KØBENHAVNS UNIVERSITET
DET JURIDISKE FAKULTET

Modforanstaltninger i cyberdomænet

Den folkeretlige ramme

Marc Schack & Astrid Kjeldgaard-Pedersen

August 2020

Kolofon

Denne rapport er en del af den forskningsbaserede myndighedsbetjening, som Det Juridiske Fakultet, Københavns Universitet, i samarbejde med Forsvarsakademiet leverer til Forsvarsministeriet og de politiske partier bag forsvarsforliget. Rapporten sætter fokus på 'modforanstaltninger', som udgør et af de centrale modsvar, Danmark inden for rammerne af folkeretten kan bringe i spil i forhold til fjendtlige cyberoperationer. Formålet med rapporten er at gøre status over de aktuelle retlige udviklinger og overvejelser på området, ligesom muligheder og begrænsninger i retten til at foretage modforanstaltninger afdækkes og analyseres.

Om InterMil-projektet: InterMil gennemfører praksisnær juridisk forskning og forskningsbaseret myndighedsbetjening inden for militære studier. InterMil-projektet er etableret ved en aftale mellem Det Juridiske Fakultet (i samarbejde med Forsvarsakademiet) og Center for Militære Studier på Københavns Universitet som led i implementeringen af forsvarsforliget 2018-2023, hvori forligskredsen har udtrykt et ønske om "øget fokus på de folkeretlige udfordringer forbundet med bl.a. deltagelse i internationale operationer, cyber, droner og højteknologiske og elektroniske kampmidler."

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

Læs mere om InterMil-projektet

Forfattere:
Adjunkt, ph.d. Marc Schack & Professor MSO Astrid Kjeldgaard-Pedersen

Masthead

This report is a part of the policy research services delivered by the Faculty of Law, University of Copenhagen, in collaboration with the Royal Danish Defence College, to the Danish Ministry of Defence and the political parties to the Defence Agreement 2018-2023. The report focuses on 'countermeasures' as one of the central responses under international law in situations where Denmark is the victim of malicious cyber operations. In light of recent developments in both the practice and theory of international law, the purpose of the report is to review and analyse the opportunities and limitations attached to the right to invoke countermeasures in response to cyber operations against Denmark.

About the InterMil project: In 2019, the Faculty of Law (in collaboration with the Royal Danish Defence College) entered into an agreement with the Centre for Military Studies on strategic research and research-based public-sector consultancy within the field of military studies. The agreement is part of the implementation of the Defence Agreement 2018-2023, which calls for an "increased focus on the challenges to international law associated with participation in international operations, cyber, drones and high tech and electronic warfare".

This report contains analyses based on legal research methodology. Its conclusions should not be understood as a reflection of the views of the Danish Government, the Danish Armed Forces, or any other authority.

Read more about the InterMil project

Authors:
Assistant Professor, Dr. Marc Schack & Professor WSR Astrid Kjeldgaard-Pedersen

ISBN: 978-87-93510-50-0

Indholdsfortegnelse

English abstract and recommendations

The cyber domain is increasingly becoming a major arena for state-on-state interactions, and at the same time digital tools and infrastructures seem to generate more and more opportunities for individuals and groups, who want to influence states. These developments entail greater risk in the digital sphere. For the foreseeable future, however, Denmark is mainly expected to face challenges in the cyber domain that fall below the legal threshold of 'armed attacks' – which, under international law, would trigger a right to self-defence. Therefore, it seems prudent to focus more intently on the modes of action available to Denmark in response to scenarios where states, non-governmental groups, and/or individuals launch cyber operations against Denmark that do not constitute 'armed attacks' but nonetheless carry the potential of causing significant damage to core Danish interests. One of the central responses allowed for under international law in such cases are 'countermeasures'. In light of recent developments in both the practice and theory of international law, this report aims to review and analyse the opportunities and limitations attached to the right to invoke countermeasures in connection with cyber operations against Denmark.

The report identifies several uncertainties about when, how, and against whom states can legally take countermeasures. A number of important questions involving, for example, the possibility of employing collective countermeasures and using countermeasures in relation to non-state actors, remain difficult to answer. Nevertheless, these challenges must be addressed in order to ensure greater stability and predictability in the cyber domain.

On that basis, we recommend that Denmark continue its active participation in relevant international fora and processes, e.g. under the auspices of the UN, which may help to solidify the law in this area. Moreover, we recommend that Denmark take further steps to contribute actively to the ongoing development by publishing 'the Danish views on international law in cyberspace', which *inter alia* should address the issues touched upon in the present report. This recommendation is based not only on Denmark's general interest in maintaining a rule-based international order that includes cyberspace. It also reflects our impression that even small states, like Denmark, are currently able to influence the development of international law in this area, and thus push these rules in a direction deemed desirable by Danish decision makers. So far, only a few states have – seemingly with good effect – been willing to present their views on the way that international law functions in cyberspace and further contributions are warranted.

Dansk resumé og anbefalinger

Cyberdomænet udgør en stadigt mere væsentlig kontaktflade mellem stater, og udviklingen af digitale værktøjer og infrastrukturer synes at skabe nye muligheder for individer og grupper, som ønsker at påvirke stater. Disse forhold medfører en øget risiko for indblanding i og kompromittering af danske myndigheders og virksomheders digitale forhold. De fleste udfordringer, som Danmark inden for overskuelig fremtid forventes at møde i cyberdomænet, ligger dog formentlig under barren for 'væbnet angreb', som efter folkeretten udløser en ret til selvforsvar. Der er derfor behov for at sætte fokus på de modreaktioner, som Danmark kan bringe i spil i scenarier, hvor stater, ikke-statslige grupper og individer iværksætter cyberoperationer mod Danmark, der ikke udgør 'væbnede angreb', men ikke desto mindre kan forvolde betydelig skade på væsentlige danske samfundsinteresser. Et af de helt centrale modsvar, som folkeretten muliggør i sådanne situationer, er 'modforanstaltninger'. På baggrund af de seneste års retlige udvikling i både teori og praksis er målet med denne rapport at gøre status over og analysere de muligheder og begrænsninger, der ligger i retten til at foretage modforanstaltninger i forbindelse med eventuelle cyberoperationer mod Danmark.

Rapporten identificerer adskillige grundlæggende uklarheder i den folkeretlige regulering af, hvornår, hvordan og mod hvem stater lovligt kan gennemføre modforanstaltninger. En række væsentlige spørgsmål, herunder vedrørende muligheden for kollektive modforanstaltninger og brug af modforanstaltninger i forhold til ikke-statslige aktører, står fortsat åbne. Disse folkeretlige udfordringer må håndteres for at sikre øget stabilitet og forudsigelighed i cyberdomænet.

Det anbefales på denne baggrund, at Danmark fortsætter sin aktive deltagelse i relevante internationale fora og processer, herunder i FN-regi, som kan bidrage til at klargøre folkerettens rolle i cyberspace. Det anbefales herudover, at Danmark bidrager aktivt til udviklingen af folkeretten på dette område ved at fremlægge sine synspunkter om folkerettens anvendelse i cyberspace, herunder vedrørende de elementer som berøres i denne rapport. Denne anbefaling beror ikke kun på Danmarks generelle interesse i at opretholde en regelbaseret verdensorden – inklusiv i cyberspace – men også på, at selv en lille stat som Danmark netop i disse år synes at have gode muligheder for at påvirke den folkeretlige udvikling i den retning, som danske beslutningstagere måtte finde ønskelig. Indtil videre har kun få stater – med relativt stor effekt – fremlagt klare, samlede juridiske analyser

af og holdninger til folkerettens anvendelse i cyberspace, og der er behov for yderligere bidrag.

1. Indledning

Da Forsvarets Efterretningstjeneste (FE) for første gang i 2004 offentliggjorde sin nu årlige sikkerhedspolitiske risikovurdering, stod der intet om cybertruslen mod Danmark[1]. Den var formentlig også beskeden på daværende tidspunkt – i hvert fald sammenlignet med de øvrige trusler fra bl.a. terrororganisationer som Al-Qaeda. Emnet blev derfor heller ikke berørt i de fem efterfølgende vurderinger, og først i 2010 begyndte FE helt kortfattet at beskrive cybertruslen. Man noterede sig dengang, at truslen "fra grupperinger og enkeltpersoner i cyberspace udgør en sikkerhedsrisiko for dansk forsvar og udsendte enheder"[2], og at det var "sandsynligt, at truslen vil udvikle sig og på langt sigt udgøre en større sikkerhedsrisiko."[3] Det må siges at have været rigtigt set – om end der ikke skulle gå lang tid, før det skærpede trusselsbillede blev en realitet. Allerede året efter, i 2011, fik cybertruslen således sit eget punkt i FE's risikovurdering og kom med i rapportens hovedkonklusioner – og siden 2012 har cybertruslen været et centralt tema i alle FE's årlige trusselsvurderinger. I 2016 begyndte FE's Center for Cybersikkerhed (CFCS) – etableret i 2012 – desuden at udgive sine egne cybertrusselsvurderinger (CTV) med mere detaljerede beskrivelser af denne specifikke trussel.

Med dette indledningsvise oprids over de danske cybertrusselsvurderinger ønsker vi blot at understrege, at mens cybertruslen ikke er et nyt fænomen – eller en negligeret trussel – er der heller ikke tale om et emne, som Danmark har haft fokus på længe. Det er en simpel pointe, som let fortaber sig her relativt få år senere, hvor cyberangreb er blevet hverdag. Vi befinder os i 2020 i en tid, hvor NATO definerer cyberspace som et operationsdomæne på linje med land, vand, luft og rummet,[4] og hvor danskerne bekymrer sig mere om, at Danmark kan blive udsat for cyberangreb end for terrorangreb.[5] Hverken Danmark eller andre lande har imidlertid haft lejlighed til at tage stilling til alle de væsentlige juridiske udfordringer, der er forbundet med cybertruslen, ligesom der fortsat blandt folkeretseksperter er udbredt uenighed om en række helt centrale spørgsmål.[6]

Med denne historik og disse iboende tvivlsspørgsmål som baggrundstæppe behandler nærværende rapport Danmarks retlige handlerum i forhold til cyberangreb, der ligger under tærsklen for et 'væbnet angreb', og derfor ikke kan imødegås med (kollektivt) selvforsvar. I sådanne situationer er den mest hårdtslående reaktion, som Danmark kan bringe i spil inden

for rammerne af folkeretten, de såkaldte 'modforanstaltninger' – defineret som handlinger, en stat under normale omstændigheder ville ifalde folkeretligt ansvar for, men som i det konkrete tilfælde er lovlige, fordi formålet med dem er at bringe en anden stats folkeretsbrud til ophør.

Rapporten gør status over de aktuelle retlige udviklinger og overvejelser på området, ligesom muligheder og begrænsninger i retten til at foretage modforanstaltninger afdækkes og analyseres. Inden vi bevæger os ind i substansen, vil vi dog først se nærmere på relevante dele af de seneste års internationale folkeretlige debat samt FE's og CFCS's efterretningsmæssige vurdering af truslen mod Danmark.

1.1 Den folkeretlige debat

Det er ikke mange år siden, at den folkeretlige debat på cyberområdet primært fokuserede på, hvordan juraen forholdt sig til egentlig 'cyberkrig'. Dengang var det centrale spørgsmål, hvornår et cyberangreb kunne udgøre et 'væbnet angreb', som berettigede brugen af væbnet magt i selvforsvar, og hvordan krigsrettens regler i øvrigt forholdt sig til det digitale domæne. Et godt eksempel på dette fokus ses i det nok mest indflydelsesrige værk om de retlige forhold i cyberdomænet: *Tallinn-manualen*. *Tallinn-manualen* har baggrund i NATO's *Cooperative Cyber Defence Centre of Excellence*, der i 2009 inviterede en gruppe uafhængige eksperter til at deltage i en proces, som skulle føre til udarbejdelsen af en manual om folkerettens rolle i cyberspace. *Tallinn-manualen* indeholder således et antal 'regler' med tilhørende kommentarer, der grundlæggende udtrykker, hvordan en række juridiske eksperter ser på den folkeretlige regulering af cyberområdet. Den første udgave af manualen (*Tallinn-manualen 1.0)* blev udgivet i 2013 og var i al væsentlighed en manual om digitalt udført krig.[7] *Tallinn-manualen 1.0* adresserede således primært spørgsmål om magtanvendelse og krigsrettens betydning i digitale sammenhænge, mens handlinger i cyberdomænet, der lå under tærsklen for væbnet magtanvendelse, ikke blev behandlet i detaljen. Det skete først med manualens andenudgave (*Tallinn-manualen 2.0*) fra 2017, som bredte emnefeltet ud til at omfatte konflikter, der foregår uden for de egentlige krigsscenarier og under tærsklen for væbnet magtanvendelse.

Udvidelsen af *Tallinn-manualens* fokus afspejler de seneste års generelle akademiske debat på området, der også i stigende grad har koncentreret sig om aktuelle praktiske udfordringer baseret på efterretningsmæssige trusselsvurderinger. Ud fra en erkendelse af, at langt størstedelen af stat-mod-stat cyberangreb foregår på et lavintensitetsniveau, udgav

eksempelvis *Chatham House* – den anerkendte, London-baserede tænketank for udenrigspolitiske forhold – i december 2019 en rapport med dette specifikke tema.[8] En central anbefaling lød her på, at stater bør sikre, at de folkeretlige debatter om, hvordan retlige normer vedrørende 'suverænitetskrænkelser' og 'ikke-intervention' finder anvendelse i cyberdomænet, føres adskilt fra overvejelser om magtanvendelse og væbnet konflikt.[9] Hermed introducerede rapporten en egentlig sondring mellem 'krigstids'-cyberjura og 'fredstids'-cyberjura.

