder endog

særdeles store vanskeligheder at identificere ikke bare den aktør, der står bag skadevoldende cyberaktiviteter, men også den stat, hvorfra disse aktiviteter udgår (afsnit 2). Herefter gennemgår rapporten de generelle principper om suverænitet, der danner baggrund for den mere detaljerede folkeretlige regulering på området (afsnit 3). Rapporten vender sig herefter mod de folkeretlige 'figurer', der kan være af relevans, når det skal vurderes, hvornår statslige myndigheder må agere på andre staters netværk uden samtykke for at imødegå cyberangreb. Det drejer sig om henholdsvis udøvelsen af selvforsvar (afsnit 4), iværksættelsen af modforanstaltninger (afsnit 5) og endelig nødretlige betragtninger (afsnit 6). Rapporten rundes af med en kort konklusion og et par konkrete anbefalinger til de danske myndigheder, der skal operere i den til tider mudrede folkeretlige virkelighed på området (afsnit 7).

Til sidst, et par korte bemærkninger om definitioner og terminologien i rapporten. Begrebet "cyberspace" defineres med udgangspunkt i den definition, der opstilles i det amerikanske forsvar, hvorefter cyberspace er:

> the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded processors and controllers.[14]

Som i rapporten fra 2012 skal begrebet 'cyberangreb' og/ eller computer netværk operationer i denne rapport forstås som: "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers or networks themselves."[15] Betegnelsen skadevoldende cyberaktiviteter benyttes synonymt hermed.

2. Udfordringerne i cyberspace

Cyberspace udfordrer på en række områder de stater, der, som Danmark, ønsker at imødegå skadevoldende cyberaktiviteter, der udgår fra andre stater. Rapporten fra 2012 redegjorde for den udfordring, der består i, at det kan være vanskeligt at vurdere, hvorledes cyberangreb skal klassificeres folkeret, herunder hvornår cyberangreb har karakter af ulovlige interventioner, magtanvendelse i henhold til FN Pagten osv. En anden væsentlig udfordring har at gøre med det forhold, at der ofte er endog særdeles store vanskeligheder forbundet med at identificere den aktør, der står bag et konkret cyberangreb. Som det blev bemærket i en rapport fra 2011 fra det britiske Chatham House, så er et af de største problemer ved cyberspace ganske enkelt "the shield of anonymity it offers, at least in the short term. Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity.[16] Det er i den forbindelse værd at bemærke, at det ikke kun er en aktørs mulighed for at "anonymisere" *sin egen computer*, der skaber problemer. Det samme gør hackere og andre aktørers mulighederne for at "overtage" andres computere til brug for iværksættelsen af cyberangreb – såkaldte "*zombie-angreb*". Med til historien om identifikationsproblemerne hører også, at cyberspace gør det muligt for aktører at iværksætte deres skadevoldende angreb uden varsel for herefter at 'forsvinde' igen.[17] Som Duncan B. Hollis bemærker, så er det et faktum, at "anonymity, no attribution, prevails. Current information technology makes it difficult to identify the actual server from which an attack (or exploit) originates, let alone its perpetrators."[18]

De vanskeligheder, der er forbundet med at identificere den aktør, der står bag skadevoldende aktiviteter i cyberspace, betyder, at det ikke altid er klart for den stat, der gøres til genstand for aktiviteterne, om det er en privat aktør eller en anden stat, der står bag. Og ikke nok med det. Identifikationsproblemerne kan undertiden være så store, at det kan være vanskeligt at finde ud af, fra hvilken stat de pågældende aktiviteter i det hele taget udgår.

I fraværet af viden om, hvorvidt det er en stat eller en privat aktør, der står bag skadevoldende aktiviteter i cyberspace, er det ofte svært at vurdere, hvad formålet/ motivet med de pågældende aktiviteter er. For som Susan W. Brenner beskriver, så er vores traditionelle opfattelser af, hvad der ligger til grund for en given skadevoldende aktivitet i høj grad bundet op på nogle basale antagelser om, at identiteten af den aktør, der står bag den givne aktivitet, fortæller os noget om aktivitetens formål. Kategorier som 'krig', 'spionage', 'terrorisme', 'kriminalitet', 'hærværk', 'tyveri' osv. er baseret på en forestilling om, at det er

henholdsvis en stat eller en privat aktør, der står bag.[19] Stater står bag krigshandlinger og spionage, mens private aktører står bag forskellige typer af kriminalitet osv. Den samme skadevoldende aktivitet klassificeres med andre ord forskelligt afhængigt af, om det er en stat eller en privat aktør, der udøver den.

Det er vigtigt at forstå, at de vanskeligheder, der er forbundet med at identificere formålet med en skadevoldende aktivitet, ikke kun er af akademisk interesse. Det statslige beredskab over for skadevoldende handlinger er nemlig i høj grad knyttet op på netop viden om disse handlingers formål. Forskellige former for beredskab med forskellige procedurer håndterer de forskellige typer af skadevoldende handlinger. Det militære beredskab tager sig groft sagt af de skadevoldende handlinger, som andre stater står bag (krigshandlinger), mens det civile politimæssige beredskab tager sig af de handlinger, som private aktører står bag (kriminalitet). Hertil kommer et eventuelt beredskab, der kan aktiveres i forhold til andre typer af krisesituationer, såsom naturkatastrofer og lignende.[20]

De eksisterende kategorier og procedurer for håndteringen af skadevoldende adfærd opløses altså, når det vedrører imødegåelsen af skadevoldende handlinger i cyberspace, og derfor forekommer en af de primære udfordringer for de stater, der, som Danmark, ønsker at imødegå skadevoldende aktiviteter i cyberspace at være, at de skal skabe et system, der gør det muligt imødegå skadevoldende handlinger uden kendskab til bagmændenes identitet eller motiver.[21] Formålet med denne rapport er at bidrage til at kaste lys over, hvornår de konkrete tiltag kan forenes med folkeretten.

I den resterende del af denne rapport gøres der på den baggrund en række betragtninger om de tiltag af folkeretlig karakter, som Danmark med fordel kan skele til med henblik på at skabe det folkeretlige set-up, der er nødvendigt for at kunne imødegå skadevoldende aktiviteter i cyberspace ved – undertiden – at operere på andre staters netværk. Gennemgangen indledes i den forbindelse i det følgende med en oversigt over de almindelige folkeretlige principper om suverænitet, der ligger til grund for den mere konkrete folkeretlige regulering af modreaktioner i cyberspace.

3. Suverænitet i cyberspace – rettigheder og pligter

3.1. Baggrund

Det hed sig ofte i 1990'erne, at cyberspace ville være et nyt og helt særligt domæne – *sui generis* – der var undtaget staters normale kontrol.[22] I modsætning til de 'fysiske' domæner, som landmasserne, luftrummet og det åbne hav, skulle cyberspace således være et selvreguleret område, hvor de almindelige folkeretlige principper om suverænitet og staters jurisdiktion ikke skulle gælde.

Cyberspace adskiller sig ganske rigtigt på mange måder fra de vanlige og mere fysiske domæner, og som både rapporten fra 2012 og denne rapport illustrerer, så er der heller ingen tvivl om, at cyberspaces særlige karakteristika stiller store krav til de jurister, der skal forsøge at identificere den rette regulering på området. Men at cyberspace skulle være afkoblet fra de vanlige folkeretlige principper, og et sted hvor staterne derfor skulle være afskåret fra at gøre sig gældende, er der intet belæg for at hævde. Internettet er aldrig blevet selvreguleret og udviklingen viser med al tydelighed, at staterne er "til stede" i cyberspace.[23] I dag er adfærd på nettet da også underlagt såvel national som international regulering.[24]

Et af mest fundamentale principper i folkeretten er suverænitetsprincippet, og staternes gensidige respekt for territoriel suverænitet er med Den Internationale Domstols ord "an essential foundation of international relations". [25] For at forstå den folkeretlige regulering af cyberspace og baggrunden for de beføjelser, som en stat, der er udsat for cyberangreb fra udlandet er udstyret med, er det nødvendigt at forstå, at principperne om *territoriel suverænitet* betyder, at en stat både har rettigheder og pligter over sit territorium og i forhold til de aktiviteter, der foregår derpå.

3.2. Principperne om territoriel ukrænkelighed

Det er for det første værd at hæfte sig ved, at statens territorielle suverænitet anses som ukrænkeligt, hvilket i praksis betyder, at stater som udgangspunkt er afskåret fra at bryde andre staters suverænitet og udøve deres myndighed på andre staters territorium. Hvis en stat ikke desto mindre alligevel udøver sin myndighed på en anden stats territorium, vil handlingerne derfor med ganske få undtagelser have karakter af folkeretsstridige suverænitetskrænkelser. Undtagelserne vedrører først og fremmest de tilfælde, hvor fremmede staters magtanvendelse er baseret på et mandat fra FN's Sikkerhedsråd i henhold til FN Pagtens kapitel 7 eller er foreneligt med udøvelsen af lovligt selvforsvar i henhold til

artikel 51 i pagten. Stat A's cyberrelaterede myndighedsudøvelse på stat B's territorium har derfor som udgangspunkt også karakter af krænkelser af B's suverænitet.[26]

Det skal dog understreges, at der formentlig gælder en *de minimis*-regel på området, hvorefter mindre alvorlige handlinger på en anden stats territorium, der alene forårsager minimal skade, falder uden for området for suverænitetskrænkelser.[27] Det er derfor også muligt, at en territorialstat må acceptere cyberoperationer, der alene forårsager meget begrænset skade. Til støtte herfor taler, at spionage som udgangspunkt ikke er at anse som folkeretsstridige suverænitetskrænkelser eller på anden vis i strid med folkeretten, medmindre den er rettet mod kommunikation, der er særlig beskyttet.[28] Cyberoperationer, der alene *passerer/ routes* gennem territorialstatens cyberinfrastruktur, vil derfor heller ikke blive anset for at udgøre suverænitetskrænkelser.

Det hører herudover med til historien, at samtykke er en såkaldt ansvarsfrihedsgrund, og at en stat derfor ikke ifalder et folkeretligt ansvar for de handlinger på en anden stats territorium, der normalt ville udgøre krænkelser af denne stats suverænitet, hvis der foreligger et samtykke fra territorialstaten.[29] Et samtykke skal være givet inden den adfærd, der ville have udgjort et brud på folkeretten.[30]

3.3. Principperne om udøvelse af suverænitet

Suverænitetsprincippet betyder også, at en stat kan udøve sin suverænitet i form af jurisdiktion over sit territorium[31] og over de aktiviteter, der udøves herpå. Som Den Permanente Internationale Voldgiftdomstol udtalte i *Island of Palmas*: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[32] Med de undtagelser der følger af de folkeretlige principper om diplomatisk immunitet[33] og retten til uskadelig passage i havretten[34], må en stat derfor udøve jurisdiktion over de dele af cyberspace, der er "beliggende" på dets territorium, herunder på skibe og fly indregistreret i staten, og de cyberaktiviteter, der udøves herpå.[35]

Det er den forbindelse at vigtigt være opmærksom på, at cyberspace ikke kun er et "virtuelt" rum, men i høj grad er knyttet op på en fysisk infrastruktur i form af servere, kabler og lignende, der som regel er beliggende på en stats territorium. På samme måde som brugerne af cyberspace, såsom hackere og diverse internetaktivister, som regel opholder sig fysisk på en eller anden stats territorium, når de trykker på de taster på deres tastatur, der skaber en elektronisk aktivitet på nettet. Der kan ganske vist være særlige forhold, der i praksis gør det

vanskeligt for stater at udøve deres suverænitet på en effektiv måde i cyberspace, men det betyder ikke, at de almindelige principper om suverænitet og jurisdiktion ikke finder anvendelse. Som Wolff Heintschel von Heinegg har bemærket om suveræniteten over cyberinfrastruktur:

> While, in view of the genuine architecture of cyberspace, it may be difficult to exercise sovereignty, the technological and technical problems involved do not prevent a State from exercising its jurisdiction over the cyber infrastructure located in areas in its sovereign territory.[36]

Territorialstatens ret til at udøve suverænitet over sit territorium betyder i praksis, at den er tillagt vide rammer i forhold til at regulere, begrænse og forbyde adgang til den cyberinfrastruktur, der er beliggende på dets territorium, ligesom den i vidt omfang kan håndhæve sin lovgivning i forhold til de cyberaktiviteter, der finder sted på territoriet. Det hører dog med til historien, at den konkrete udøvelse af jurisdiktion efter omstændighederne kan være begrænset af statens folkeretlige forpligtelser, herunder menneskeretlige. De menneskeretlige aspekter af staters ageren i cyberspace behandles ikke i denne rapport.

3.4. Pligten til at beskytte andre stater mod skadevoldende handlinger

Med suverænitet kommer imidlertid ikke kun rettigheder men også *pligter*, og en af de primære af disse er, at en stat har pligt til at sikre, at dets territorium ikke anvendes til skade for andre stater. Som Den Internationale Domstol konkluderede i *Corfu Channel*, så må en stat ikke ”knowingly” tillade ”its territory to be used for acts contrary to rights of other States.”[37] Overført på cyberspace betyder denne pligt – der genfindes i den internationale miljøret og i *Trail Smelter*-sagen[38] og i praksis antager karakter af en form for handlepligt – at en stat ikke må lade dets territorium, herunder dets cyberinfrastruktur, anvende til brug for iværksættelsen af skadelige cyberaktiviteter mod andre stater, hvis staten har viden herom.[39]

og det er værd at hæfte sig ved, at handlepligten ikke kun omfatter de handlinger, der er kriminelle, men alle handlinger, der må anses for på den ene eller anden måde at forvolde skade på en anden stat.[40] Det er med Tallinn-manualens ord ikke et krav, at “the cyber operation in question result in physical damage to objects or injuries to individuals; it need only produce a negative effect.”[41] Det manglende forbud mod spionage tilsiger imidlertid også på dette punkt, at cyberoperationer, der ikke forårsager skade, vil falde uden for.[42]

Det er oplagt, at der vil kunne være divergerende opfattelser fra stat til stat af, hvilke handlinger, der er at anse som ”skadevoldende” og hvilke, der ikke er, og at der i sagens natur

også vil kunne opstå uenighed mellem stat A og stat B om, hvornår eksempelvis stat B's pligt til at skride ind over for en privat aktør aktiveres.

Pligten til at handle over for skadevoldende cyberaktiviteter gælder under alle omstændigheder som berørt kun i forhold til de cyberaktiviteter, som en stat har viden om ("knowingly"), og spørgsmålet er selvfølgelig, hvad der mere præcist ligger heri. I henhold til Tallinn-manualen foreligger der "viden", når territorialstaten selv opdager de pågældende skadevoldende cyberaktiviteter eller gøres opmærksom herpå af en anden stat, såsom den stat, der er offer for aktiviteterne.[43] Altså *faktisk* viden. Manualens ekspertgruppe kunne imidlertid ikke opnå enighed om, hvorvidt "viden" også omfatter de situationer, hvor staten *burde have* viden om aktiviteterne.[44]

De særlige teknologiske forhold i cyberspace vil i praksis kunne volde problemer. Som en af medlemmerne af ekspertgruppen har bemærket, så vil en "knows-or-should-have-known" standard pålægge "far-reaching prevention obligations on States that, given the nature of the technology involved, would be difficult, if not impossible, to fulfill."[45]

Ekspertgruppen kunne heller ikke opnå enighed om, hvorvidt handlepligten i cyberspace inkluderer de aktiviteter, der alene *passerer/ routes gennem statens infrastruktur*.[46] Også her vil teknologien imidlertid formentlig kunne volde problemer, og det vil i praksis næppe giver nogen mening at "oblige the transit State to take preventive action, because the data may be rerouted, thus nevertheless arriving at their destination in the target State."[47]

3.5. Brud på pligten til at beskytte andre stater

Hvis en stat krænker sin pligt til at hindre, at cyberinfrastruktur på dets territorium anvendes til brug for skadelige cyberhandlinger mod andre stater, gør den sig skyldig i folkeretsbrud, hvorved den stat, der udsættes for de skadelige handlinger – offerstaten – efter omstændighederne kan være berettiget til at tage de fornødne initiativer på den krænkende stats territorium, herunder på dennes netværk, til at bringe handlingerne til ophør. Som redegjort for i rapporten fra 2012, afhænger omfanget af offerstatens beføjelser i høj grad af karakteren af cyberangrebet og dets styrke og intensitet. Jo voldsommere angrebet er, jo flere beføjelser. Dertil kommer, at der som oven for berørt formentlig gælder en *de minimis*-regel på området, hvorefter stater må acceptere mindre alvorlige aktiviteter på deres territorier.

Som berørt i indledningen er det primære sigte med denne rapport at kaste lys over, hvorledes en stat som Danmark kan imødegå de cyberangreb, der ikke er tilstrækkeligt alvorlige til at udgøre et 'væbnet angreb', der i henhold til artikel 51 udløser en ret til selvforsvar. For

fuldstændighedens skyld redegøres der imidlertid ikke desto mindre alligevel i det følgende i oversigtsform indledningsvis for netop de folkeretlige principper for udøvelse af selvforsvar over for væbnede angreb i cyberspace inden opmærksomheden vendes mod iværksættelsen af modforanstaltninger mod den eller de stater, der har gjort sig skyldig i et folkeretsbrud.