Et af de elementer, der har fået stigende betydning i den juridiske debat, er således netop spørgsmålet om staters handlemuligheder i situationer, hvor de udsættes for cyberangreb, der ligger under tærsklen for væbnet angreb.[10] I disse sammenhænge er spørgsmålet om modforanstaltninger det mest centrale tema – og der stilles ofte spørgsmålstegn ved, hvordan modforanstaltninger fungerer i det digitale rum, ligesom det i højere grad synes at blive genovervejet, hvorvidt modforanstaltninger f.eks. kan foretages kollektivt. Det er netop et af de spørgsmål, som for nylig blev taget op af Estland og Frankrig – og hvor det viste sig, at de to NATO-allierede var helt uenige om folkerettens rammer. Mens Estland støttede en ret til kollektive modforanstaltninger, afviste Frankrig en sådan ret.[11]

Det er i forlængelse heraf vigtig at påpege, at begrebet 'modforanstaltninger' i princippet kan dække over mange forskellige handlinger, og at en af de udfordringer, der besværliggør arbejdet med modforanstaltninger, er, at begrebet mangler en klar og autoritativ definition. Selv om Den Internationale Lovkommissions (herefter 'Lovkommissionen' eller 'ILC') *Draft articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA) indeholder den væsentligste udlægning af reglerne på området, gives ingen egentlig definition.[12] Det antages dog ofte, at modforanstaltninger nødvendigvis er "fredelige" i den forstand, at de ikke involverer magtanvendelse – hvilket er et centralt krav efter ARSIWA, artikel 50, stk. 1, litra a.[13] Det er bl.a. med denne definitionsudfordring i baghovedet, at vi i afsnit 6 behandler spørgsmålet om de øvre og nedre grænser for modforanstaltninger.

Det bør desuden nævnes, at der også er emner, som vil skabe udfordringer, uanset hvilken del af konfliktspektret man beskæftiger sig med, og som således kontinuerligt har været i fokus i den folkeretlige debat. Det gælder særligt spørgsmålet om henregnelse, som også behandles løbende i FE's og CFCS's efterretningsmæssige analyser. Dette er selvsagt en væsentlig selvstændig udfordring, som bør tages i betragtning, når cyberoperationer analyseres og overvejes. Det er dog ikke et emne, som vi undersøger nærmere i denne rapport.

1.2 De efterretningsmæssige trusselsvurderinger

I FE's seneste risikovurdering fra 2019 vurderes cybertruslen at være 'blandt de mest alvorlige trusler mod Danmark og danske interesser.'[14] Desuden fremgår det af CTV'en fra 2019, at cybertruslen 'er blevet et grundvilkår for danske myndigheder og virksomheder.'[15] Der er således ingen tvivl om truslens alvor. Men det er væsentligt at understrege, at den trussel, som FE og CFCS ser for sig, ikke i første omgang handler om større, åbne konflikter på cyberområdet. De umiddelbare problemer, Danmark står overfor, består snarere i cyberspionage og cyberkriminalitet.[16] FE forklarer om førstnævnte, at '[s]tater bruger cyberspionage til den indledende kortlægning af andre staters kritiske infrastruktur', og at den viden, som opnås herved, 'efterfølgende [kan] bruges til at udføre destruktive cyberangreb, hvis en konflikt eskalerer.'[17] FE omtaler således en form for 'dual use' spionage, hvor den konkrete handling kan forstås som klassisk spionage, udført i det digitale domæne, men samtidig kan læses som et forberedende skridt mod en eskalerende konflikt. Generelt peger CFCS dog på, at truslen primært er af politisk og kommerciel karakter.[18] Det skal i den sammenhæng erindres, at spionage i folkeretten traditionelt anses for at være et område af staternes internationale relationer, der ikke er underlagt direkte folkeretlig regulering, og som således ikke er gjort til genstand for et egentligt, generelt forbud.[19] Til gengæld vil forberedende skridt mod f.eks. et væbnet angreb på et tidspunkt overskride tærsklen for et umiddelbart forestående angreb, der efter gængs opfattelse udløser en ret til selvforsvar.

Mens destruktive cyberangreb fra andre stater således formodes at være mindre sandsynlige på kort sigt, vurderer både FE og CFCS, at der sker forberedelser herpå.[20] FE understreger endvidere, at truslen kan 'ændre sig, hvis Danmark kommer i konflikt med lande, der har kapacitet til at udføre destruktive cyberangreb'[21], ligesom det påpeges, at flere lande netop opbygger en sådan kapacitet.[22] Det bør i den forbindelse bemærkes, at FE definerer begrebet 'destruktive cyberangreb' således, at det 'dækker cyberangreb med meget forskellige konsekvenser, rangerende fra slettede data til fysisk ødelæggelse.'[23] I FE's beskrivelse af denne standard peges bl.a. på det såkaldte Stuxnet-angreb, som for nogle år tilbage ramte det iranske atomanlæg i Natanz og medførte egentlige, fysiske ødelæggelser på anlægget.[24] Dette angreb må siges at udgøre den ene ekstrem i FE's definition af 'destruktive cyberangreb', og det er formodentlig det mest alvorlige cyberangreb, som vi kender til i offentligheden. Alligevel er der her tale om et angreb, som eksperterne bag *Tallinn-manualen 2.0*, ikke kunne blive enige om at kategorisere som et 'væbnet angreb' efter FN-pagtens artikel 51.[25] Med andre ord er der stor uenighed om,

hvorvidt det mest markante eksempel på et cyberangreb, vi kender til, tillod et væbnet modsvar. Selv i den mest ekstreme situation, som FE beskriver, kan reglerne om modforanstaltninger således spille en central rolle.

En anden vigtig pointe fra FE's og CFCS's trusselsvurderinger er, at truslen i høj grad synes at bestå i cyberkriminalitet begået af enkeltpersoner og fra ikke-statslige grupper – og både FE og CFCS påpeger den ofte organiserede og professionelle karakter af de cyberoperationer, som udføres af sådanne aktører.[26] Herudover er det bemærkelsesværdigt, hvordan FE og CFCS omtaler såkaldte 'statsstøttede hackergrupper'.[27] Hverken FE eller CFCS uddyber dog, hvad der ligger i statsstøtte-begrebet i denne sammenhæng. Dette til trods for at de præcise forhold i denne sammenhæng er særdeles relevante fra en retlig synsvinkel.

Det bør endelig bemærkes, at FE og CFCS løbende har påpeget en række helt grundlæggende udfordringer, som er karakteristiske for cybertruslen. Det gøres således klart, at i sammenligning med andre kontaktflader tilbyder cyberområdet unikke muligheder for at skabe usikkerhed og forvirring.[28] FE bemærker således, at netop cyberangreb er attraktive for mange aktører, fordi det kan være 'vanskeligt for ofre med sikkerhed at afgøre, hvem der står bag.'[29] Dermed formindskes risikoen for, at den angribende part rammes af et modsvar fra den angrebne part.[30] Den udfordring har været en del af FE's analyse af området helt tilbage fra 2011,[31] og den udgør fortsat en central problematik – også fra en juridisk synsvinkel.

1.3 Tidligere rapporter om folkeretten i cyberspace

Denne rapport bygger på en række områder videre på analyser, som blev præsenteret i to CMS-rapporter fra henholdsvis 2012[32] og 2014[33] om reguleringen af egentlig cyberkrig og de mulige modreaktioner, som kan foretages ved forskelligartede cyberangreb på Danmark. I 2012-rapporten, *Cyberkrig: Folkeretten og computer network operations*, behandlede Anders Henriksen særligt folkerettens regulering af magtanvendelse – *jus ad bellum* – og konkluderede, at cyberangreb efter omstændighederne kan udgøre bl.a. ulovlig intervention, magtanvendelse og endda væbnet angreb. Det understreges dog i rapporten, at det er svært at udtale sig kategorisk om disse forhold på grund af den (dengang) begrænsede retlige udvikling af området. I 2014-rapporten, *Folkeretten og modreaktioner i cyberspace*, fulgtes op herpå med en overordnet redegørelse for Danmarks beføjelser til i overensstemmelse med folkeretten at reagere på cyberangreb fra udlandet. 2014-rapporten omfattede både

suverænitetsprincippet, retten til selvforsvar, modforanstaltninger og nødret, og behandlede således – om end relativt kortfattet – emner af relevans for nærværende rapport. Der var dog på daværende tidspunkt fortsat begrænset relevant folkeretligt materiale at læne sig op ad med hensyn til cyberoperationer under tærsklen for magtanvendelse. *Tallinn-manualen 2.0* var endnu ikke udgivet, og Henriksen bemærkede derfor, med henvisning til Michael N. Schmitt, som er redaktør på *Tallinn-manualen*, at 'området ganske enkelt [var] uopdyrket.'[34] Dette synes ikke længere at være tilfældet. Siden 2014 er der ud over *Tallinn-manualen 2.0* udgivet en række akademiske bidrag, ligesom flere stater på forskellig vis har offentliggjort deres perspektiver på området. Der er derfor i dag et langt bedre fundament at arbejde ud fra, end tilfældet var i 2014, ligesom der netop nu synes at være behov for en mere dybdegående analyse specifikt af spørgsmålet om modforanstaltninger.

2. Hvad er modforanstaltninger?

Modforanstaltninger (der sommetider også kaldes "modforholdsregler" eller "repressalier") er som nævnt handlinger, som en stat under normale omstændigheder ville ifalde folkeretligt ansvar for, men som i det konkrete tilfælde er lovlige, fordi formålet med dem er at bringe en anden stats folkeretsbrud til ophør.[35]

Staters adgang til at iværksætte modforanstaltninger har historisk været og er fortsat et kontroversielt tema. I et folkeretligt system, hvor det klare udgangspunkt er, at tvistbilæggelse skal ske gennem brug af fredelige midler, må det nødvendigvis høre til undtagelserne, at folkeretsbrud retfærdiggør nye folkeretsbrud. Af samme grund voldte modforanstaltninger da også betydelige vanskeligheder for Lovkommissionen under arbejdet med statsansvarsreglerne, som ledte til vedtagelsen af ARSIWA i 2001.[36] I sin endelige udformning lyder artikel 22 i ARSIWA under overskriften 'Countermeasures in respect of an internationally wrongful act' som følger:

> The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State in accordance with chapter II of Part Three.

Det understreges i Lovkommissionens kommentar til artikel 22, at den underliggende folkeretlige forpligtelse hverken ophæves eller suspenderes. Staten er blot ansvarsfri i forhold til den pågældende forpligtelse, så længe betingelserne for lovlige modforanstaltninger, som er nærmere beskrevet i ARSIWA, artikel 49-54, er opfyldt. Modforanstaltninger indebærer dermed altid en 'standpunktsrisiko', idet en international

domstol efterfølgende kan vurdere, at de relevante betingelser ikke var opfyldt, og at staten derfor alligevel ifalder ansvar for sin folkeretsstridige adfærd.

Det fremhæves herudover i kommentaren til artikel 22, at stat A, der iværksætter modforanstaltninger over for stat B's folkeretsbrud, kun er ansvarsfri i forhold til stat B – og ikke i forhold til andre stater. Dette følger bl.a. af Den Internationale Domstols (ICJ) dom i *Gabčíkovo-Nagymaros Project* fra 1997, hvori Domstolen udtalte, at modforanstaltninger '… must be taken in response to a previous international wrongful act of another State and must be directed against that State.'[37] I det omfang modforanstaltningerne mod stat B medfører brud på stat A's folkeretlige forpligtelser over for stat C, vil stat A således ikke kunne påberåbe sig ansvarsfrihed efter artikel 22 i relation til stat C.[38]

3. Hvornår kan modforanstaltninger anvendes?

ARSIWA artikel 49-54, som udgør et selvstændigt kapitel i statsansvarsreglerne, opregner betingelserne for lovlige modforanstaltninger. Hver for sig understreger disse artikler, at det klare udgangspunkt er, at en stat ifalder ansvar for brud på sine folkeretlige forpligtelser. Med Lovkommissionens ord: 'Like other forms of self-help, countermeasures are liable to abuse and this potential is exacerbated by the factual inequalities between States.'[39] Formålet med reglerne i artikel 49-54 er på denne baggrund at etablere et operationelt system, der på den ene side tilgodeser staters behov for at have adækvate reaktionsmuligheder over for folkeretsbrud til rådighed, men på den anden side med rimelige betingelser og begrænsninger sikrer, at adgangen til at iværksætte modforanstaltninger holdes inden for acceptable rammer.