4. Udøvelse af selvforsvar mod cyberangreb

Rapporten fra 2012 om "Cyberkrig, folkeretten og computer network operations" havde som berørt til formål at redegøre for cyberoperationers forenelighed med de dele af folkeretten, der regulerer, hvornår stater er berettiget til at gøre brug af magt i deres internationale relationer, og rapporten redegjorde i den forbindelse for, at det fortsat er uafklaret, hvornår – om overhovedet – cyberangreb kan sidestilles med det magtbegreb, der ligger til grund for den regulering af interstatslig magtanvendelse, der findes i FN pagten fra 1945, herunder i dennes artikel 2, stk. 4.

Det konkluderes ikke desto mindre, at det er sandsynligt, at stater vil anlægge en "effektbaseret tilgang"[48], og at cyberangreb derfor vil blive sidestillet med 'magt', når det har "tilstrækkelig lighed med kinetisk magt".[49] Det konkluderedes derfor også, at det ikke kan "udelukkes, at særligt voldsomme cyberangreb vil kunne opfylde betingelserne for at udgøre et 'væbnet angreb'", der i henhold til artikel 51 i FN Pagten udløser en ret til selvforsvar for den stat, der er offer for angrebet.[50] Den effektbaserede tilgang genfindes i Tallinn-manualen.[51]

Rapporten henledte herefter opmærksomheden på de folkeretlige krav til lovlig udøvelse af selvforsvar mod et væbnet angreb, herunder kravene om nødvendighed og proportionalitet[52], ligesom der blev redegjort for de folkeretlige principper for staters ansvar for private personers handlinger. Det blev i den forbindelse konkluderet, at "en stat kun er ansvarlig for private personers cyberangreb, når staten har været i stand til at udøve 'effektiv kontrol' over personerne under de operationer, hvor cyberangrebene finder sted."[53] Det blev imidlertid i den forbindelse også bemærket, at dette ikke nødvendigvis betyder, at en stat, der er udsat for cyberangreb fra private aktører, så ikke kan være berettiget til at forsøge at bringe angrebene til ophør. Der vil nemlig efter omstændighederne være grundlag for, at staten kan forsvare sig imod den private aktør, hvis den stat, hvori den private aktør opholder sig, "har vist sig at mangle enten den fornødne vilje eller evne til at standse angrebene fra den private aktør".[54]

Doktrinen om mangel på "vilje og evne" – the "able and willing" doctrine – udspringer af de folkeretlige principper om neutralitet under væbnede konflikter, der har til formål at regulere forholdet mellem de stater, der er involveret i en væbnet konflikt, og stater, der ikke er.[55] Principperne er baseret på to hensyn. For det første et hensyn til de stater, der ønsker at holde sig ude af den væbnede konflikt og undgå de negative konsekvenser af krigen, og for det

andet et hensyn til de stridende parters og deres legitime ønsker om at forhindre handlinger, der gavner fjenden.[56]

Det første hensyn tilsiger, at de stridende parter skal respektere andre staters neutralitet og derfor hverken må angribe neutrale stater eller gennemføre krigshandlinger på neutrale staters territorium.[57] Til gengæld herfor er de neutrale stater så forpligtet til at respektere de stridende parter, og neutrale stater må ikke tillade, at de krigsførende stater anvende dets territorium eller infrastruktur uden for territoriet til at gennemføre krigshandlinger, hvis de har viden herom.[58] Herved imødekommes det andet hensyn. Hvis en neutral stat har viden om, at et sådant misbrug finder sted og ikke griber ind og indstiller det, vil den krigsførende stat, der gøres til genstand for de handlinger, der udgår fra det neutrale territorium, være berettiget til selv at forsøge at standse handlingerne.

I det omfang, at en neutral stat ikke lever op til sine forpligtelser om at standse de operationer, som en krigsførende stat foretage fra dets territorium eller infrastruktur i strid med reglerne om neutralitet, kan den krigsførende part, der gøres til genstand for de pågældende operationer, gribe til modforanstaltninger og tage de skridt, der er nødvendige for at bringe operationerne til ophør.[59] To betingelser skal imidlertid være opfyldt. For det første skal overtrædelserne af neutralitetsreglerne være alvorlige[60] og for det andet skal krænkelserne udgøre en så umiddelbar trussel mod den krigsførende stat, at der ikke er nogen reelle alternativer til indgriben. Modforanstaltningerne er derfor også kun mulige over for den neutrale stat, der mangler viljen eller evnen til selv at standse de operationer, der udgår fra dets territorium eller infrastruktur i udlandet.[61]

Rapporten fra 2012 redegjorde for, at det er et omdiskuteret spørgsmål, om der i særlige tilfælde eksisterer en ret til selvforsvar mod en privat aktør.[62] Den Internationale Domstol har indtil videre været afvisende[63] og et bekræftende svar er derfor kontroversielt.[64] Rapporten konkluderede ikke desto mindre, at den internationale reaktion på terrorangrebene i USA den 11. september 2001 viste, at en sådan ret formentlig *er* opstået.[65]

Overført på cyberspace gives en sådan ret til selvforsvar en stat, der er udsat for særdeles voldsomme cyberangreb, beføjelser til at forsøge at bringe angrebene til ophør ved – om fornødent – at ty til egentligt væbnet magt i en anden stat for at bringe cyberangrebene til ophør. Da selvforsvarsretten imidlertid alene kan udøves over for særdeles omfattende cyberangreb, der forårsager endog særdeles store økonomiske ødelæggelse og/ eller tab af menneskeliv,[66] vil denne ret kun særdeles sjældent finde anvendelse. Hertil kommer, at

udøvelse af selvforsvar forudsætter, at det er muligt at identificere den stat, hvorfra den skadevoldende aktivitet udgår, og som har gjort sig skyld i en folkeretsstridig adfærd. Som berørt i afsnit 2 er dette ikke altid muligt.

5. Modforanstaltninger

5.1. Baggrund

De folkeretlige principper om iværksættelsen af modforanstaltninger mod andre staters folkeretsstridige handlinger giver som udgangspunkt en stat mulighed for at forsøge at imødegå alle de skadevoldende cyberangreb, der ikke er tilstrækkeligt alvorlige til at udgøre væbnede angreb, der udløser en ret til selvforsvar.[67] Og principperne fungerer herved som et velegnet supplement til selvforsvaretten.

De relevante principper for iværksættelsen af modforanstaltninger opregnes i Den Internationale Lovkommissions retningslinjer for statsansvar fra 2002, der i høj grad anses for at udtrykke de gældende regler på området.[68] Det fremgår heraf, at en stat, der har været udsat for et folkeretsbrud fra en anden stat, selv kan være berettiget til at bryde folkeretten over for denne stat.[69] Eller som Voldgiftsdomstolen i *US-French Air Services Arbitration* formulerede det: "If a situation arises, which in one State's view, results in the violation of an international obligation by another State, the first State is entitled … to affirm its right through 'countermeasures'".[70] En stat, der har været udsat for et folkeretsstridigt cyberangreb fra en anden stat, kan derfor være berettiget til at bryde sine folkeretlige forpligtelser, herunder i cyberspace, over for denne stat.[71] Det er imidlertid også her værd at bemærke, at stater i henhold til en *de minimis*-regel må acceptere mindre alvorlige cyberangreb.

Muligheden for at gengælde en folkeretskrænkelse med en anden folkeretskrænkelse giver i hvert fald i teorien en stat en ganske vidtrækkende beskyttelse mod de skadefulde effekter af andre staters folkeretsbrud, herunder i cyberspace.[72] Det skal i den forbindelse understreges, at adgangen til at iværksætte modforanstaltninger mod en anden stat ikke kun gælder, når det er denne stat selv, der står bag de pågældende cyberaktiviteter, men efter omstændighederne også, når det er en privat aktør, der opererer fra statens territorium.[73] Som berørt i forrige afsnit gør en stat sig nemlig skyldig i et folkeretsbrud, hvis den ikke standser de skadevoldende cyberoperationer mod andre stater, som den er vidende om udøves fra dets territorium.[74] Den konkrete modforanstaltning består her i, at offerstaten ikke længere respekterer det folkeretlige forbud mod at krænke andre staters suverænitet, fordi den anden stat ved sin manglende opfyldelse af sine folkeretlige forpligtelser ej heller respekterer forbuddet.[75]

Det fremgår af lovkommissionens retningslinjer, at modforanstaltninger alene er tænkt som en *midlertidig foranstaltning*, der har til formål at få den stat, der gøres til genstand for

foranstaltningerne, til at (gen)opfylde sine folkeretlige forpligtelser.[76] Foranstaltninger i cyberspace, der er baseret på hævnmotiver, er derfor ikke tilladte.[77] Modforanstaltningernes midlertidige karakter betyder også, at modforanstaltninger i cyberspace bør iværksættes på en sådan måde, at de kan bringes til ophør, når den stat, der gøres til genstand for foranstaltningerne, har indstillet sine folkeretsstridige adfærd i cyberspace.[78] Som Den Internationale Domstol udtalte i *Gabcikovo-Nagymaros Project*, så skal modforanstaltningerne være "reversible."[79] Hertil kommer, at modforanstaltningerne altid skal indstilles, så snart den folkeretsstridige adfærd ophører.[80]

Det fremgår også af retningslinjerne, at der er en række folkeretlige forpligtelser, der er så grundlæggende, at de ikke må gøres til genstand for modforanstaltninger. Det drejer sig indledningsvis om *forpligtelsen til at respektere forbuddet mod brug af magt i artikel 2, stk. 4, i FN Pagten.*[81] Modforanstaltninger i cyberspace må derfor ikke være så indgribende og intense, at de har karakter af 'magtanvendelse' i henhold til artikel 2, stk. 4.[82] Kun i de tilfælde, hvor et cyberangreb er så alvorligt, at det har karakter af et 'væbnet angreb', vil den stat, der er offer for angrebet, være berettiget til at krænke magtforbuddet i art. 2, stk. 4. Som beskrevet i 2012-rapporten betyder det i praksis, at en stat rent undtagelsesvis ikke altid er berettiget til at reagere på et cyberangreb ved at iværksætte en reaktion af samme styrke.[83]

Retningslinjerne foreskriver dernæst, at modforanstaltninger i cyberspace ej heller må rette sig mod en række *grundlæggende rettigheder og basale humanitære principper*.[84] Det drejer sig om henholdsvis grundlæggende menneskerettigheder[85], forbuddet mod repressalier i den humanitære folkeret[86] og de forpligtelser, der har karakter af *jus cogens*.[87] Det er ikke helt klart, hvilke rettigheder, der specifikt henvises til, men lovkommissionens kommentarer til retningslinjerne indikerer, at forbuddet retter sig mod de allermest grundlæggende rettigheder, såsom retten til liv, forbuddet mod tortur, slaveri, udsultning af civilbefolkningen og forbuddet mod repressalier mod visse persongrupper i internationale væbnede konflikter og lignende.[88] Det er svært at se, at cyberaktiviteter skulle kunne rettes mod nogle af disse rettigheder og forbud, og det er derfor også vanskeligt at forestille sig, at denne del af retningslinjerne har praktisk betydning for modforanstaltninger i cyberspace.

Endelig forskriver lovkommissionens retningslinjer, at modforanstaltninger i cyberspace skal respektere de *folkeretlige principper om diplomatisk og konsulær ukrænkelighed*.[89]

5.2. Særligt om proportionaliteten af modforanstaltninger

Det fremgår af lovkommissionens retningslinjer, at modforanstaltninger skal være "commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[90] Der gælder med andre ord et generelt princip om *proportionalitet*, hvorefter der skal findes en passende balance mellem den folkeretsstridige handling og den foranstaltning, som offerstaten iværksætter som en reaktion herpå. Spørgsmålet er imidlertid, hvordan dette krav overføres på modforanstaltninger i cyberspace. For hvad er det mere præcist, at en foranstaltning skal være proportional med?

I henhold til Tallinn-manualen er der flere muligheder.[91] Den ene er at anlægge en "øje-for-øje' tilgang, hvorefter modforanstaltningen i styrke og intensitet skal være proportional med den retsstridige handling, foranstaltningen iværksættes som en reaktion på. Den udlægning synes at støttes af bl.a. Thomas Franck.[92] Den anden er, at proportionalitetsvurderingen tager afsæt i en afvejning af, hvad der skal til for at få den ansvarlige stat til at bringe den folkeretsstridige adfærd til ophør. Det synes at være opfattelsen hos bl.a. Nigel White og Ademola Abass[93], og hos Antonio Cassesse.[94]

Proportionalitet er altid faktum-afhængig og det giver derfor ikke altid mening at lægge sig meget fast på en given målestok. Da modforanstaltninger imidlertid som berørt har til formål at få den ansvarlige stat til at indstille sine folkeretsstridige handlinger giver det ikke desto mindre i udgangspunktet i hvert fald bedst mening at anlægge den generelle betragtning, at proportionalitet skal vurderes i forhold til, hvad der er nødvendigt for at opnå dette formål.

I forhold til proportionaliteten af modforanstaltninger i cyberspace er især to forhold af betydning. Det første er, at der i teorien ikke gælder noget krav om, at modforanstaltningerne skal have samme karakter som den folkeretsstridige handling, som foranstaltningen er en reaktion på, og at der derfor heller ikke er noget principielt i vejen for, at en offerstat imødegår en folkeretsstridig handling i cyberspace med ikke-cyberrelaterede midler. Det er imidlertid også oplagt, at *modforanstaltninger af samme karakter* i udgangspunktet vil have lettere ved at fremstå proportionale og dermed i praksis også vil være mindre kontroversielle end andre typer modforanstaltninger. Som Oona A. Hathaway m.fl., bemærker, så er "reciprocal measures … favored over other types because they are more likely to comply with the requirement of necessity and proportionality."[95] Det lader da også til at være opfattelsen i en rapport fra det amerikanske forsvarsministerium fra 1999.[96]

Det andet er, at kravet om proportionalitet ikke kun giver en stat mulighed for at iværksætte *defensive* modforanstaltninger, der alene har til formål at afvise et konkret cyberangreb. I sin rapport fra 1999 skriver det amerikanske forsvarsministerium da også:

> If it is capable of doing so … the victim nation may be justified in launching a computer attack in response, intended to disable the equipment being used by the intruder. Disabling one computer may or may not defeat a state-sponsored operation. It may, however, serve as a 'shot across the bow' warning of more serious consequences if the offending behavior continues.[97]

Hvis det er nødvendigt for at få den ansvarlige stat til at ophøre med sin folkeretsstridige handlinger, kan foranstaltningerne også inkludere *aktive* handlinger, hvor der tages skridt til at uskadeliggøre kilden til angrebet.

Der er ingen tvivl om, at netop proportionalitetsprincippet stiller endog særdeles store krav til den stat, der ønsker at imødegå skadevoldende cyberangreb fra andre stater. Det er nemlig langt fra sikkert, at en modreaktion på et cyberangreb kan begrænses til den eller de aktører, der står bag et konkret cyberangreb eller at det kan undgås, at en modreaktion mod en konkret cyberangreb vil kunne have følgevirkninger, der i omfang langt overstiger det, som en proportional modreaktion umiddelbart tilsiger. Det er derfor også muligt, at praktiske og / eller politiske hensyn kan betyde, at en stat undlader at forsøge at imødegå en eller flere konkrete cyberangreb, som det måtte blive udsat for. Selvom folkeretten eventuelt måtte tillade det.

5.3. Processuelle krav til iværksættelsen af modforanstaltninger

Lovkommissionen opstiller i sine retningslinjer en række processuelle krav til den stat, der ønsker at iværksætte modforanstaltninger som en reaktion på en andens stats folkeretsstridige adfærd. Det fremgår bl.a. heraf, at modforanstaltninger som udgangspunkt forudsætter, at den stat, der gøres til genstand for foranstaltningerne, først er blevet anmodet om at opfylde sine folkeretlige forpligtelser.[98] Stat A kan med andre ord som udgangspunkt først indlede sine modforanstaltninger mod stat B i cyberspace, når sidstnævnte ikke har efterkommet en anmodning fra stat A om at standse de skadeforvoldende cyberaktiviteter. Det fremgår også, at den ansvarlige stat skal orienteres, når foranstaltningerne iværksættes og samtidig tilbydes forhandling.[99] Kravene kan i et vist omfang udledes af de almindelige principper om proportionalitet.

De processuelle krav kan i praksis gøre det særdeles vanskeligt for en stat at iværksætte modforanstaltninger mod de cyberangreb, der kommer uden varsel, og det er derfor også af stor praktisk betydning, at lovkommissionen åbner op for, at de formelle krav efter omstændighederne kan tilsidesættes, *hvis det skønnes nødvendigt* for at beskytte en stats rettigheder.[100] Der bør formentlig anerkendes staterne en vis skønsmargin i forhold til at vurdere, hvornår der er et uopsætteligt behov for at iværksætte modforanstaltninger mod igangværende cyberangreb. Som Katharine C. Hinkle noterer sig:

> … the nature of cyber-force weighs in favor of an injured state resorting rapidly, and with broad discretion, to countermeasures. Because cyber-attacks are often both unexpected and capable of significantly impairing critical infrastructure, they are more likely to be viewed as 'emergency scenarios' justifying reasonable state discretion in employing countermeasures.[101]

Eksistensen af en sådan skønsmargin gør, at principperne om modforanstaltninger også kan fungere i forhold til den folkeretsstridige adfærd, der måtte komme som et lyn fra en klar himmel.