Artikel 49 udpensler således indledningsvist formålet med modforanstaltninger og begrænsningerne i deres anvendelse. Ifølge artikel 49, stk. 1, må 'offerstaten' udelukkende iværksætte modforanstaltninger over for 'gerningsstaten', dvs. den stat, der er ansvarlig for det oprindelige folkeretsbrud, med det formål at få gerningsstaten til at leve op til sine folkeretlige forpligtelser.[40] Modforanstaltninger kan således ikke anvendes som straf eller gengældelse for folkeretsbrud, men alene som et instrument til at opnå overholdelse af folkeretten.[41] En afgørende forudsætning for, at en stat kan bringe modforanstaltninger i anvendelse, er følgelig, at der kan identificeres et brud på en folkeretlig forpligtelse over for denne stat. Som nærmere beskrevet nedenfor, er dette en væsentlig del af problemstillingen i forhold til cyberangreb, der udgår fra ikke-statslige aktører, fordi der her ofte vil opstå spørgsmål om, i hvilken udstrækning de relevante folkeretlige forpligtelser påhviler andre

enheder end stater. I kommentaren til artikel 49, stk. 1, understreger Lovkommissionen, at det er en objektiv vurdering, om der har fundet et folkeretsbrud sted, som offerstaten lovligt kan reagere imod ved brug af modforanstaltninger. Offerstaten bærer således, som nævnt ovenfor, altid risikoen for, at det senere viser sig (f.eks. ved prøvelse ved en international domstol), at forudsætningerne for lovlige modforanstaltninger alligevel ikke var til stede. På det punkt adskiller modforanstaltninger sig ikke fra de øvrige ansvarsfrihedsgrunde i ARSIWA. Det ligger ifølge Lovkommissionen ligeledes i ordet 'only' i artikel 49, stk. 1, at det er en betingelse for anvendelsen af modforanstaltninger, at de rettes mod den stat, der bærer ansvaret for det relevante folkeretsbrud. Hvis offerstatens folkeretlige forpligtelse gælder over for flere stater, er det kun i relation til gerningsstaten, at offerstaten er ansvarsfri. Tredjestater og eventuelle andre tredjeparter må dog i et vist omfang tåle 'indirect or collateral effects'. Dette er, som også fremhævet i *Tallinn-manualen 2.0*, af særlig betydning i cyberdomænet, idet statslige myndigheder, private virksomheder og individer overvejende gør brug af den samme cyber-infrastruktur.[42]

Herudover foreskriver artikel 49, stk. 2, at modforanstaltninger er begrænset til midlertidig ikke-opfyldelse af offerstatens folkeretlige forpligtelser over for gerningsstaten. Bestemmelsen understreger, at formålet med modforanstaltninger ikke er straf eller gengældelse, men genopretning af en situation, hvor alle stater overholder deres respektive folkeretlige forpligtelser. Ifølge Lovkommissionens kommentar er muligheden for lovlig anvendelse af modforanstaltninger imidlertid ikke begrænset til situationer, hvor offerstaten søger at bringe gerningsstatens folkeretskrænkelse til ophør. De kan også anvendes til at opnå 'reparation' fra gerningsstaten for et folkeretsbrud, der er ophørt.[43]

Endelig følger det af artikel 49, stk. 3, at modforanstaltninger så vidt muligt skal tage en sådan form, at offerstaten efterfølgende kan genoptage opfyldelsen af sin folkeretlige forpligtelse. Blandt flere mulige lovlige og effektive modforanstaltninger skal offerstaten derfor vælge den, der i højest grad er reversibel. I ekspertgruppen bag *Tallinn-manualen 2.0* var der uenighed om, hvorvidt stater nødvendigvis skal vælge den cyber-modforanstaltning, som er lettest at 'trække tilbage' eller blot en, der faktisk er reversibel. Som eksempel nævner manualen en situation, hvor offerstaten kan vælge mellem en cyberoperation, den kan afslutte igen, og en cyberoperation, der vil kræve, at gerningsstaten skal rekonfigurere den berørte del af sin cyber-infrastruktur. Et flertal af eksperterne var af den opfattelse, at offerstaten frit kan vælge mellem de to alternativer, så længe den overholder de øvrige betingelser for lovlig iværksættelse af modforanstaltninger, herunder proportionalitetskravet, jf. nedenfor.[44]

Det følger desuden af ARSIWA, artikel 50, stk. 1, at visse grundlæggende folkeretlige forpligtelser ikke kan suspenderes i forbindelse med modforanstaltninger. Offerstater vil for det første aldrig blive ansvarsfri for brud på magtanvendelsesforbuddet. Det samme gælder overtrædelse af fundamentale menneskerettigheder og ufravigelige regler (*jus cogens*) efter den generelle folkeret. Derudover kan modforanstaltninger ikke påvirke forbud mod repressalier, der følger af den humanitære folkeret.[45]

For at fremme en mindelig løsning af den konflikt, der har givet anledning til modforanstaltningerne, følger det endvidere af artikel 50, stk. 2, at offerstater fortsat har en forpligtelse til at indgå i de procedurer for tvistbilæggelse, der måtte gælde mellem offerstat og gerningsstat. Af samme årsag ændrer iværksættelse af modforanstaltninger ikke på, at de implicerede staters diplomater og konsuler såvel som ambassader mv. er ukrænkelige.

Artikel 51 udpinder proportionalitetsprincippet, som det kommer til udtryk i forbindelse med modforanstaltninger: 'Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.' Offerstaten kan således ikke opnå ansvarsfrihed, medmindre modforanstaltningerne er proportionale med det folkeretsbrud, de har til formål at imødegå. Proportionalitetsprincippet sætter dermed en væsentlig grænse for, hvornår og med hvilke midler modforanstaltninger kan iværksættes. Ifølge Lovkommissionens kommentar til artikel 51 skal proportionalitetsvurderingen inddrage både kvantitative elementer, forstået som omfanget af den skade, offerstaten har lidt på grund af gerningsstatens folkeretsbrud, og kvalitative elementer, forstået som vigtigheden af den interesse, der beskyttes i kraft af den relevante folkeretlige regel, og alvorligheden af det konkrete brud. Med formuleringen 'the rights in question' menes ifølge kommentaren både offerstatens og gerningsstatens rettigheder, ligesom andre staters rettigheder også skal tages i betragtning i det omfang, modforanstaltningerne påvirker dem. Der ligger ikke i proportionalitetsprincippet, jf. artikel 51, et krav om gensidighed, forstået på den måde, at offerstatens modforanstaltninger skal udgøres af samme folkeretsbrud, som gerningsstaten har gjort sig skyldig i. Folkeretsbrud i form af cyberoperationer kan således besvares med modforanstaltninger uden for cyberdomænet og omvendt.[46] Det følger imidlertid af Lovkommissionens kommentar, at '[c]ountermeasures are more likely to satisfy the requirements of necessity and proportionality if they are taken in relation to the same or a closely related obligation.'[47] Ifølge *Tallinn-manualen 2.0* er stater, der ønsker at iværksætte modforanstaltninger i form af en eller flere cyberoperationer, nødt til at udvise særlig omhu i proportionalitetsvurderingen.

Hvorvidt vurderingen er fyldestgørende og inddrager alle relevante faktorer afhænger bl.a. af, om de potentielle konsekvenser af den konkrete cyberoperation var forudsigelige.[48]

Artikel 52 i ARSIWA indeholder processuelle forskrifter, som stater, der ønsker at iværksætte modforanstaltninger, skal overholde. Efter artikel 52, stk. 1, litra a, skal offerstaten først anmode gerningsstaten om at opfylde sine folkeretlige forpligtelser.[49] Sker dette ikke, skal offerstaten, jf. artikel 52, stk. 1, litra b, oplyse gerningsstaten om sin beslutning om iværksættelse af modforanstaltninger og tilbyde gerningsstaten at forhandle om problemstillingen. De to meddelelser efter henholdsvis litra a og b kan efter omstændighederne gives samtidig. Væsentligt i forhold til cyberdomænet åbner artikel 52, stk. 2, endvidere mulighed for, at stater på trods af bestemmelserne i stk. 1 kan 'take such urgent countermeasures as are necessary to preserve its rights.' Endelig følger det af artikel 52, stk. 3, at modforanstaltninger er udelukket – eller skal afbrydes uden unødigt ophold – hvis gerningsstatens folkeretskrænkelse ophører, eller hvis tvisten mellem parterne er indbragt for et prøvelsesorgan med kompetence til at træffe bindende afgørelse. Det præciseres i stk. 4, at stk. 3 ikke finder anvendelse, hvis gerningsstaten ikke implementerer den pågældende tvistbilæggelsesprocedure i god tro.

I sin kommentar til artikel 52 gentager Lovkommissionen, at modforanstaltninger er en kontroversiel selvhjælps-mekanisme – et 'nødvendigt onde' i et internationalt retssystem, hvor stater ofte ikke har adgang til et upartisk konfliktløsningsorgan, som kan prøve sagen under behørig hensyntagen til relevante retssikkershedsgarantier. Hvis mulighed for en sådan prøvelse foreligger, skal offerstaten dog som det klare udgangspunkt gøre brug heraf frem for at iværksætte modforanstaltninger, jf. artikel 52, stk. 3, litra b. I relation til cyberangreb må der imidlertid relativt ofte formodes at kunne opstå situationer, hvor stater i medfør af artikel 52, stk. 2, kan iværksætte 'urgent countermeasures' for at beskytte deres rettigheder.[50] Det er i den sammenhæng værd at bemærke, at de 'rettigheder', bestemmelsen henviser til, omfatter både de folkeretlige rettigheder, konflikten vedrører, og retten til at iværksætte modforanstaltninger.

Artikel 53 indeholder en udtrykkelig bestemmelse om, hvad der følger implicit af de øvrige artikler i ARSIWA om modforanstaltninger, nemlig at offerstaten skal bringe modforanstaltningerne til ophør så snart gerningsstaten (igen) opfylder sine folkeretlige forpligtelser. Endelig indeholder artikel 54 en såkaldt 'savings clause', der forklarer, at kapitlet om modforanstaltninger alene behandler foranstaltninger foretaget af offerstaten. Der tages således ikke stilling til andre staters mulighed for at foretage eventuelle lovlige

foranstaltninger i den sammenhæng. Denne problemstilling vender vi i det følgende afsnit 4.

4. Hvem kan anvende modforanstaltninger?

De regler, som er beskrevet ovenfor, er alene henvendt til den eller de stater, der kan defineres som offerstater efter statsansvarsreglerne, og tager ikke eksplicit stilling til situationer, hvor andre end offerstater måtte ønske at gennemføre modforanstaltninger, jf. ARSIWA artikel 54.[51] Det er derfor værd at dvæle lidt ved, først hvem der kan defineres som ofre i denne sammenhæng,[52] og dernæst hvordan forholdene er for andre stater, som måtte ønske at gennemføre modforanstaltninger. Det er særligt interessant fordi det fremgår ganske klart af omstændighederne omkring statsansvarsreglernes tilblivelse, at den manglende regulering af sidstnævnte spørgsmål ikke skal tolkes sådan, at andre modforanstaltningsscenarier er udelukket. Der er blot ikke taget stilling hertil i statsansvarsreglerne. Vi vender tilbage til den pointe nedenfor i afsnit 4.2. I det følgende klarlægges indledningsvist, hvordan de 'offerstater' – der utvivlsomt har en ret til at foretage modforanstaltninger – defineres i ARSIWA.

4.1 Offerstatens ret til modforanstaltninger

En offerstat er i statsansvarsreglernes forstand en stat, der kan siges at have lidt en skade som følge af en 'internationally wrongful act'[53] (en 'folkeretsstridig handling'). ARSIWA artikel 42 lyder som følger:

> A State is entitled as an injured State to invoke the responsibility of another State if the obligation breached is owed to:
>
> (a) That State individually; or
>
> (b) A group of States including that State, or the international community as a whole, and the breach of the obligation:
>
> (i) Specifically affects that State; or
>
> (ii) Is of such a character as radically to change the position of all the other States to which the obligation is owed with respect to the further performance of the obligation.

Som det fremgår, findes der tre situationer, hvor en eller flere stater kan siges at være 'offerstat' inden for statsansvarsreglernes system – og således tre situationer, hvor disse stater utvivlsomt opnår retten til at foretage modforanstaltninger. Den første situation, som er beskrevet i artikel 42(a), er den mest enkle: Stat A er direkte forpligtet til at overholde en

konkret folkeretlig forpligtelse over for stat B, og stat B defineres følgelig som 'offerstat', hvis stat A ikke overholder den relevante folkeretlige forpligtelse. Denne situation foreligger eksempelvis, når to stater indgår en bilateral traktat, som efterfølgende misligholdes.

De to øvrige situationer, som dækkes af artikel 42(b), handler om krænkelser af kollektive folkeretlige forpligtelser. Først behandles i artikel 42(b)(i) den situation, hvor en eller flere stater kan siges at være specifikt eller særligt påvirket af en krænkelse af en kollektiv forpligtelse, selv om de ikke er individuelt påvirkede efter artikel 42(a). Det kan f.eks. være tilfældet, hvis krænkelsen af en kollektiv forpligtelse rammer nogle stater hårdere end andre – uanset at flere stater (eller måske endda *alle* stater) i princippet rammes af krænkelsen. Et oplagt eksempel herpå, som også nævnes af Lovkommissionen, er brud på en havretlig forpligtelse til at hindre forurening af havmiljøet.[54] En misligholdelse af denne forpligtelse vil kunne have større konsekvenser for nogle stater end andre – f.eks. de stater, som ligger i nærheden af det forurenede havmiljø. Hvilke stater, der påvirkes i en sådan grad, at de kan anses for offerstater i en sådan sammenhæng, må afgøres *ad hoc* på baggrund af de konkrete omstændigheder.[55]

Noget lignende er tilfældet i den sidste situation, som beskrives i artikel 42(b)(ii). Her er der tale om krænkelser, der generelt påvirker alle de stater, som de relevante forpligtelser retter sig mod, fordi de kan siges at være så forbundne og indbyrdes afhængige, at gensidig overholdelse må forstås som en betingelse. Lovkommissionen nævner som eksempel herpå nedrustningsaftaler, der i sagens natur som oftest er baseret på gensidighed.[56] I hvilken udstrækning specifikke folkeretlige aftaler kan siges at indebære et tilstrækkeligt gensidighedselement til at være omfattet af artikel 42(b)(ii) beror på en konkret vurdering.

På trods af, at der altså kan være uklare grænser for, hvornår stater defineres som offerstater i tilfælde, hvor de ikke er individuelt ramt af en krænkelse, er det vigtigt at holde sig for øje, at Lovkommissionen havde til hensigt at skabe en relativt skarp adskillelse mellem sådanne offerstater, som defineres i artikel 42, og de stater, der "blot" har en retlig interesse i overholdelsen af den relevante retlige forpligtelse – men altså ikke eksplicit er tildelt en ret til at iværksætte modforanstaltninger.[57] Sidstnævnte stater beskrives således i artikel 48, stk. 1:

> 1. Any State other than an injured State … if:
>
> (a) The obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or
>
> (b) The obligation breached is owed to the international community as a whole.