Det siger sig selv, at det i praksis kan være endog særdeles vanskeligt at vurdere, hvornår en værtsstat ikke har gjort tilstrækkeligt for at standse de skadevoldende cyberaktiviteter, der måtte udgå fra dets territorium. Hertil kommer, at der eventuelt vil kunne være en masse praktiske forhold, der kan gøre det svært for værtsstaten at leve op til sine forpligtelser i forhold til at standse de pågældende handlinger. Det vil eksempelvis være tilfældet, hvis indgriben forudsætter involvering af private virksomheder.

Adgangen til at udøve modforanstaltninger lider herudover af den samme svaghed som retten til selvforsvar i den forstand, at også den forudsætter, at det er muligt at identificere den stat, hvorfra den skadevoldende aktivitet udgår. Retten til at iværksætte modforanstaltninger giver stat A ret til at bryde folkeretten over for stat B, fordi *denne* har brudt sine forpligtelser over for stat A. Eller som Oona A. Haathaway m.fl. har bemærket om modforanstaltninger i cyberspace: "they require the identity of the attacker and the computer or network from which the attack originates to be accurately identified."[102] Som tidligere berørt er det ikke altid muligt at opnå en sådan grad af identifikation.

6. Nødret

Det er ikke mindst på baggrund af netop identifikationsproblemer, at nødretsfiguren er af særlig relevans i forhold til etableringen af et fintmasket statsligt system for imødegåelse af cyberangreb fra udlandet. I modsætning til hvad angår både retten til selvforsvar og retten til at iværksætte modforanstaltninger kan nødretslige betragtninger nemlig bringes i anvendelse uanset, om der foreligger en folkeretsstridig handling fra en konkret stat eller ej.

Nødretten har levet en tumultarisk tilværelse i folkeretten, men Den Internationale Domstol anerkendte dens eksistens som en ansvarsfrihedsgrund i *Gabcikovo-Nagymaros Project*.[103] Domstolen noterede sig imidlertid også ved samme lejlighed, at den kun vil kunne bringes i anvendelse under exceptionelle omstændigheder[104] og kun, hvis der ikke består andre alternativer til at bryde folkeretten.[105]

De nærmere betingelser for nødret som ansvarsfrihedsgrund er opregnet i artikel 25 i Den Internationale Lovkommissions tidligere nævnte retningslinjer for statsansvar, og det følger heraf at en stat kan være berettiget til at foretage handlinger, der under normale omstændigheder ville udgøre krænkelser af folkeretten, hvis det er nødvendigt for at forsvare en "essential interest" mod en alvorlig og overhængende fare, og hvis handlingen ikke i alvorlig grad "impair an essential interest" hos den stat eller de stater "towards which the obligation exists", eller hos det internationale samfund som helhed.[106] Det fremgår imidlertid også af artikel 25, at en stat ikke kan påberåbe sig nødret i forhold til forpligtelser, der eksplicit ikke kan brydes af nødret eller hvis staten selv har bidraget til "the situation of necessity".

Det hører også med til historien, at det af artikel 26 i retningslinjerne fremgår, at nødret ikke kan gøres gældende over for krænkelser af regler, der har karakter af såkaldt *jus cogens*, hvorved forstås en regel, der er ufravigelig og ikke kan fraviges ved indgåelsen af en traktat.[107] I det omfang magtforbuddet i pagtens artikel 2, stk. 4, er udtryk for *jus cogens* vil nødretsfiguren altså ikke kunne legitimere foranstaltninger, hvis disse opfylder betingelserne for at udgøre egentlig magtanvendelse. Der er ikke enighed om magtforbuddets status af *jus cogens*, og der kan være gode grunde til at forholde sig kritisk.[108] Det ændrer imidlertid ikke på, at det er en ret udbredt opfattelse i den folkeretlige litteratur, at forbuddet *har* en sådan karakter.[109]

Nødretsfigurens potentielle anvendelse på cyberangreb genfindes i Tallinn-manualen[110], hvor det bemærkes:

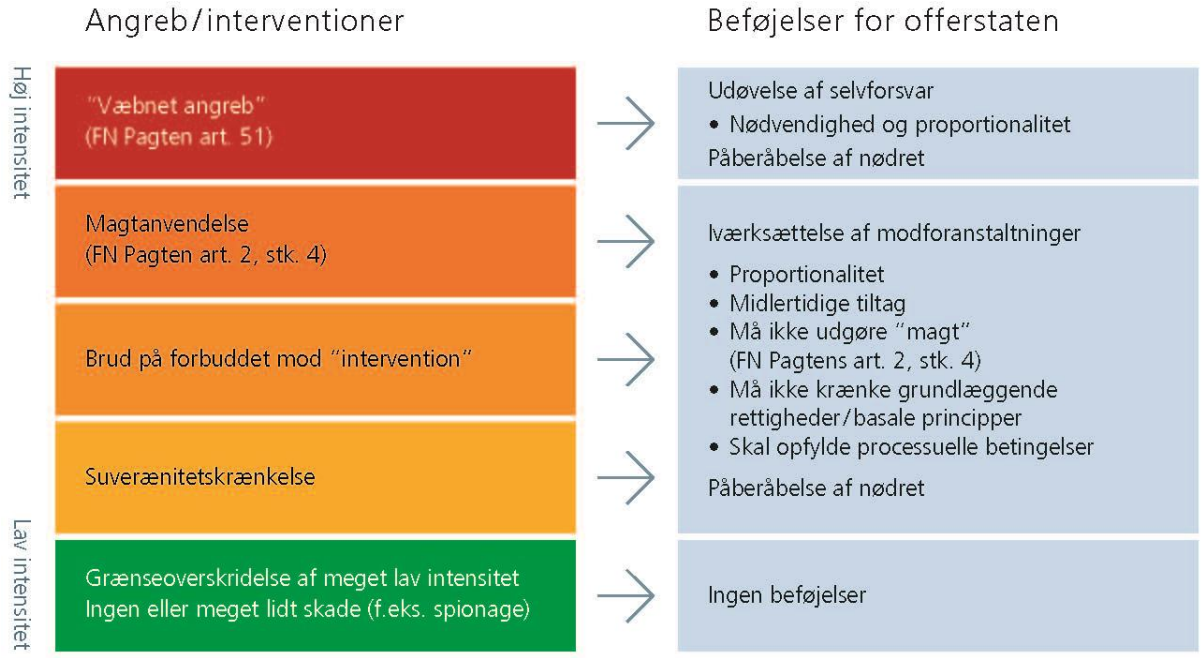
> In cases where the exact nature and, in particular, origin of a cyber incident are unclear, certain protective (cyber) measures may be justified on the basis of the plea of necessity. For example, if a State is faced with a cyber incident that endangers its essential interests and there is no other way to address the situation, it may in some cases temporarily shut off certain cyber infrastructure, even if doing so affects cyber systems in other States (sic). Similarly, if faced with significant cyber operations against a State's critical infrastructure, the plea of necessity could justify a State's resort to counter-hacking.[111]

I forhold til reaktioner i cyberspace fungerer nødretsfiguren altså på den måde, at den rent undtagelsesvis kan fritage stat A for det folkeretlige ansvar, der vil være forbundet med at foretage sig folkeretsstridige handlinger over for stat B, herunder på dennes netværk, hvis de retsstridige handlinger er nødvendige for at beskytte stat A's essentielle interesser. Det er derfor også ret oplagt, at figuren kan fungere som et ganske nødigt supplement til udøvelsen af selvforsvar og iværksættelsen af modforanstaltninger.

7. Konklusion – og anbefalinger

Cyberspace udfordrer som berørt de stater, der, som Danmark, ønsker at imødegå skadevoldende cyberaktiviteter, der udgår fra andre stater, og formålet med denne rapport har været at redegøre for de forskellige folkeretlige 'figurer', der kan være af relevans i forhold til at skabe et system, der effektivt og lovligt gør det muligt at imødegå skadevoldende aktiviteter i cyberspace uden kendskab til bagmændenes identitet eller motiver. Der er derfor blevet redegjort for staters ret til selvforsvar, de folkeretlige principper for modforanstaltninger og endelig for nødretten som en ansvarsfrihedsgrund. Disse 'figurer' er opsummeret i figur 1.