Som det fremgår, anses en generel retlig interesse i overholdelsen af forpligtelser at foreligge i tilfælde, hvor forpligtelsen enten rettes mod en gruppe af stater, eller hvor forpligtelsen rettes mod det internationale samfund som helhed. Sådanne forpligtelser betegnes ofte som henholdsvis *erga omnes partes* og *erga omnes* forpligtelser. Tilbage står dog spørgsmålet, om der er tilfælde, hvor stater, der blot har en generel retlig interesse i en folkeretsstridig handling, også kan iværksætte modforanstaltninger over for gerningsstaten. En sådan ret fremgår ikke af statsansvarsreglerne, men spørgsmålet blev debatteret heftigt af Lovkommissionen og Generalforsamlingens 6. Komite, da reglerne blev udarbejdet – og det er fortsat til debat.[58] Problemstillingen kan grundlæggende koges ned til, om der findes situationer, hvor stater har en ret til at udøve 'kollektive' modforanstaltninger,[59] i situationer hvor en *erga omnes (partes)* norm krænkes. Nedenfor giver vi vores bud.

4.2 Debatten om kollektive modforanstaltninger

Muligheden for i overensstemmelse med folkeretten at iværksætte kollektive modforanstaltninger har i stigende grad været til debat i de senere år. I grove træk omhandler problemstillingen to typer af scenarier: Det ene scenarie er situationer, hvor tredjestater måtte ønske at gennemføre modforanstaltninger for at bistå en offerstat, der har været udsat for en krænkelse – ofte på baggrund af en anmodning eller opfordring fra offerstaten. Det andet scenarie er situationer, hvor der ikke nødvendigvis findes en egentlig offerstat, fordi den ulovlige handling er foregået inden for en enkelt stats grænser. Det omfatter tilfælde, hvor en stat begår folkeretsstridige overgreb mod egne borgere, eller hvor en større konflikt udspiller sig mellem grupperinger inden for en stats territorium, og hvor sådanne forhold giver anledning til en reaktion fra andre stater. Førstnævnte scenarie har således en vis parallelitet til reglerne om kollektivt selvforsvar, som reguleres i FN-pagtens artikel 51, mens sidstnævnte mere ligner de forhold, vi kender fra debatten om humanitær intervention.

4.2.1 Lovkommissionens udarbejdelse af statsansvarsreglerne (ARSIWA)

Debatten om kollektive modforanstaltninger tager ofte sit udgangspunkt i det arbejde, som blev udført af Lovkommissionen og Generalforsamlingens 6. Komite i forbindelse med udarbejdelsen af ARSIWA. Her diskuterede man nemlig – særligt i slutningen af processen – hvorvidt statsansvarsreglerne skulle indeholde regler om kollektive modforanstaltninger. Det var oprindeligt planen, men bl.a. på grund af skepsis blandt medlemslandene blev en sådan regulering udeladt. I stedet findes blot en såkaldt "savings clause" i ARSIWA artikel

54, som grundlæggende indeholder en beslutning om ikke at beslutte noget på området. Af artikel 54, som afrunder statsansvarsreglernes kapitel om modforanstaltninger, fremgår det således at:

> This chapter does not prejudice the right of any State, entitled under article 48, paragraph 1, to invoke the responsibility of another State, to take lawful measures against that State to ensure cessation of the breach and reparation in the interest of the injured State or of the beneficiaries of the obligation breached.

Bestemmelsen siger altså blot, at reglerne i kapitlet ikke har til formål at afgøre spørgsmålet om, hvorvidt tredjestater i forbindelse med brud på *erga omnes (partes)* normer har ret til at iværksætte lovlige foranstaltninger imod den krænkende stat. Det har med andre ord siden vedtagelsen af ARSIWA i 2001 været et åbent spørgsmål, om folkeretten tillader kollektive modforanstaltninger – og i den debat synes skeptikerne at have fyldt mest.[60]

4.2.2 Cyberområdet som fokus for debatten

I de senere år er cyberområdet blevet den måske vigtigste ramme for debatten om kollektive modforanstaltninger. Den udbredte skepsis reflekteres bl.a. af *Tallinn-manualen 2.0*, hvor et flertal af de deltagende eksperter fandt, at modforanstaltninger, som blev foretaget 'on behalf of another State', var ulovlige.[61] Flertallet mente øjensynligt, at ICJ's dom i *Nicaragua*-sagen[62] måtte føre til, at kollektive modforanstaltninger er ulovlige, ligesom man henviste til Lovkommissionens vurdering af den begrænsede statspraksis.[63] Et mindretal fandt dog, at kollektive modforanstaltninger kunne være lovlige i situationer, hvor en offerstat har anmodet om bistand.[64] Selv om spørgsmålet om kollektive modforanstaltninger således indgår i *Tallinn-manualen 2.0*, er det dog vigtigt at påpege, at manualens behandling heraf er relativt kortfattet, og at de fremlagte rationaler læner sig tungt op ad traditionelle opfattelser, som tilsyneladende ikke er blevet udviklet siden 2001. Dette til trods for at der på tidspunktet fra manualens udarbejdelse allerede var gennemført en række studier, der anfægter den gængse tilgang.[65]

I 2019 tog både Estland og Frankrig eksplicit stilling til spørgsmålet om kollektive modforanstaltninger i deres respektive udmeldinger om folkeretten i cyberspace. De to NATO-allierede nåede, som også nævnt ovenfor, til hver sin modsatrettede konklusion. I maj 2019 argumenterede Estlands præsident, Kersti Kaljulaid, således for, at stater, 'which are not directly injured may apply countermeasures to support [a] state directly affected by [a] malicious cyber operation.'[66] Nogle få måneder senere frigav det franske Ministerium for De Væbnede Styrker et notat, hvori det franske syn på folkeretten i cyberspace blev

udfoldet.[67] Heraf fremgik det, at kun offerstater kan anvende modforanstaltninger.[68] Disse udtalelser har skubbet til den folkeretlige debat om modforanstaltninger, men debatten er fortsat fastlåst af de traditionelle rationaler, som bl.a. fremgår af *Tallinn-manualen 2.0*. Der er imidlertid grund til at genoverveje kerneargumenterne bag disse rationaler. Ved nærmere eftersyn synes flere af de centrale indvendinger imod kollektive modforanstaltninger nemlig mindre problematiske end hidtil antaget – særligt i forbindelse med kollektive modforanstaltninger, som foretages på baggrund af en anmodning fra offerstaten. Nedenfor overvejes derfor følgende spørgsmål:

1) Er ICJ's dom i *Nicaragua*-sagen så afvisende overfor kollektive modforanstaltninger, som det forudsættes i bl.a. *Tallinn-manualen 2.0*?
2) Er den tilgængelige statspraksis på området så begrænset, som det ofte antages?
3) Var de stater, som deltog i udarbejdelsen af statsansvarsreglerne, så skeptiske overfor retten til kollektive modforanstaltninger, som det traditionelt antages?

4.2.3 Synet på kollektive modforanstaltninger i *Nicaragua*-sagen

At *Nicaragua*-sagen spiller så stor en rolle i debatten om kollektive modforanstaltninger skyldes, at det er den eneste dom fra ICJ, der forholder sig eksplicit til emnet. I sin kerne handlede sagen om USA's forskellige former for indblanding – fra relativt banale suverænitetskrænkelser til egentlig magtanvendelse – i Nicaraguas interne forhold.[69] USA argumenterede ved ICJ for, at man med sine handlinger i Nicaragua blot havde udøvet en ret til kollektivt selvforsvar af Nicaraguas nabolande, der havde været udsat for en række krænkelser (under tærsklen for 'væbnet angreb') fra Nicaraguas side.[70] Det argument afviste domstolen dog bl.a. med henvisning til, at Nicaraguas nabolande slet ikke havde anmodet USA om at yde bistand,[71] og at en sådan anmodning var nødvendig for at kunne retfærdiggøre anvendelsen af magt.[72] USA præsenterede ikke andre argumenter for domstolen, men dommerne overvejede ikke desto mindre om bl.a. en ret til kollektive modforanstaltninger kunne anvendes. Den mulighed blev dog afvist med følgende formulering:

> The acts of which Nicaragua is accused … could only have justified proportionate counter-measures on the part of the State which had been the victim of these acts, namely El Salvador, Honduras or Costa Rica. They could not justify counter-measures taken by a third State, the United States, and particularly could not justify intervention involving the use of force.[73]

Skeptikere over for retten til kollektive modforanstaltninger har ofte tolket denne formulering og andre elementer i dommen som en eksplicit og generel afvisning af en sådan ret.[74] Men

deres læsning kan udfordres. Dels havde Nicaraguas naboer netop ikke i situationen anmodet USA om bistand, hvilket indebar, at USA slet ikke kunne påstå at have ret til at handle på deres vegne. Dermed bliver det i hvert fald svært at hævde, at dommen indeholder en egentlig afvisning af en ret til at udøve kollektive modforanstaltninger på anmodning fra offerstaten, da den manglende anmodning var af afgørende betydning i sagen. Herudover var det spørgsmål, som domstolen behandlede i sammenhængen primært USA's brug af væbnet magt, som jo i alle tilfælde falder uden for en eventuel ret til at foretage modforanstaltninger. Disse forhold synes at svække *Nicaragua*-dommens relevans for spørgsmålet om, hvorvidt kollektive modforanstaltninger kan være lovlige i situationer, hvor en offerstat har anmodet om bistand, og hvor sagen ikke omfatter magtanvendelse.[75]

Denne vurdering står vi ikke alene med. James Crawford, som var *special rapporteur* for Lovkommissionens arbejde med statsansvarsreglerne i perioden 1997-2001, har ligeledes lagt vægt på, at domstolen i *Nicaragua*-sagen ikke tog stilling til, hvordan situationen havde set ud, hvis der havde foreligget en anmodning fra en offerstat.[76] Jonathan Charney vurderer samstemmende, at domstolens analyse af kollektive modforanstaltninger blot indebar et forbud mod kollektive modforanstaltninger i situationer, hvor der ikke er afgivet anmodning fra offerstaten.[77] En lignende konklusion kan desuden findes i Samuli Haataja's artikel om kollektive modforanstaltninger mod cyberoperationer, mens Przemyslaw Roguski i en artikel om samme emne helt vælger at ignorere afgørelsen.[78] Det er således langt fra sikkert, at ICJ i *Nicaragua*-dommen reelt mente, at kollektive modforanstaltninger skulle være ulovlige *per se*. En mere retvisende forståelse synes at være, at en række omstændigheder i den konkrete sag gjorde sådanne handlinger ulovlige – herunder brugen af væbnet magt og den manglende anmodning om bistand fra offerstaterne. Under alle omstændigheder synes det rimeligt på baggrund af usikkerheden om domstolens perspektiv at være tilbageholdende med at drage for vidtgående konklusioner.

4.2.4 Den tilgængelige statspraksis

Det næste spørgsmål, som angår forståelsen af den tilgængelige statspraksis, har ligeledes været et centralt tema i debatten om kollektive modforanstaltninger. Det kan bl.a. udledes af *Tallinn-manualen 2.0*, hvori flertallet som et kerneargument imod retten til kollektive modforanstaltninger påpeger, at Lovkommissionen i sin analyse af emnet nåede til den konklusion, at statspraksis var 'sparse and involves a limited number of States.'[79] Der er dog grund til at stille spørgsmålstegn ved denne vurdering – samt til at opdatere analysen.

Det er for det første bemærkelsesværdigt, at Lovkommissionens analyse fremstår relativt usammenhængende. Den består grundlæggende af en kortfattet gennemgang af situationer, der alle synes at illustrere staters villighed til at udføre kollektive modforanstaltninger i forskellige sammenhænge. Efter denne gennemgang afsluttes analysen imidlertid med en kort konstatering af, at praksis på området er begrænset og ikke kan føre til, at der kan identificeres en klar ret til at foretage kollektive modforanstaltninger.[80] Analysen er påfaldende, fordi den alene peger på statspraksis, der taler *for* en ret til kollektive modforanstaltninger – og blot omtaler disse som *eksempler* fra praksis – og på denne baggrund finder, at relevant praksis er for begrænset, uden i øvrigt at fremlægge nogen klar argumentation herfor, endsige eksplicitte overvejelser, der understøtter en sådan afvisning af en ret til kollektive modforanstaltninger. Der henvises eksempelvis intet sted til situationer, hvor stater har udtrykt skepsis over for denne praksis, ligesom der ikke henvises til andre forhold, der kunne pege i en sådan negativ retning. Øjensynligt har Lovkommissionen ment, at der ikke fandtes anden væsentlig og relevant praksis end de situationer, kommissionen fremhæver – og at det forhold må føre til den konklusion, at praksis er yderst begrænset. Alt i alt synes analysen derfor relativt usammenhængende. Forklaringen herpå skal formentlig findes i det forhold, at analysen bygger på en gennemgang af praksis, som oprindelig blev foretaget af *Special Rapporteur* James Crawford i hans tredje rapport om statsansvar.[81] Crawfords gennemgang er i lange stræk identisk med Lovkommissionens endelige analyse, men ender med en næsten modsatrettet konklusion. Mens Crawford ganske vist på linje med Lovkommissionen vurderer, at praksis på området ikke tillader klare konklusioner, noterer han alligevel, at den identificerede praksis peger i retning af en kollektiv ret til at udføre modforanstaltninger.[82] Med visse forbehold konkluderer Crawford således, at der i statspraksis findes 'support for the view that a State injured by a breach of a multilateral obligation should not be left alone to seek redress for the breach.'[83] Denne konklusion passer alt andet lige bedre med den identificerede praksis end Lovkommissionens konklusion, hvilket kan siges at svække anvendeligheden af Lovkommissionens analyse. Det er endvidere bemærkelsesværdigt, at flere juridiske eksperter de senere år har identificeret langt mere statspraksis, end Lovkommissionens analyse inddrager. Disse eksperter når desuden ofte frem til helt andre konklusioner end Lovkommissionen. Hvor Lovkommissionens analyse af statspraksis således omfatter 8 situationer, identificerer Jarna Petman i sin analyse fra 2004 i alt 14 situationer af relevans for spørgsmålet. Petman når desuagtet til samme resultat som Lovkommissionen, baseret på en lignende logik.[84] Efterfølgende har en række studier

imidlertid identificeret endnu mere praksis, og her konkluderes, modsat Lovkommissionen og Petman, at den identificerede praksis kan understøtte en ret til kollektive modforanstaltninger i visse sammenhænge. På grund af forskelle i disse studiers fokus, analysemetode og konkrete retlige vurderinger er der variationer i deres analyser – men de peger alle i samme retning.

Christian J. Tams identificerer således i 2005 i alt 17 situationer af relevans for spørgsmålet. Dette materiale kan, ifølge Tams, siges at tale for lovligheden af kollektive modforanstaltninger, og at han vurderer, at den identificerede praksis 'certainly contradicts the widely held view that countermeasures could only be taken by individually injured States.'[85] Tams kalder på denne baggrund Lovkommissionens og James Crawfords konklusioner for 'over-cautious'.[86] Når det gælder situationer, der involverer systematiske eller alvorlige overtrædelser af folkeretlige *erga omnes* normer, finder Tams således, at der synes at være 'a settled practice of countermeasures by States not individually injured.'[87]

En lignende analyse findes hos Elena Katselli Proukaki, som i 2010 udkom med en bog om udfordringerne ved at håndhæve folkeretten.[88] I bogen foretager Proukaki en analyse af den tilgængelige statspraksis, og hun identificerer her hele 37 forløb, som hun mener enten illustrerer brugen af kollektive modforanstaltninger – eller på anden måde underbygger hendes konklusion om, at det findes en hel del praksis, som understøtter en ret til at tage kollektive modforanstaltninger. Proukaki finder således, at brugen af kollektive modforanstaltninger 'is well developed by state practice and *opinio juris*, satisfying the essential legal requirements for the claim that a customary rule of international law on the right to solidarity measures has now come into existence.'[89] Med andre ord finder Proukaki et sædvaneretligt grundlag for kollektive modforanstaltninger.

Endelig finder Martin Dawidowicz i sin bog fra 2017 om kollektive modforanstaltninger, at i hvert fald 21 situationer illustrerer deres anvendelse i forskellige sammenhænge.[90] Over 125 sider gennemgår Dawidowicz disse situationer og konkluderer, at analysen 'strongly suggests that State practice on third-party countermeasures can today hardly be described as neither limited nor embryonic.'[91] Med disse formuleringer peger han direkte på Lovkommissionens konklusioner, som han ikke kan genkende, da statspraksis efter hans opfattelse er langt mere udbredt og repræsentativ, end Lovkommissionen formodede.[92] Dawidowicz bemærker desuden, at de beskrevne situationer kun førte til relativt få og beskedne protester.[93] På den baggrund konkluder han, at der findes betydelig støtte for, at kollektive modforanstaltninger er 'permissible under international law.'[94]

De beskrevne værker identificerer således i alt 44 situationer, der hver for sig synes at styrke tanken om, at kollektive modforanstaltninger kan være tilladelige efter folkeretten. I flere af disse situationer indgår desuden dansk praksis – som dog oftest udgør en del af en samlet EU-tilgang til konkrete udfordringer. Et eksempel herpå er den situation, der opstod i 1982, da Argentina forsøgte at erobre Falklandsøerne fra Storbritannien. Her anmodede briterne sine (dengang) EF-allierede om bistand til at bekæmpe det argentinske pres gennem vedtagelsen af sanktioner. EF-medlemmerne, herunder Danmark, vedtog på denne baggrund en sanktionspakke, hvor man bl.a. forbød al import fra Argentina, uanset gældende GATT-forpligtelser og eksisterende handelsaftaler.[95] Disse sanktioner udgjorde umiddelbart et brud på EF-medlemslandenes folkeretlige forpligtelser over for Argentina,[96] og det er således bemærkelsesværdigt, at den officielle argumentation for deres lovlighed var, at de blev iværksat på baggrund af medlemslandenes 'inherent rights', som bl.a. reflekteret i GATT-aftalens undtagelser om national sikkerhed.[97] Med andre ord var Danmark en del af en gruppe af lande, der argumenterede for, at der gælder visse iboende folkeretlige rettigheder, som understøtter muligheden for at foretage kollektive modforanstaltninger – omend det aldrig blev gjort klart, hvad det præcist indebar.

4.2.5 Staters skepsis under udarbejdelsen af Statsansvarsreglerne

En væsentlig del af den tilbageholdenhed over for kollektive modforanstaltninger, som vi fortsat oplever i dag, kan formodentlig tilskrives, at en række stater udtrykte sig stærkt skeptisk i Generalforsamlingens 6. Komité i forbindelse med udarbejdelsen af statsansvarsreglerne. Navnlig har James Crawfords og Lovkommissionens udlægning af diskussionen i 6. Komité været betydningsfuld, idet de pågældende staters udtalelser tilsyneladende var den afgørende årsag til, at en bestemmelse, som eksplicit tillod kollektive modforanstaltninger, blev fjernet. I artikel 54 i et 2000-udkast til ARSIWA foreskrev stk. 1 en ret til at udøve kollektive modforanstaltninger på anmodning fra en offerstat, mens der i stk. 2 var formuleret en ret til at udøve kollektive modforanstaltninger i andre tilfælde – ved særligt alvorlige brud på *erga omnes* forpligtelser.[98] Som følge af staternes kritiske udtalelser i den 6. Komite blev bestemmelsen dog fjernet og erstattet af den ovenfor omtalte "savings clause", som groft sagt indeholder en beslutning om ikke at beslutte noget om kollektive modforanstaltninger.[99] I den sammenhæng er det værd at bemærke, at James Crawford dengang vurderede, at '[t]he thrust of Government comments [was] that article 54, and especially paragraph 2, ha[d] no basis in international law and would be destabilizing.'[100] Lovkommissionen nåede frem til en lignende konklusion.[101] Selv om Crawford således

erkendte, at den oprindelige artikel 54 måtte fjernes, mente han ikke, at man blot kunne slette artiklen, fordi 'the mere deletion of article 54 [would] carry the implication that countermeasures can only be taken by injured States, narrowly defined.'[102] Ifølge Crawford ville dette give et misvisende billede af den folkeretlige sædvaneret, og en "savings clause" var derfor efter hans opfattelse nødvendig – og der endte debatten om kollektive modforanstaltninger således i den omgang.[103]

Som bl.a. Christian Tams dog påpeger, har Crawford måske været for forsigtig i sin læsning af staternes udtalelser i 6. Komité, hvilket har ledt ham til at konkludere for kategorisk med hensyn til deres skepsis. F.eks. er det interessant, at staterne bredt set ikke gav udtryk for en markant skepsis, da de i slutningen af 1990'erne debatterede et tidligere udkast til ARSIWA, der også tillod kollektive modforanstaltninger.[104] Herudover er det bemærkelsesværdigt, at endog forholdsvis mange stater synes at have støttet eller accepteret en ret til kollektive modforanstaltninger under de afsluttende debatter om ARSIWA – selv om der ganske vist også var en række stater, der enten udtrykte skepsis eller afviste tanken.[105]

Gennemgår man således staternes udtalelser fra denne periode, som bl.a. Christian Tams har gjort det, finder man, at der øjensynlig var flere stater, der støttede de foreslåede bestemmelser i udkastets artikel 54, end der var stater, der afviste bestemmelserne.[106] Tams konkluderer da også på den baggrund, at Crawfords vurdering 'seems rather difficult to sustain.'[107] For Danmarks vedkommende er det i den forbindelse værd at bemærke, at vi sammen med de øvrige nordiske lande spillede en aktiv og støttende rolle i debatten om kollektive modforanstaltninger, og at det var Danmark, der førte pennen, da de nordiske lande den 5. februar 2001 indgav skriftlige kommentarer til 2000-udkastet. Her argumenterede de nordiske lande for, at det foreslåede kapitel om modforanstaltninger, herunder artikel 54, 'contains all the essential elements for regulating this most sensitive issue and it is placed in the right context of implementing State responsibility'.[108] Senere, da det stod klart, at udkastet var forkastet, og at artikel 54 skulle erstattes af en "savings clause", roste Finland, på vegne af de nordiske lande, '[the] efforts to establish a public law enforcement system in the case of a breach of obligations owed to the international community as a whole.'[109] Man noterede sig desuden, at '[a]lthough unfortunately reduced to a simple saving clause, article 54, on measures by States other than an injured State, did go some way towards recognizing the principle that all States were entitled to take countermeasures in case of a violation of an obligation owed to the international community as a whole.'[110] Med disse ord synes de nordiske lande at have udtrykt støtte til ideen om en

ret til kollektive modforanstaltninger – og til tanken om, at processen bag statsansvarsreglerne peger i retning af en anerkendelse af en sådan ret ved brud på *erga omnes* normer.

Udover Crawfords øjensynlige overvurdering af staternes skepsis, bør det også bemærkes, som bl.a. påpeget af Martin Dawidowicz, at der findes visse modsætninger mellem, hvad nogle stater sagde under debatten om statsansvarsreglerne, og hvordan de rent faktisk har handlet i praksis.[111] En meget skeptisk stat som Israel har eksempelvis anmodet allierede om at udføre *prima facie* kollektive modforanstaltninger bl.a. i forbindelse med Libyens støtte til anti-israelske terrorgrupper i 1970-80, ligesom to andre skeptiske stater, Cuba og Mexico, begge tog del i de *prima facie* kollektive modforanstaltninger, der blev gennemført mod den Dominikanske Republik i 1960.

Endelig er det værd at bemærke, at staterne var langt mindre kritiske over for muligheden for kollektive modforanstaltninger efter anmodning fra en offerstat, end i tilfælde hvor en sådan anmodning ikke forelå.[112]

På denne baggrund synes der at være et vist rum for fortolkning i forhold til en eventuel ret til at foretage kollektive modforanstaltninger på anmodning fra en offerstat, og det synes muligt at anlægge en tilgang, som ser mere positivt på en sådan ret end den hidtil gængse opfattelse. Vi befinder os desuden på nuværende tidspunkt i en situation, hvor der er stigende opmærksomhed på dette spørgsmål – ikke mindst i forbindelse med debatten om folkerettens rolle i cyberspace – samtidig med, at kun få stater indtil videre har givet eksplicit udtryk for deres holdning. Som også modtagelsen af Estlands udtalelser om spørgsmålet vidner om, synes der således netop nu at være en enestående mulighed for at påvirke den retlige udvikling.

4.3 Kun stater har ret til at anvende modforanstaltninger

Som afrunding af nærværende afsnit bør det understreges, at retten til at foretage modforanstaltninger, herunder eventuelt kollektive modforanstaltninger, er forbeholdt stater. Der findes næppe støtte i folkeretten til, at ikke-statslige aktører selvstændigt kan påberåbe sig modforanstaltninger som ansvarsfrihedsgrund. Det kan forekomme at være en oplagt konklusion, som måske ikke behøver nærmere uddybning. På cyberområdet er det imidlertid et vigtigt element at holde sig for øje, da det ofte vil være sådan, at større virksomheder udsættes for cyberangreb, og at de ofte selv vil være bedst i stand til at udføre effektive modforanstaltninger. Selv om det derfor kan være fristende for en større virksomhed, der

udsættes for cyberangreb – eller for de cybersikkerhedsfirmaer, der ansættes til at håndtere denne trussel – f.eks. at blokere et angreb ved at nedlægge servere i udlandet, eller gengælde angreb igennem *prima facie* ulovlige handlinger foretaget i udlandet, findes der i dag ingen selvstændig folkeretlig ret til at gøre noget sådant.[113] Omvendt vil den type handlinger udført af virksomheder som oftest ikke udgøre en selvstændig krænkelse af folkeretten,[114] men snarere rejse spørgsmål om virksomhedens hjemlands 'due diligence'-forpligtelser over for det ramte land.[115]

Det er i forlængelse heraf værd at bemærke, at det står stater frit for at købe ydelser fra private virksomheder – også i forbindelse med statens cybersikkerhed. Det indebærer, at stater principielt har ret til at delegere i hvert fald dele af sin cybersikkerhed til private virksomheder, der således på statens vegne vil kunne udføre modforanstaltninger. Det vil dog i sådanne sammenhænge formelt være staten og ikke den private virksomhed,[116] der foretager modforanstaltninger. Alle krav og forpligtelser, der påhviler staten, vil derfor fortsat skulle iagttages. I det hele taget findes ingen klar regulering af dette område, og uden for situationer reguleret af særlovgivning (f.eks. i forbindelse med en væbnet konflikt) vil der være relativt få begrænsninger i staters mulighed for at engagere private virksomheder til at udføre modforanstaltninger.

5. Mod hvem kan modforanstaltninger anvendes?

Der er, som netop omtalt, udbredt enighed om, at det kun er stater, der kan påberåbe sig modforanstaltninger som grundlag for ansvarsfrihed for folkeretsbrud. Som modstykke hertil er der tilsvarende enighed om, at modforanstaltninger udelukkende kan rettes mod stater. Den gennemgående konsensus hænger naturligt sammen med, at reglerne om modforanstaltninger i ARSIWA, som det udtrykkeligt fremgår af artikel 22, kun omhandler forholdet mellem stater. Det følger således eksplicit af artikel 49, stk. 1, at modforanstaltninger kun rettes mod den stat, der bærer ansvaret for det relevante folkeretsbrud, idet tredjestater og eventuelle andre tredjeparter i en vis udstrækning må finde sig i 'indirect or collateral effects'.[117]

Spørgsmål om modforanstaltninger opstår med andre ord kun mellem offerstat og gerningsstat, og det er kun i tilfælde, hvor en gerningsstat på nærmere bestemte måder er involveret i en ikke-statslig aktørs handlinger, at modforanstaltninger som ansvarsfrihedsgrund kan komme på tale. Det er disse nærmere bestemte måder, der er temaet for dette afsnit.

Den folkeretlige debat har primært fokuseret på, hvad der skal til, før en offerstat lovligt kan iværksætte modforanstaltninger over for en værtsstat, forstået som en stat fra hvis territorium en ikke-statslig aktør gennemfører cyberoperationer rettet mod offerstaten. Mere præcist diskuteres det, 1) hvornår en ikke-statslig aktørs handlinger kan henregnes til værtsstaten, således at værtsstaten ifalder folkeretligt ansvar, og 2) hvornår værtsstaten i overensstemmelse med "due diligence-princippet" er forpligtet til at sikre, at folkeretsstridige cyberoperationer ikke udgår fra dens territorium.