Figur 1: Folkeretlige beføjelser ('figurer') ved forskellige angrebstyper.



Gennemgangen har vist, at en velovervejet anvendelse af disse forskellige figurer – eller 'redskaber' om man vil – i teorien i hvert fald giver en stat som Danmark de fornødne *folkeretlige* beføjelser til at foretage sig de handlinger, der er nødvendige for at standse de skadevoldende aktiviteter i cyberspace, der måtte udgå fra udlandet.

Det kan på baggrund af gennemgangen konkluderes, at de danske retningslinjer for imødegåelse af skadevoldende aktiviteter i cyberspace bør være baseret på den helt oplagte præmis, at det altid er at foretrække, at Danmark ikke foretager sig handlinger i andre stater, der er at anse som krænkelser af disse staters suverænitet. Det følger som en naturlig

konsekvens heraf, at de relevante danske myndigheder altid bør *anmode de relevante stater om selv at tage de fornødne skridt* til at bringe de skadevoldende aktiviteter, der er rettet mod Danmark, der udgår fra dets territorium, til ophør. Kun i de tilfælde, hvor værtsstaten af den ene eller anden grund ikke selv standser de pågældende aktiviteter, bør de danske myndigheder selv gribe til handling.

I de tilfælde, hvor det fra dansk side skønnes nødvendigt, at danske myndigheder agerer på andre staters netværk, bør de danske tiltag så vidt muligt være baseret på en eller anden form for *samtykke fra værtsstaten*, hvormed de danske handlinger vil være forenelige med folkeretten.

Det er kun i de situationer, hvor en værtsstat *hverken selv griber ind eller tillader Danmark at gribe ind* for at standse de skadevoldende handlinger, der udgår fra dets territorium, at det fra dansk side overhovedet bør overvejes, om de relevante danske myndigheder uden samtykke bør iværksætte de tiltag, der måtte være nødvendige for at bringe aktiviteterne til ophør. Det konkrete folkeretlige grundlag for indgriben vil her afhænge af, om de skadevoldende handlinger overstiger en nedre grænse for, hvad stater skal acceptere, og om det er muligt at identificere den stat, hvorfra de pågældende aktiviteter udgår, og dermed også den stat, der forbryder sig mod sine folkeretlige forpligtelser ved at undlade at forsøge at bringe aktiviteterne til ophør, eller ej.

Hvis det *er* muligt at identificere den pågældende stat, vil de danske tiltag tage udgangspunkt i enten en ret til selvforsvar i henhold til artikel 51 i FN pagten eller – mere sandsynligt – i de folkeretlige principper om iværksættelsen af modforanstaltninger, der kan finde anvendelse i forhold til de skadevoldende aktiviteter, der er af mindre alvorlig karakter, men dog overstiger en nedre grænse. Betragtninger om proportionalitet tilsiger under alle omstændigheder, at de danske myndigheder så vidt muligt alene iværksætter tiltag, der er af samme karakter som de skadevoldende aktiviteter, de har til formål at imødegå.

Hvis det derimod *ikke* er muligt at identificere den stat, hvorfra de skadevoldende handlinger udgår, bør de danske tiltag udspringe af nødretlige betragtninger.

Det hører med til historien om den relevante folkeretlige regulering, at der fortsat er en vis uklarhed på relevante områder, og at denne uklarhed skaber praktiske problemer for de stater, der, som Danmark, ønsker at imødegå skadevoldende cyberhandlinger fra udlandet. Uklarheden er bl.a. knyttet til det forhold, at der ofte vil være uenighed blandt staterne om, hvornår en handling er "skadelig" for en anden stat, og derfor også om, hvornår

territorialstatens pligt til at standse den konkrete handling træder ind. Og selv i de tilfælde, hvor der *er* enighed om, at en cyberaktivitet er skadelig, vil der kunne være uklarhed om, hvor store krav der bør stilles til territorialstaten i forhold til at bringe aktiviteterne til ophør.

Det skal også med, at der som berørt kan være flere forhold, der gør, at en stat som Danmark vælger at afstå fra et forsøge at udnytte en folkeretlig adgang til at imødegå en skadevoldende cyberaktivitet, der måtte udgå fra udlandet. Og her spiller bl.a. risikoen for utilsigtede skadevirkninger ved modreaktioner ind.

De to sidstnævnte forhold leder frem til følgende anbefalinger:

1) Danmark bør arbejde for, at stater lever op til deres folkeretlige forpligtelse til at standse de skadevoldende cyberaktiviteter, der udgår fra deres territorier.

2) De relevante danske myndigheder bør udarbejde klare retningslinjer for, hvorledes man fra dansk side håndterer de situationer, hvor Danmark gøres til genstand for større cyberangreb fra udlandet, og hvor det må forventes, at de lokale myndigheder i værtsstaten hverken selv foretager sig det fornødne for at bringe angrebene til ophør eller giver samtykke til, at de danske myndigheder kan forsøge at standse angrebene. Det anbefales i den forbindelse, at de danske myndigheder gør brug af de folkeretlige 'figurer', der opstilles i rapporten, og skaber den fornødne grad af operationel klarhed over, hvornår danske modreaktioner, der krænker andre staters suverænitet, kan undtages i henhold til henholdsvis principperne om udøvelse af ret til selvforsvar, modforanstaltninger og nødret. Den nødvendige operationelle klarhed vil eventuelt kunne skabes i forbindelse med afholdelsen af diverse former for scenariebaserede øvelser.[112]

3) De danske politikere bør overveje, hvor voldsomme cyberangreb, vi fra dansk side er parate til at acceptere inden de relevante danske myndigheder påbegynder cyberangreb, der krænker andre staters suverænitet. Resultatet af disse overvejelser bør kommunikeres klart til de relevante danske myndigheder.

4) Eventuelle danske modreaktioner mod skadevoldende cyberaktiviteter bør så vidt muligt have samme karakter som de pågældende aktiviteter.

8. Noter

[1] For oplysninger om centret, se http://fe-ddis.dk/CFCS/Pages/cfcs.aspx

[2] Anders Henriksen (2012), *Cyberkrig, folkeretten og computer network operations*, Centre for Militære Studier, s. 5.

[3] Ibid.

[4] Se gennemgangen i Henriksen (n 2).

[5] Ibid, s. 28-29.

[6] Ibid s. 29.

[7] Center for Cybersikkerhed, *Cybertruslen mod kritisk infrastruktur*, november 2013

[8] Den megen krigsretorik, der omgærder cyberspace, er bl.a. blevet kritiseret af Mary Ellen O'Connell (2012),'Cyber Security without Cyber war', *Journal of Conflict & Security Law*, Vol 17, no. 2., 187-209.

[9] Michael N. Schmitt (2013), *The Tallinn Manual on the International Law applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge University Press. Der er ikke nævneværdige forskelle i konklusionerne i 2012-rapporten og indholdet af Tallinn-manualen.

[10] Dieter Fleck (2013), 'Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual,' *Journal of Conflict & Security Law* , Vol. 18, no. 2, s. 1-21

[11] Julian Hale, 'NATO-backed Project Explores Legal Options To Respond to Cyberattacks', *Defensenews.com*, January 23rd, 2014, http://www.defensenews.com/apps/pbcs.dll/article?AID=/201401231228/DEFREG04/301230033

[12] Ibid, s. 11. Se også Michael N. Schmitt (2012), 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', *Harvard International Law Journal*, vol. 54, s. 1-37.

[13] Privat e-mail-korrespondance.

[14] *Presidential Policy Directive /PPD-20, October 16 2012.*

[15] *United States National Military Strategy for Cyberspace Operations,* GL-1

[16] Paul Cornish m.fl. (2010), *On Cyber Warfare*, Chatham House, s. 11.

[17] Se også Nicholas Tsagourias (2012), 'Cyber attacks, self-defence and the problem of attribution', *Journal of Conflict & Security Law*, s. 5.

[18] Duncan B. Hollis (2011) "An e-SOS for Cyberspace", *Harvard International Law Journal*, Vol. 52, No. 2 s. 378.

[19] Susan W. Brenner, (2007) "'At Light Speed': Attribution and Response to Cybercrime/ Terrorism/ Warfare", *Journal of Criminal Law and Criminology*, Vol. 97, no. 2 s. 379-475. Se også Hollis (n 18) s. 374-432 og Hunker, Jeffrey, Bob Hutchinson, & Jonathan Margulies (2008), 'Role and Challenges for Sufficient Cyber-Attack Attribution', Institute for Information Infrastructure Protection, s. 7-10, January, tilgængelig på: http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf (besøgt 2. Februar 2014)

[20] Se hertil også Kristian Cedervall Lauta m.fl. (2013), 'Cyberwarfares udfordringer af begrebet kritisk infrastruktur', *Center for Militære Studier*.