5.1. Hvornår kan ikke-statslige aktørers folkeretsbrud henregnes til staten

Reglerne om henregnelse af handlinger til en stat er beskrevet i kapitel 2 i ARSIWA. I relation til cyberoperationer udført af ikke-statslige aktører er det især reglerne i artikel 8 og artikel 11, der påkalder sig interesse. Udgangspunktet er, at handlinger udført af private – individer såvel som grupper – ikke henregnes til staten.[118] Men det følger af artikel 8, at ikke-statslige aktørers handlinger skal henregnes til en stat, hvis den ikke-statslige aktør handler 'on the instructions of, or under the direction or control of' den pågældende stat. Ifølge Lovkommissionens kommentar til artikel 8 skal der kun ske henregnelse, hvis den pågældende stat dirigerede eller udøvede kontrol med den specifikke operation, som de relevante handlinger var en del af. Handlinger, der blot er tilfældigt eller perifært knyttet til en operation, og som sådan ikke dirigeres eller kontrolleres af staten, henregnes derimod ikke.[119] Et kontroversielt spørgsmål er dog, hvad der nærmere bestemt skal til, før en ikke-statslig aktørs handlinger kan siges at være udført 'on the instructions of, or under the direction or control of' en stat. I *Nicaragua*-dommen fandt Den Internationale Domstol, at bistand i form af 'financing, organizing, training, supplying, and equipping' ikke er tiltrækkeligt til at statuere henregnelse. Det afgørende er, om staten udøver 'effektiv kontrol' med den ikke-statslige aktørs handlinger.[120] I forhold til cyberoperationer udført af ikke-statslige aktører vil betingelserne for henregnelse til en stat være opfyldt, hvis staten kan afgøre, hvordan operationen skal udføres, og har kompetence til at godkende og eventuelt afbryde den.[121] Det er derimod ikke tilstrækkeligt til at statuere henregnelse, at staten blot udstyrer den ikke-statslige aktør med f.eks. malware, men ikke har indflydelse på, hvordan og hvornår malwaren benyttes. Udførlig planlægning af den ikke-statslige aktørs cyberoperation er i sig selv heller ikke tilstrækkeligt, og der vil ikke ske henregnelse, hvis den ikke-statslige aktør handler uden for rammerne af de instrukser, staten har givet.[122] Tærsklen for henregnelse efter artikel 8 er med andre ord ganske høj.

Det følger af desuden af artikel 11 i ARSIWA, at ikke-statslige aktørers handlinger, der ikke er omfattet af en efter de øvrige regler i kapitel 2, alligevel skal henregnes til staten '…to the extent that the State acknowledges and adopts the conduct in question as its own.' Denne sædvaneretlig regel blev bragt i anvendelse af ICJ i *Teheran Hostages*-dommen fra 1980.[123] Også her er der tale om en relativt høj tærskel, idet det eksempelvis ikke er tilstrækkeligt, at staten blot anerkender eksistensen af de pågældende handlinger og verbalt bifalder dem.[124] Ikke-statslige aktørers handlinger vil imidlertid kunne henregnes til staten, hvis staten "gør handlingerne til sine egne" ved for eksempel at beskytte den ikke-statslige aktør imod modreaktioner og derved muliggøre fortsættelsen af de relevante handlinger.[125]

Det er væsentligt at holde sig for øje, at vurderingen af henregnelsesspørgsmålet er løsrevet fra vurderingen af, om værtstatens bistand til den ikke-statslige aktør udgør en selvstændig krænkelse af en folkeretlig regel. Hvor en stats finansiering og træning af en ikke-statslig aktør eksempelvis ikke er nok til at statuere henregnelse efter artikel 8 i ARSIWA, kan sådanne handlinger være tilstrækkelige til, at staten selv overtræder sine folkeretlige forpligtelser, herunder vedrørende forbuddet mod magtanvendelse.[126] Ligeledes kan blot viden om, at folkeretsstridige og skadevoldende handlinger udgår fra dens territorium, betyde, at værtsstaten overtræder princippet om "due diligence".

5.2. Due diligence-princippet

Due diligence-princippet er en del af den generelle folkeret og foreskriver, at stater skal udvise "due diligence" for at sikre, at deres territorium ikke anvendes til at krænke andre staters folkeretlige rettigheder eller til at forvolde alvorlig skade på andre stater. Due diligence-princippet er særligt interessant i forhold til ikke-statslige aktørers skadevoldende handlinger i cyberdomænet, da princippets anvendelse – i modsætning til henregnelses-problematikken, som er beskrevet ovenfor – ikke forudsætter identifikation af den individuelle aktør. Det er ikke afgørende, om den pågældende aktør er et individ, en virksomhed, en væbnet oprørsstyrke eller en anden stat. Hvis de relevante betingelser, som vil blive gennemgået i dette afsnit, i øvrigt er opfyldt, er det tilstrækkeligt til at statuere en overtrædelse af en stats due diligence-forpligtelse, at den skadevoldende adfærd påviseligt udgår fra eller benytter sig af statens cyberinfrastruktur.[127]

Der er generel konsensus om, at stater ikke er objektivt ansvarlige for ikke-statslige aktørers handlinger, alene fordi der kan etableres et link mellem den pågældende handling og statens territorium.[128] Men det er omdiskuteret, hvad der præcis skal til, før der på

sædvaneretligt grundlag påhviler stater en forpligtelse til at forhindre skadevoldende handlinger, der er undergivet deres jurisdiktion.[129]

I en ledende dom i *Corfu Channel*-sagen fra 1949 udtalte Den Internationale Domstol, at alle stater er forpligtet til ikke bevidst at lade deres territorium anvende til handlinger, der strider imod andre staters rettigheder.[130] Det har siden været debatteret i den folkeretlige litteratur, hvad der nærmere ligger i begrebet "andre staters rettigheder" og i kravet om viden. I regel nr. 6 i *Tallinn-manualen 2.0* er due diligence-princippet formuleret som følger:

> A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.

Det fremgår umiddelbart af reglens ordlyd, at cyberoperationen skal udgøre en krænkelse af offerstatens folkeretlige rettigheder, og at denne krænkelse skal indebære alvorlige negative konsekvenser for offerstaten. Betingelserne er kumulative, og det er således ikke tilstrækkeligt, at cyberoperationen krænker eksempelvis interventionsforbuddet, hvis offerstaten ikke lider nævneværdig skade derved. Eksperterne bag *Tallinn-manualen 2.0* var enige om, at offerstaten må tåle 'inconvenience, minor disruption, or negligible expense'.[131] Det er dog ikke en betingelse for overtrædelse af due diligence-princippet, at cyberoperationen har medført personskade eller anden fysisk skade. Som eksempler på alvorlige negative konsekvenser for offerstaten, der opfylder betingelserne i regel nr. 6, nævner eksperterne indblanding i offerstatens kritiske infrastruktur eller væsentlig påvirkning af offerstatens økonomi.[132]

For så vidt angår kravet til værtsstatens viden om den ikke-statslige aktørs skadevoldende handlinger, udtalte ICJ i *Corfu Channel*-sagen:

> It cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein, nor yet that it necessarily knew, or should have known, the authors.[133]

Hvis værtstaten faktisk er vidende om de relevante handlinger, er videnskravet naturligvis opfyldt. Det kontroversielle spørgsmål er, under hvilke omstændigheder "burde viden" er nok til, at værtsstatens due diligence-forpligtelse bliver aktuel. Ifølge eksperterne bag *Tallinn-manualen 2.0* vil der være tale om et brud på due diligence-princippet, hvis staten 'is in fact unaware of the cyber operations in question, but objectively should have known that its territory was being used for the operation.'[134] I vurderingen af, hvad en stat objektivt burde have vidst, skal man ifølge manualen tage udgangspunkt i, hvordan en 'reasonable' stat i

en sammenlignelig situation ville have ageret.[135] Der stilles ikke krav om monitorering eller andre tiltag, som kan advare myndighederne om misbrug af statens cyberinfrastruktur, men videns-kravet vil være opfyldt, hvis en stat under lignende omstændigheder – med lignende teknologiske ressourcer – ville have været vidende om cyberoperationen.[136] Regel nr. 7 i *Tallinn-manualen 2.0* indeholder et bud på en præcisering af, hvilke tiltag stater skal tage for at efterleve due diligence-princippet, når betingelserne i regel nr. 6 er opfyldt:

> The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States.[137]

I kommentaren til denne regel indleder eksperterne bag *Tallinn-manualen 2.0* med at understrege, at det nærmere indhold af den due diligence, staterne skal udvise, er et uafklaret spørgsmål. Det ligger fast, at due diligence-princippet indebærer en handlepligt, som stater kan forbryde sig imod både ved manglende indgriben eller ved ineffektiv og utilstrækkelig indgriben i tilfælde, hvor mere virksomme tiltag var mulige. Således var eksperterne enige om, at en stat, der modtager troværdig underretning om, at dens cyberinfrastruktur bliver benyttet af en terrororganisation til en cyberoperation rettet mod en anden stat, og undlader at tage rimelige midler i brug for at stoppe operationen, ikke lever op til sin due diligence-forpligtelse.[138]

Et af de omstridte spørgsmål i relation til regel nr. 7 var, om der gælder en forpligtelse for stater til faktisk at forhindre, at der udgår fjendtlige cyberoperationer mod andre stater fra deres territorium. Indebærer due diligence-princippet med andre ord en ”duty to prevent” forstået som en forpligtelse til at tage forebyggende skridt, der effektivt afskærer muligheden for krænkelse af andre staters folkeretlige rettigheder? Her lænede eksperterne bag *Tallinn-manulaen 2.0* sig op ad Den Internationale Domstols dom i *Genocide*-sagen, som ikke foreskrev en generel forpligtelse til at forhindre folkedrab, men en forpligtelse til at handle, der indtræder, når videnskravet er opfyldt.[139] Konkret i forhold til cyberdomænet vurderede eksperterne, at det ville være urimeligt at pålægge staterne en generel ”duty to prevent”, blandt andet fordi det rent praktisk ville være overordentlig vanskeligt for staterne at leve op til en sådan forpligtelse, og fordi staterne i bestræbelserne herpå ville risikere at krænke andre folkeretlige forpligtelser som for eksempel den menneskeretlige ret til privatliv. Det ligger i overensstemmelse hermed ikke i regel nr. 7, at staterne er forpligtet til at monitorere cyberaktivitet på deres respektive territorier.

For så vidt angår de specifikke tiltag, der forlanges af staterne i forhold til at standse cyberoperationer, som de har viden om, var eksperterne enige om, at ’…the territorial State

must use all feasible, that is, reasonably available, means within its sovereign prerogatives that a reasonably acting State in the same or similar circumstances would employ (i.e., undertake so-called 'best efforts').'[140] Hvad der konkret vil blive anset som tilstrækkeligt afhænger af de nærmere omstændigheder, og der kan være forskel på, hvad der forlanges af forskellige stater. Mens det eksempelvis kan kræves af stort set alle stater, at de blokerer bestemte IP-adresser, kan de krav, der stilles til forskellige stater, variere i tilfælde, hvor det er nødvendigt at tage mere avancerede midler i brug for effektivt at bringe en kompleks og dynamisk cyberoperation til ophør. En teknologisk avanceret stat med sofistikerede cyber-sporingsredskaber til rådighed vil således skulle gøre relativt mere for at forhindre cyberoperationer fra sit territorium end en stat med ringere teknologisk formåen.[141]

Eksperterne bag *Tallinn-manualen 2.0* vurderede ikke, at der på sædvaneretligt grundlag gælder en forpligtelse for staterne til at etablere en bestemt retstilstand,[142] som muliggør efterlevelse af due diligence-forpligtelsen. Der gælder efter deres opfattelse heller ikke en forpligtelse til at retsforfølge de pågældende gerningsmænd. Due diligence-forpligtelsen består ifølge *Tallinn-manualen 2.0* udelukkende i, at staterne skal tage rimelige midler i brug for at standse relevante cyberoperationer. Staterne er således ikke forpligtet til at lykkes med at standse cyberoperationer, der udgår fra deres territorier, så længe de ved hjælp af rimelige midler har gjort et reelt forsøg.