[21] Se også Hollis (n 18)

[22] Se bl.a. Declaration of Independence of Cyberspace fra 1996 på https://projects.eff.org/~barlow/Declaration-Final.html

[23] Se også Jack Goldsmith (2006), *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press.

[24] Cyberrelaterede handlinger er i dag reguleret i nationale straffelove og med Europarådets konvention om cyberkriminalitet fra 2001 er handlinger i cyberspace nu også underkastet eksplicit international regulering.

[25] *Corfu Channel* (U.K. v. Alb.) 1949, ICJ Rep. 6, s. 35.

[26] Tallinn-manualen (n 9), regel 1, pkt. 5-6.

[27] Ibid, regel 1, pkt. 6.

[28] Wolff Heintschel von Heinegg (2013), 'Territorial Sovereignty and Neutrality in Cyperspace, *International Law Studies*, Vol. 89, s. 129. Se også Simon Chesterman (2006), 'The Spy who Came in from the Cold War: Intelligence and International Law', *Michigan Journal of International Law*, Vol. 27, s. 1081-1090. Folkeretten indeholder særlige regler, der har til formal at beskytte bl.a. diplomater i statslige diplomatiske repræsentationer og FN-ansatte, se bl.a. art. 27, 29-30 i Wienerkonventionen fra 1961 om diplomatiske relationer og art. 2 i FN-Konventionen fra 1946 om FN's privilegier og immunitet.

[29] Art. 20, stk. 1, i Den Internationale Lovkommissions retningslinjer for statsansvar, se hertil Generalforsamlingsresolution 56/83 af 12. december 2001. Se også Ashley S. Deeks (2012), 'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense', *Virginia Journal of International Law*, Vol. 52, s. 483-550.

[30] Ole Spiermann (2006), *Moderne Folkeret*, Jurist- og Økonomforbundets Forlag, s. 245.

[31] Til territorium henføres også statens hav og luftterritorium og skibe og fly, der er indregistreret i staten.

[32] *Island of Palmas* (Neth. V. U.S.), 2. R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928)

[33] Se hertil art. 27, stk. 1, i Wiener-konventionen fra 1961 om diplomatiske relationer.

[34] Se havretskonventionen fra 1982, artiklerne 17-26, 37-42, 45, og 52-53.

[35] Tallinn-manualen (n 9) regel 2 og 3.

[36] von Heinegg (n 28) s. 126. Se også Tallinn-manualen (n 9) regel 2, pkt. 3.

[37] *Corfu Channel* (n 22) pr. 22.

[38] Se bl.a. *Trail Smelter Case (United States, Canada)*, 16 April 1938 and 11 March 1941, Report of International Arbitral Awards, Vol. III, s. 1905.

[39] Tallinn-manualen (n 9) regel 5.

[40] Ibid, regel 5, pkt. 3.

[41] Tallinn-manualen (n 9) regel 5, pkt. 5.

[42] Se også von Heinegg (n 28) s. 136.

[43] Tallinn-manualen (n 9) regel 5, pkt. 10.

[44] Ibid, pkt. 11.

[45] von Heinegg (n 28) s. 137.

[46] Tallinn-manualen (n 9) regel 5, pkt. 12.

[47] von Heinegg (n 28) s. 138.

[48] Henriksen (n 2) s. 13-14

[49] Ibid s. 14.

[50] Ibid s. 17.

[51] Se Tallin-manual (n 9) regel 11, pkt. 8-10, og regel 13, pkt. 3.

[52] Henriksen (n 2) 2012 s. 20. Se også Tallinn-manualen (n 9) regel 14 og 15.

[53] Ibid Henriksen (n 2) 2012 s. 22. Se også Tallinn-manualen (n 9) regel 6, pkt. 10-11

[54] Ibid Tallin-manualen (n 9) regel 94, pkt. 4

[55] Se Haager-konvention V og XIII fra 1907 og folkeretlig sædvane. Reglerne finder som udgangspunkt kun anvendelse i internationale væbnede konflikter, men principperne kan uden de store vanskeligheder overføres på ikke-internationale væbnede konflikter, hvor en stat er involveret i en væbnet konflikt mod en privat aktør, se Nils Melzer (2011), 'Cyberwarfare and International Law' UNIDIR 13, s. 21, og Ashley Deeks (2013), 'The Geography of Cyber Conflict: Through a Glass Darkly', *International Law Studies*, Vol. 89, s. 8.

[56] von Heinegg (n 28), s. 143.

[57] Art. 1 og 2 i V Haagerkovention og art. 1 og 2 i XIII Haagerkonvention.

[58] Art. 5 i V Haagerkonvention.

[59] Tallinn-manualen (n 9) regel 94. Se også von Heinegg (n 28), s. 154f.

[60] Se Tallinn-manualen (n 9) regel 94, pkt. 3.

[61] Ibid pkt. 4.

[62] Henriksen (n 2) s. 24.

[63] Se bl.a. *Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ICJ Reports 2004 136, pr. 139.

[64] Se også Spiermann (n 30) s. 431-432 og gennemgangen i Anders Henriksen, *Krigens folkeret – og international væbnet terrorbekæmpelse*, Jurist- og Økonomforbundets forlag, 2010, s. 113-141.

[65] Henriksen (n 2) s. 24.

[66] Se Henriksen (n 2) s. 17-19.

[67] Ibid s. 21. Det blev dog samme sted noteret, at cyberangreb, der udgør magtanvendelse i strid med magtforbuddet i FN Pagtens art. 2, stk. 4, men ikke er tilstrækkelig alvorligt til at udgøre et 'væbnet angreb' i henhold til art. 51, ikke må gengældes med foranstaltninger af samme styrke.

[68] Se også Spiermann (n 30) s. 234.

[69] Den Internationale Lovkommissions retningslinjer for staters ansvar (n 26), art. 22. Se også *Gabcikovo-Nagymaros Project (Hungary v. Slovakia)*, ICJ Reports 1997 7, pr. 83. For en general gennemgang, se Nigel White & Ademola Abass (2010), 'Countermeasures and Sanctions', i Malcolm D. Evans, *International Law*, 3. udg., s. 531-545.

[70] *Air Services Agreement* case (1978) 54 ILR 303, s. 337

[71] Tallinn-manualen (n 9) regel 9.

[72] Se også Heather Harrison Dinniss (2012), *Cyber Warfare and the Laws of War*, Cambridge University Press, s. 107-108.

[73] Se også Henriksen (n 2) s. 21.

[74] Oona A. Hathaway m.fl (2012)., 'The Law of Cyber-Attack', *California Law Review*, vol. 100, s. 857-858, note 171.

[75] Ibid s. 858.

[76] Lovkommissionens retningslinjer for statsansvar (n 29) art. 49, stk. 1.

[77] Se også Spiermann (n 30) s. 246.

[78] Lovkommissionens retningslinjer for statsansvar (n 29), art. 49, stk. 3. Tallinn-manualen (n 9) regel 9, stk. 6.

[79] *Gabcikovo-Nagymaros Project* (n 69), pr. 87.

[80] Lovkommissionens retningslinjer for statsansvar (n 29) art. 52, stk. 3 (a). Tallinn-manualen (n 9) regel 9, stk. 3.

[81] Lovkommissionens retningslinjer for statsansvar (n 29), art. 50, stk. 1 (a)

[82] Tallinn-manualen (n 9) regel 9, stk. 5.

[83] Henriksen (n 2) s. 22.

[84] Lovkommissionens retningslinjer for statsansvar (n 29) art. 50, stk. 1 (b) – (d)

[85] Ibid, art. 50, stk. 1 (b)

[86] Art. 50, stk. 1 (c)

[87] Art. 50, stk. 1 (d)

[88] Commentary to the Draft articles on Responsibility of States for Internationally Wrongful Acts, 2001, gengivet i *Yearbook of the International Law Commission*, 2001, vol. II, Part Two, s. 132, pkt. 6-9.

[89] Lovkommissionens retningslinjer for statsansvar (n 29) art. 50, stk. 2 (b). Artikel 50, stk. 2 (a) foreskriver, at iværksættelsen af modforanstaltninger ikke fritager den udøvende stat fra eventuelle bestemmelser om bilæggelse af tvister, som staten måtte være bundet af over for den pågældende stat.

[90] Se også *Gabcikovo-Nagymaros Project* (n 69) pr. 85 og Tallinn-manualen (n 9) regel 9, stk. 7.

[91] Tallinn-manualen (n 9) regel 9, stk. 7.