5.3. Mulig udvikling i retning af lovlige modforanstaltninger mod ikke-statslige aktører?

Nogle folkeretsjurister taler om, at der i visse situationer er et "responsibility deficit" i cyberdomænet,[143] fordi ikke-statslige aktører på denne arena har kapacitet til at udøve betydelig magt og forvolde omfattende skade for både stater og individer, uden at der er mulighed for at stille dem direkte til ansvar efter de nugældende folkeretlige regler. Det forhold, at statsansvarsreglerne kun åbner for mulighed for lovlige modforanstaltninger over for stater, er blot et element heri. Den primære årsag til "the responsibility deficit" er indholdet af de nugældende materielle folkeretlige regler. Der er udbredt enighed blandt folkeretseksperter om, at ikke-statslige aktører – uanset omfanget og konsekvenserne af deres fjendtlige cyberoperationer – ikke kan krænke staters suverænitet, og at deres handlinger ikke selvstændigt kan udgøre en overtrædelse af bl.a. interventionsforbuddet.[144] Forklaringen er, at disse folkeretlige regler, som retstilstanden ser ud på nuværende tidspunkt, udelukkende har stater som pligtsubjekter. Det er imidlertid værd at bemærke, at

der formelt set ikke er noget til hinder for at pålægge ikke-statslige aktører direkte folkeretlige forpligtelser, herunder med samme indhold som de forpligtelser der påhviler stater. Man kan endda med en vis rimelighed sige, at der allerede ligger en indirekte anerkendelse af, at ikke-statslige aktører kan krænke folkeretten pga. kravet om folkeretsbrud (rights of other states) i due diligence-princippet. Og der ville naturligvis ikke være noget i vejen for, at der både påhvilede den ikke-statslige aktør en forpligtelse til at overholde visse folkeretlige regler, samtidig med at værtsstaten var forpligtet til at forhindre et brud på disse. Direkte folkeretlige forpligtelser for ikke-statslige aktører ville "blot" kræve, at der blev etableret en folkeretlig retssædvane med et sådant indhold, eller at der blev indgået en traktat mellem stater, der har jurisdiktion i forhold til den ikke-statslige aktør.[145] Her kan man oplagt drage en parallel til diskussionen om den sædvaneretlige ret til selvforsvar imod væbnede angreb. Idet spørgsmålet fortsat er kontroversielt, har mange folkeretseksperter – navnlig efter 11. september 2001 – forfægtet det synspunkt, at der ikke blot gælder en ret til selvforsvar over for stater, men også over for ikke-statslige aktører.[146]

6. De øvre og nedre grænser for modforanstaltninger

Som beskrevet i indledningen til denne rapport, kan begrebet "modforanstaltninger" i princippet dække over mange forskellige handlinger. Det skaber ofte udfordringer, som grundlæggende skyldes, at begrebet mangler en klar og autoritativ definition. Det er en af grundene til, at vi oplever, at begrebet i daglig tale ofte anvendes til at beskrive både handlinger, der ligger under grænsen for det traditionelle modforanstaltningsbegreb – f.eks. fordi handlingerne ikke involverer et *prima facie* folkeretsbrud – samt handlinger, der ligger over denne grænse – f.eks. fordi de involverer magtanvendelse.[147] Det skaber uklarheder, som vi i dette afsnit vil forsøge at udrede.

6.1. Den nedre grænse for modforanstaltninger

Udsættes Danmark for et folkeretsbrud, er det ikke givet, at det modsvar, som Danmark måtte foretrække at bringe i anvendelse, udgør en modforanstaltning i retlig forstand. Af både politiske og juridiske grunde er det imidlertid relevant at tage stilling til dette spørgsmål og dermed overveje, hvordan en konkret handling må ventes at blive opfattet af andre stater såvel som folkeretseksperter.

For så vidt angår de politiske overvejelser kan det være væsentligt at klassificere en handling som enten 1) en *prima facie* lovlig modreaktion, 2) en modreaktion, der ligger på

grænsen til et *prima facie* folkeretsbrud, eller 3) en modreaktion, som må forventes *prima facie* at udgøre et folkeretsbrud. Det skyldes, at staters handlinger ofte har til formål at sende et signal til omverdenen om deres tilgang til den relevante konflikt – og til folkeretten. Det kan derfor være centralt for den danske signalgivning at gøre det klart, hvor Danmark står.

Hvis Danmark desuden måtte ønske at iværksætte en modreaktion, der ikke lever op til de materielle eller processuelle krav, der stilles til modforanstaltninger – f.eks. fordi man ønsker at foretage en ikke-reversibel handling,[148] eller ikke ønsker at fortælle åbent om sammenhængen mellem en oprindelig folkeretskrænkelse og det danske modsvar[149] – er det væsentligt at afklare, om det overvejede danske modsvar retligt klassificeres som modforanstaltninger eller ej. Er det tilfældet, risikerer Danmark at begå folkeretsbrud. Er det ikke tilfældet, vil Danmark ikke være forpligtet til at følge de retlige krav til iværksættelse af modforanstaltninger, jf. ARSIWA.

Det kan i mange tilfælde være svært at vurdere præcist, om der i en konkret sammenhæng er tale om et *prima facie* folkeretsbrud, hvilket skyldes uklarheder i de retlige standarder. Dette gælder eksempelvis for interventionsforbuddet, som grundlæggende forbyder stater gennem tvangsforanstaltninger at påvirke andre stater i situationer, hvor det står disse stater frit for at fastlægge egne, interne forhold (*domaine réservé*). Princippet omfatter bl.a. staters ret til at vælge egne politiske, økonomiske, sociale og kulturelle systemer, samt at udforme egen udenrigspolitik.[150] En krænkelse af sådanne rettigheder vil således være en folkeretsstridig handling, der kan udløse en ret til at foretage modforanstaltninger. Det kan dog være svært at afgøre, om en konkret indblanding i en anden stats affærer har et tilstrækkeligt tvangselement til, at det omfattes af forbuddet, ligesom det kan være uklart, om handlingen påvirker en offerstats *domaine réservé*.[151]

Der knytter sig ligeledes adskillige tvivlsspørgsmål til det såkaldte ”suverænitetsprincip”, som efter en klassisk definition bl.a. berettiger stater til inden for eget territorium at udøve ’to the exclusion of any other State, the functions of a State.’[152] Princippet omfatter staters interne suverænitet, herunder retten til at udøve jurisdiktion inden for eget territorium og andre staters udelukkelse herfra, ligesom princippet omfatter ekstern suverænitet, herunder staters ret til at føre egen udenrigspolitik.

En krænkelse af staters suverænitet kan udgøre et folkeretsbrud, der udløser retten til at gennemføre modforanstaltninger. Det har i hvert fald været den almindelige forståelse af reglerne – også i den cyber-specifikke debat – indtil for ganske nylig.[153] Der er dog de senere år blevet sat spørgsmålstegn ved, om suverænitetsprincippet nu også udgør en selvstændig folkeretlig regel, der kan krænkes og således udløse modforanstaltningsbeføjelser – eller

om der blot er tale om et retligt princip, der ikke i sig selv kan krænkes.[154] Den diskussion har skabt uklarhed og uvished, som gør det nødvendigt kort at behandle emnet her.

I første omgang var det en række højtstående amerikanske embedsmænd, der i deres personlige kapacitet udfoldede et synspunkt om, at suverænitetsprincippet ikke udgjorde en egentlig regel i folkeretten men blot et folkeretligt princip.[155] Under stor bevågenhed fremlagde Storbritanniens daværende Attorney General, Jeremy Wright, i en tale ved *Chatham House* samme synspunkt i maj 2018.[156] Senest har General Counsel ved det amerikanske forsvarsministerium, Paul Ney, udtalt en vis støtte til den britiske tilgang, uden dog at lægge sig fast på en klar amerikansk holdning.[157] At dømme ud fra andre staters udtalelser om spørgsmål og den akademiske litteratur fra de senere år[158] synes briterne og amerikanerne imidlertid at stå relativt alene med deres retlige udlægning af suverænitetsprincippet. Da den estiske præsident, Kersti Kaljulaid eksempelvis talte ved CyCon-konferencen i 2019 og fremlagde det officielle estiske perspektiv på folkerettens rolle i cyberspace, var det bemærkelsesværdigt, at hun valgte slet ikke at tage emnet op. Det var påfaldende, fordi hendes tale blev afholdt omkring et år efter Wrights *Chatham House* tale – på et tidspunkt, hvor det britiske standpunkt blev diskuteret heftigt. Det fravalg er svært at tolke på, men der var utvivlsomt tale om et bevidst fravalg.

En egentlig afvisning af det britiske synspunkt blev fremlagt nogle måneder senere i de franske og nederlandske bidrag til debatten.[159] Som det eksempelvis fremgik af den nederlandske udtalelse:

> According to some countries and legal scholars, the sovereignty principle does not constitute an independently binding rule of international law that is separate from the other rules derived from it. The Netherlands does not share this view. It believes that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act.[160]

Det er desuden bemærkelsesværdigt, at den tyske ambassadør og kommissær for international cyberpolitik, Norbert Riedel, allerede i 2015 synes at have afvist den britisk-amerikanske tilgang,[161] ligesom Michael N. Schmitt og Liis Vihul har fremlagt overbevisende støtte til det traditionelle synspunkt, at suverænitetsprincippet udgør såvel et folkeretligt princip som en selvstændig regel.[162] Flere stater har endvidere for nylig udtrykt støtte til det traditionelle synspunkt i forbindelse med såvel den igangværende *Open-Ended Working Group* proces som andre lignende processer.[163]

Som det fremgår, indeholder såvel interventionsforbuddet som suverænitetsprincippet en række uklarheder. Dette afspejles ikke blot i de principielle debatter om deres indhold og status men også i debatterne om lovligheden af konkrete hændelser og handlinger. Et

eksempel herpå er debatten om lovligheden af Ruslands indblanding i det amerikanske præsidentvalg i 2016, som forskellige juridiske forskere har analyseret på forskellige måder og udlagt divergerende opfattelser af.[164]

6.2. Den øvre grænse for modforanstaltninger

Hvis vi i stedet vender os mod de modforanstaltninger, der befinder sig i den anden ende af skalaen – dem, der potentielt krydser grænsen til magtanvendelse – finder vi tilsvarende udfordringer. I disse år pågår nemlig en helt grundlæggende debat om, hvordan den traditionelle folkeretlige regulering af magtanvendelse finder anvendelse i cyberspace. Spørgsmålet er vigtigt at holde sig for øje, da lovlige modforanstaltninger ikke kan involvere magtanvendelse i strid med FN-pagten, jf. ARSIWA artikel 50, stk. 1, litra a – og da udførelsen af foranstaltninger, der krydser denne grænse, derfor kan underminere den retlige beskyttelse, som ellers ligger i modforanstaltningssystemet.

Det er i forlængelse heraf værd at bemærke, at et brud på magtanvendelsesforbuddet, der falder under grænsen for et 'væbnet angreb', jf. FN-pagtens artikel 51, ikke udløser en ret til at svare igen med magt.[165] Udsættes Danmark således for sådan ulovlig magtanvendelse, i strid med FN-pagtens artikel 2(4), udløses alene en ret til "fredelige" modforanstaltninger. Danmark vil dog formentlig have adgang til at foretage mere vidtgående modforanstaltninger i sådanne tilfælde, da det selvsagt er lettere at overholde proportionalitetsprincippet i ARSIWA, artikel 51, når man reagerer mod en ulovlig magtanvendelse, end ved reaktioner mod fredelige folkeretskrænkelser.

På baggrund af disse forhold er det relevant at overveje grænsedragningen mellem (lovlige) modforanstaltninger og magtanvendelse nærmere – i lyset af de senere års debat herom. Indledningsvist bør visse elementer af den almindelige forståelse af artikel 2(4) dog fremhæves.

6.2.1. Magtanvendelsesbegrebet

Artikel 2(4) anvender det relativt generiske begreb 'force' ('magt') som omdrejningspunkt for bestemmelsens anvendelsesområde. Selv om folkeretten ikke indeholder en klar og entydig definition heraf, synes der at være bred enighed om, at begrebet skal læses som omfattende *væbnet* magt – altså magtanvendelse, der har en vis militær karakter, og som involverer anvendelsen af våben.[166] I den foreliggende sammenhæng er det relevante spørgsmål naturligvis om, og i givet fald hvilket omfang, cyberoperationer er omfattet.

Det er indledningsvis væsentligt at slå fast, at artikel 2(4) ikke er begrænset til væbnet magt i den forstand, at der kræves brug af kinetisk energi til at udføre direkte, fysiske skader. Det følger dels af praksis fra ICJ i *Nicaragua*-sagen, hvor domstolen gjorde klart, at også indirekte handlinger, såsom bevæbning og træning af oprørsgrupper, kan være omfattet.[167] Herudover følger det af det forhold, at magtanvendelsesforbuddet utvivlsomt omfatter brug af f.eks. kemiske og biologiske våben. Mens disse våben selvsagt har fysiske effekter, er denne magtanvendelse kvalitativt anderledes end den virkning, der traditionelt forbindes med væbnet magt.

Det er desuden værd at notere sig ICJ's bemærkninger vedrørende våbenbegrebet, som de fremgår af *Nuclear Weapons*-sagen.[168] Her forklarede ICJ, at artikel 2(4) ikke specificerer, hvilke våben der omfattes af dens anvendelsesområde, og at bestemmelsen således må 'apply to any use of force, regardless of the weapons employed.'[169] I den forbindelse er det desuden interessant, at ICJ også lader til at have accepteret en dynamisk fortolkning af bl.a. artikel 2(4), således at staters udtalelser og praksis over tid kan påvirke forståelsen heraf.[170]

Endelig bør det bemærkes, at den traditionelle debat om magtanvendelsesbegrebet i artikel 2(4) ikke har handlet om forholdet mellem fysiske og ikke-fysiske konsekvenser, som det ofte synes forudsat i den cyber-specifikke debat, men snarere om forholdet mellem væbnede magtmidler og andre former for magtmidler. Det ses bedst illustreret i debatten om, hvorvidt økonomiske og diplomatiske magtmidler er indeholdt i artikel 2(4), hvilket bredt afvises,[171] ligesom det kan ses afspejlet i debatten om, hvorvidt "fysisk, men ikke væbnet, magtanvendelse" er indeholdt i bestemmelsen. Den sidstnævnte debat gør det tydeligt, at der ikke uden videre kan sættes lighedstegn mellem fysiske skader og væbnet magt – omend det må antages, at deltagerne i debatten formentlig har haft en formodning om, at væbnet magt generelt involverer fysisk skade. Ikke desto mindre forklarer Randelzhofer og Dörr om netop "fysisk, men ikke-væbnet, magt", at:

> [a]dmittedly, physical force can affect a State just as severely as the use of military force. But, as has been pointed out with regard to measures of political and economic coercion, the purpose of Art. 2 (4) is to ban only one means of coercion, namely military force.[172]

Med andre ord synes det at være det militære/væbnede element, der er afgørende for magtanvendelsesbegrebet, frem for det strengt fysiske element.