[92] Thomas Franck (2008), 'On Proportionality of Countermeasures in International Law', *American Journal of International Law*, vol. 102, no. 4, s. 763

[93] White & Abass (n 69) s. 539-540.

[94] Antonio Cassese (2005), *International Law* (2. udg..), Oxford University Press, s. 306.

[95] Hathaway m.fl. (n 74) s. 858. Se også White & Abass (n 69) s. 535: "Countermeasures … are more likely to accord with the conditions of proportionality and necessity if they are so taken."

[96] DoD, Office of Legal Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, s. 19.

[97] Ibid s. 20.

[98] Lovkommissionens retningslinjer for statsansvar (n 29) art. 52, stk. 1 (a). Se også *Gabcikovo-Nagymaros Project* (n 69) pr. 84: "… the injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it."

[99] Lovkommissionens retningslinjer for statsansvar (n 29) art. 52, stk. 1 (b)

[100] Ibid art. 52, stk. 2. Se også Tallinn-manualen (n 9) regel 9, stk. 4.

[101] Katharine C. Hinkle (2011), 'Countermeasures in the Cyber Context: One more Thing to Worry About', *Yale Journal of International Law*, Vol. 37, s. 18.

[102] Hathaway m.fl. (n 74) s. 859.

[103] *Gabcikovo-Nagymaros Project* (n 69) pr. 51.

[104] Ibid.

[105] Ibid, pr. 55f.

[106] Lovkommissionens retningslinjer for statsansvar (n 29) art. 25, stk. 1.

[107] Se art. 53 i Traktatretskonventionen.

[108] Se bl.a. kritikken i Ole Spiermann (2002), 'Humanitarian Intervention as a Necessity and the Threat or Use of *Jus Cogens*', *Nordic Journal of International Law*, vol. 71, s. 523-543 og Andreas Laursen (2006), *Changing International Law to Meet New Challenges*DJØF, s. 249-254.

[109] Christine Gray (2008), *International Law and the Use of Force*, 3 udg., Oxford University Press, s. 30.

[110] Tallinn-manualen (n 9) regel 9, stk. 10-13.

[111] Ibid., pkt. 12.

[112] Se Lauta m.fl. (n 18).

9. Litteratur

Allan, Collin S. (2013), Attribution Issues in Cyberspace, Chicago-Kent Journal of International & Comparative Law, 55

Barkham, Jason (2001-2002), 'Information Warfare and International Law on the Use of Force', *New York University Journal of International Law and Politics*, vol. 34, 57

Brenner, Susan W., (2007) "'At Light Speed': Attribution and Response to Cybercrime/ Terrorism/ Warfare", *Journal of Criminal Law and Criminology*, Vol. 97, no. 2, 379.

Cassesse, Antonio (2005), *International Law* (2. udg..), Oxford University Press

Chesterman, Simon (2006), 'The Spy who Came in from the Cold War: Intelligence and International Law', *Michigan Journal of International Law*, Vol. 27, 1071

Cornish, Paul, m.fl. (2010), *On Cyber Warfare*, Chatham House

Commentary to the Draft articles on Responsibility of States for Internationally Wrongful Acts, 2001, gengivet i *Yearbook of the International Law Commission*, 2001, vol. II, Part Two, s. 132, pkt. 6-9.

Cybersikkerhed, Center for (2013), *Cybertruslen mod kritisk infrastruktur*, november

Deeks, Ashley S. (2012), 'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense', *Virginia Journal of International Law*, Vol. 52, 483

Deeks, Ashley S. (2013), 'The Geography of Cyber Conflict: Through a Glass Darkly', *International Law Studies*, Vol. 89, 1

Dinstein, Yoram (1999),'Computer Network Attacks and Self-Defense', i *Computer network attack and international law; Symposium on Computer Network Attack and International Law*, Naval War College

Dinniss, Heather Harrison (2012), *Cyber Warfare and the Laws of War*, Cambridge University Press

Electronic Frontier Foundation (1996), *Declaration of Independence of Cyberspace*, https://projects.eff.org/~barlow/Declaration-Final.html (besøgt 2. februar 2014)

Fleck, Dieter (2013), 'Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual,' *Journal of Conflict & Security Law* , Vol. 18, no. 2, 1

Franck, Thomas (2008), 'On Proportionality of Countermeasures in International Law', *American Journal of International Law*, vol. 102, no. 4, 751

Jamnajad, Maziar & Michael Wood (2009), 'The Principle of Non-intervention', *Leiden Journal of International Law*, vol. 22, 345

Goldsmith, Jack (2006), *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press.

Gray, Christine (2008), *International Law and the Use of Force*, 3 udg., Oxford University Press, s. 30.

Hale, Julian (2014), 'NATO-backed Project Explores Legal Options To Respond to Cyberattacks', *Defensenews.com*, January 23rd, http://www.defensenews.com/apps/pbcs.dll/article?AID=/201401231228/DEFREG04/301230033 (besøgt 2. februar 2014.

Hathaway, Oona A, m.fl (2012)., 'The Law of Cyber-Attack', *California Law Review*, vol. 100, 817

Healey, Jason (2012), *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, Atlantic Council, January

Henriksen, Anders (2012), *Cyberkrig, folkeretten og computer network operations*, Centre for Militære Studier, april

Henriksen, Anders (2010), *Krigens folkeret – og international væbnet terrorbekæmpelse*, Jurist- og Økonomforbundets forlag

Hinkle, Katharine C. (2011), 'Countermeasures in the Cyber Context: One more Thing to Worry About', *Yale Journal of International Law*, Vol. 37, 11

Hoisington, Matthew (2009), 'Cyberwarfare and the Use of Force Giving Rise to the Right to Self-Defense', *Boston College International & Comparative Law Review*, vol. 32, 439

Hollis, Duncan B. Hollis (2011) "An e-SOS for Cyberspace", *Harvard International Law Journal*, Vol. 52, No. 2, 374.

Hunker, Jeffrey, m.fl., 2008), 'Role and Challenges for Sufficient Cyber-Attack Attribution', Institute for Information Infrastructure Protection, January, http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf (besøgt 2. februar 2014)

International Law Commission, Draft articles on State Responsibility, se Generalforsamlingsresolution 56/83 af 12. december 2001

Kuehl, Daniel (1999) 'Information Operations, Information Warfare, and Computer Network Attack', i *Computer network attack and international law; Symposium on Computer Network Attack and International Law*, Naval War College

Laursen, Andreas (2006), *Changing International Law to Meet New Challenges*, DJØF

Lauta, Kristian Cedervall, m.fl. (2013), 'Cyberwarfares udfordringer af begrebet kritisk infrastruktur', *Center for Militære Studier*

O'Connell, Mary Ellen (2012),'Cyber Security without Cyber war', *Journal of Conflict & Security Law*, Vol 17, no. 2., 187.

Melzer, Nils (2011), 'Cyberwarfare and International Law' UNIDIR 13

Presidential Policy Directive /PPD-20, October 16 2012.

Roscini, Marco (2010), 'World Wide Warfare – Jus ad bellum and the Use of Cyber Force', *Max Planck UNYB*, 14, 85

Ryan, Julie J. C. H., Daniel J. Ryan & Eneken Tikk, 'Cyber Security Regulation: Using Analogies to Develop Frameworks for Regulation', i *International Cyber Security: Legal & policy Proceedings*, CCDCOE, 2010

Schmitt, Michael N. (2013), *The Tallinn Manual on the International Law applicable to Cyber Warfare, Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge University Press.

Schmitt, Michael N. (2012), 'International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed', *Harvard International Law Journal*, vol. 54, 1.

Spiermann, Ole (2006), *Moderne Folkeret*, Jurist- og Økonomforbundets Forlag

Spiermann, Ole (2002), 'Humanitarian Intervention as a Necessity and the Threat or Use of *Jus Cogens*', *Nordic Journal of International Law*, vol. 71, 523

United States Department of Defense, *United States National Military Strategy for Cyberspace Operations*, GL-1

Tikk, Eneken m.fl. (2010), *International Cyber Incidents: Legal Considerations*, CCDCOE

Tsagourias, Nicholas (2012), 'Cyber attacks, self-defence and the problem of attribution', *Journal of Conflict & Security Law*, 1.

von Heinegg, Wolff Heintschel (2013), 'Territorial Sovereignty and Neutrality in Cyperspace, *International Law Studies*, Vol. 89, 123.

Waxman, Matthew c. (2011), 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), *Yale Journal of International Law*, vol. 36, 421

White, Nigel & Ademola Abass (2010), 'Countermeasures and Sanctions', i Malcolm D. Evans, *International Law*, 3. Udg, Oxford University Press.

United States Department of Defense (1999), Office of Legal Counsel, *An Assessment of International Legal Issues in Information Operations*, May