6.2.2. Den cyber-specifikke debat

Med udgangspunkt i denne korte gennemgang af elementer fra den bredere debat om magtanvendelsesbegrebet kan vi bevæge os videre til den specifikke debat om cyberoperationers klassificering. Her har vi set en del udvikling de senere år, som giver os mulighed for at nå til lidt klarere konklusioner, end vi kunne for blot få år siden. Selv om der fortsat rejses mange legitime spørgsmål om, hvordan reglerne om magtanvendelse fungerer i cyberdomænet, og selv om en række helt basale spørgsmål fortsat fremstår uafklarede, kan vi begynde af identificere konturerne af mindst tre forhold:

For det første er der ikke længere reel tvivl om, at cyberangreb i hvert fald i nogle tilfælde kan udgøre magtanvendelse under FN-pagtens artikel 2(4).[173] Dette antages nu af stort set alle deltagere i debatten.[174]

For det andet forekommer det klarere i dag end for blot få år siden, at den såkaldte ”effektbaserede” tilgang til magtanvendelsesbegrebet er dominerende.[175] Det er tilfældet både blandt folkeretseksperter og blandt de stater, der har udtalt sig om emnet.[176] Tilgangen baserer sig på praksis fra ICJ, herunder om den såkaldte ”scale and effect”-analyse, som domstolen anvendte i *Nicaragua*-sagen.[177] Når vi derfor i dag skal søge at besvare spørgsmål om, hvilke handlinger, der er omfattet af magtanvendelsesbegrebet i cyberspace, bør udgangspunktet for vurderingen være, om cyberoperationens effekter er sammenlignelige med de effekter, der følger af konventionel væbnet magtanvendelse.

Det tredje spørgsmål, som vi kan besvare mere præcist i dag end for få år siden – idet det dog kræver en noget mere udførlig gennemgang end i de to foregående – kan opsummeres som følger: Kan cyberoperationer, der ikke medfører fysiske skader, omfattes af magtanvendelsesbegrebet? Dette spørgsmål har været debatteret indgående de seneste to årtier, hvilket ikke mindst afspejler dets praktiske relevans – også for fremtidige cyberoperationer. Gennemgår man den juridiske litteratur om magtanvendelsesbegrebet på cyberområdet finder man hurtigt ud af, at der fortsat er udbredt uenighed. Russell Buchan’s gennemgang af litteraturen når eksempelvis frem til, at ‘[t]he generally accepted interpretation of Article 2(4) is that only those interventions that produce physical damage will be regarded as an unlawful use of force’,[178] mens Marco Roscini’s analyse fører til en næsten modsatrettet konklusion.[179] Forvirringen øges af Samuli Haataja, som i én tekst skriver, at magtanvendelse efter den generelle vurdering kræver fysiske skader, mens han i en anden tekst opsummerer samme analyse således, at magtanvendelse i cyberdomænet kræver *enten* fysiske effekter *eller* betydelige forstyrrelser af kritisk infrastruktur – også selv

om sidstnævnte ikke medfører fysiske effekter.[180] Uklarheden fremgår også tydeligt af Claus Kress' nylige analyse, hvori han blot noterer, at stater, som rammes af alvorlige ikke-fysiske angreb på kritisk infrastruktur (f.eks. børserne), kan forventes at klassificere sådanne angreb som magtanvendelse – eller måske endda væbnet angreb – og at dette bør bekymre.[181] På samme måde er det bemærkelsesværdigt, hvordan udfordringen behandles i International Law Association's *Final Report on Aggression and the Use of Force* fra 2018. Her noteres uenigheden ligeledes, og det konkluderes, at '[t]he absence of State practice in relation to major cyber operations against critical financial infrastructure makes it difficult to draw definitive conclusions.'[182] Med andre ord synes spørgsmålet at stå relativt åbent i den juridiske litteratur.

Det forhold er da også reflekteret i behandling af spørgsmålet i *Tallinn-Manualen 2.0*. Manualens regel nr. 69 foreskriver således blot, at en cyberoperation 'constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.'[183] Dermed henvises til den bredt anerkendte "scale and effect"-standard nævnt ovenfor,[184] uden at der eksplicit tages stilling til, om cyberangreb uden fysiske effekter omfattes af magtanvendelsesbegrebet. Eksperterne er altså tilbageholdende, men de holder en dør åben. Det ses klart i bemærkningerne til reglen, hvori eksperterne eksplicit anerkender det perspektiv, at cyberangreb uden fysiske effekter kan underlægges en nærmere analyse med henblik på at vurdere, om stater kunne tænkes at anse et sådant angreb for omfattet af artikel 2(4).[185] Denne analyse indebærer en vurdering af konkrete cyberangreb med udgangspunkt i en række faktorer, herunder hvor alvorlige skader angrebet forvolder, hvor hurtigt og hvor direkte dets konsekvenser indtræder, og hvorvidt det er af militær karakter.[186]

Går vi væk fra litteraturen og ser nærmere på, hvad staterne har haft at sige om spørgsmålet, finder vi – i den ene ende af skalaen – lande som Nederlandene og Frankrig, der begge eksplicit peger på, at cyberangreb ikke behøver at medføre fysiske effekter for at kunne klassificeres som magtanvendelse. Den nederlandske tilgang har således været, at der bør foretages en konkret analyse af cyberangrebets effekter, og at det ikke kan udelukkes, at f.eks. angreb, der medfører meget alvorlige finansielle eller økonomiske konsekvenser, kan udgøre magtanvendelse.[187] Samtidig har Nederlandene officielt udtrykt støtte til den fremgangsmåde, som fremgår af *Tallinn-manualen 2.0*.[188] Frankrig gjorde noget lignende gældende, da man i 2019 fremlagde sit syn på folkeretten i cyberspace.[189]

De fleste andre lande, som har udtalt sig om spørgsmålet, har ladet svaret stå åbent, om end nogle stater har fokuseret mere på det fysiske element end andre. Australien påpeger

f.eks., at det afgørende spørgsmål er, om cyberangrebets 'scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law.'[190] Derfor skal man – fra det australske perspektiv – se på, om cyberangrebet kunne medføre alvorlig 'damage or destruction … to life, or injury or death to persons, or result in damage to the victim state's objects, critical infrastructure and/or functioning.'[191] Selv om der således ikke tages eksplicit stilling til ikke-fysiske skader, afviser man tydeligvis ikke muligheden. Noget lignende er tilfældet hos den tyske ambassadør og kommissær for international cyberpolitik, Norbert Riedel, som forklarer om selvforsvarsretten ved væbnede angreb, at spørgsmålet om hvorvidt cyberangreb er omfattet heraf afhænger af, om effekterne er 'comparable to an armed attack'[192]. I den forbindelse kan følgende faktorer ifølge Reidel inkluderes i de retlige overvejelser: 'the seriousness of the attack, the immediacy of its effects, depth of penetration of the cyber infrastructure and its military character.'[193] Igen støttes en bred tilgang til spørgsmålet, uden at det eksplicit hverken be- eller afkræftes, om magtanvendelse kan omfatte handlinger uden direkte fysiske effekter. I stedet anvendes en ren faktor-baseret analyse.

Den estiske præsident var ligeledes relativt uklar, da hun omtalte spørgsmålet i sin CyCon-tale fra 2019. Her noterede hun blot, at 'cyber operations, which cause injury or death to persons or damage or destruction of objects, could amount to use of force or armed attack under the UN Charter.'[194] I forlængelse heraf fremhævede hun, at Estland er meget afhængig af et stabilt og sikkert cyberspace, hvilket ledte hende til at påpege at 'growing digitalization of our societies and services can also lower the threshold for harmful effects.'[195]

Endnu mere uklare er dog udmeldingerne fra Storbritannien og USA, som synes at fokusere snævert på det fysiske element – uden eksplicit at udelukke noget. Storbritanniens Attorney General har således forklaret, at cyberangreb, der resulterer i 'death and destruction on an equivalent scale to an armed attack'[196] omfattes af artikel 51 – hvilket må reflektere en lignende analyse i relation til artikel 2(4). Han udelukker dog ikke eksplicit, at andre typer af angreb kan omfattes af magtanvendelsesbegrebet. Noget lignende er tilfældet hos amerikanerne, hvor man synes at acceptere en faktor-baseret tilgang, uden dog at udtale støtte til tanken om, at cyberangreb kan udgøre magtanvendelse selv uden fysiske skader. Harold Koh advokerede således allerede i 2012 for en faktor-drevet vurdering, men han fokuserede utvetydigt på fysiske skader.[197] Den amerikanske tilgang er senest blevet opdateret ved Paul Nay's tale fra marts 2020, som ligeledes fokuserer på cyberangrebs fysiske effekter uden eksplicit at udelukke andre angreb fra

magtanvendelsesbegrebet – hvilket der ellers kunne have være anledning til på baggrund af særligt de nederlandske og franske udtalelser beskrevet ovenfor.[198]

På denne baggrund status at være, at nogle stater mener, at cyberangreb kan udgøre magtanvendelse, uden at de nødvendigvis resulterer i fysiske skader, mens andre stater har været mindre tydelige i deres udmeldinger. Nogle af de mindre tydelige stater synes at hælde til accept af en bred definition af magtanvendelsesbegrebet, mens andre læner væk herfra.

Selvom debatten på dette område således er langt fra afsluttet, kan vi alligevel drage visse konklusioner, hvis vi ser nærmere på det samlede, tilgængelige materiale. Blandt akademikere er nogle villige til (næsten) at udelukke, at magtanvendelsesbegrebet kan omfatte cyberangreb uden fysiske effekter,[199] mens de fleste synes tilbageholdende med helt at lukke døren for denne mulighed,[200] ligesom mange aktivt støtter den.[201] Den akademiske tilgang kan sammenholdes med det forhold, at ingen stater øjensynligt har fundet anledning til eksplicit at afvise, at cyberangreb uden fysiske effekter kan udgøre magtanvendelse i nogle tilfælde – om end staternes tilgang er langt fra entydig.

7. Konklusioner og anbefalinger

Selv om cyberdomænet i dag er genstand for et stort politisk og akademisk fokus, herunder fra folkeretseksperter, bør det ikke glemmes, at udviklingen på området kun for relativt nyligt tog fart. Det var således ikke før 2012, at FE gjorde cybertruslen til et centralt tema i sine årlige trusselsvurderinger, og det er først i løbet af de senere år, at tyngdepunktet i den folkeretlige debat er rykket fra cyberkrig til reguleringen af de mindre indgribende konflikter, som vi i højere grad oplever i praksis. Selv om flere og flere stater melder sig på banen med deres syn på folkerettens rolle i cyberspace, fremstår mange centrale spørgsmål fortsat uafklarede. Det er et vigtigt udgangspunkt at holde sig for øje, når man analyserer de retlige udfordringer ved cybertruslen.

I denne rapport har vi behandlet et af de centrale modsvar, som folkeretten muliggør, når stater udsættes for folkeretlige krænkelser på cyberområdet, der ikke når tærsklen for et væbnet angreb –modforanstaltninger. Modforanstaltninger forstås i denne sammenhæng som handlinger, som en stat under normale omstændigheder ville ifalde folkeretligt ansvar for at udføre, men som i det konkrete tilfælde er lovlige, fordi formålet med dem er at bringe en anden stats folkeretsbrud til ophør. På baggrund af de seneste års udvikling i både teori og praksis har rapporten gjort status over og analyseret de muligheder og begrænsninger, der ligger i retten til at foretage modforanstaltninger i forbindelse med eventuelle

cyberoperationer rettet mod Danmark. Vi har i den forbindelse valgt at fokusere på en række hovedproblemstillinger, der aktuelt synes at være under hastig udvikling, og hvor danske beslutningstagere har en interesse i at gøre sig strategiske overvejelser om, hvilke folkeretlige synspunkter Danmark ønsker at fremme. Disse hovedproblemstillinger omhandler spørgsmålene om

1) hvem, der kan anvende modforanstaltninger, herunder muligheden for 'kollektive modforanstaltninger' (afsnit 4)
2) hvem modforanstaltninger kan rettes imod, herunder i situationer hvor cyberoperationen udgår fra ikke-statslige aktører (afsnit 5)
3) de øvre og nedre grænser for, hvornår en handling retligt kan kategoriseres som en modforanstaltning (afsnit 6).

Med henblik på at belyse disse spørgsmål har rapporten behandlet de fundamentale krav til lovlige modforanstaltninger, som fremgår af ARSIWA, og som stater må forventes at skulle iagttage også i cyberspace. Disse omfatter materielle krav om, at modforanstaltninger f.eks. skal rettes mod den stat, der bærer ansvaret for det relevante folkeretsbrud, at de ikke kan anvendes som straf eller gengældelse, men alene til at genoprette en situation, hvor folkeretten overholdes, samt at lovlige modforanstaltninger ikke kan omfatte overtrædelse af fundamentale menneskerettigheder og ufravigelige regler (*jus cogens*) efter den generelle folkeret. Derudover omfatter reguleringen en række processuelle krav, herunder at offerstaten skal anmode gerningsstaten om at opfylde sine folkeretlige forpligtelser, inden modforanstaltninger iværksættes.

Rapporten konkluderer desuden, at det kun er muligt for stater at iværksætte modforanstaltninger – og i udgangspunktet kun for offerstater. En væsentlig pointe er dog, at der synes at være et vist rum for fortolkning i forhold til en eventuel ret til at foretage kollektive modforanstaltninger på anmodning fra en offerstat, og at det synes muligt at anlægge en positiv tilgang til en sådan forståelse af folkeretten.

For så vidt angår spørgsmålet om, hvem modforanstaltninger kan rettes imod, konkluderes det i rapporten, at kun stater er omfattet af det gældende system, men at problemstillinger vedrørende ikke-statslige aktørers centrale rolle i cyberspace aktualiserer spørgsmål om principperne for henregnelse og due diligence. Det fremhæves således, at henregnelse af en ikke-statslig aktørs handlinger til en stat kræver relativt omfattende indblanding fra statens side, ligesom det bemærkes, at kravene til de enkelte stater i forbindelse med due diligence-princippet synes meget kontekst-afhængig og i høj grad hviler

på helt generelle rimelighedsbetragtninger. I forlængelse heraf gør rapporten derfor opmærksom på, at der formelt set ikke er noget til hinder for at pålægge ikke-statslige aktører direkte folkeretlige forpligtelser, og at man endda med en vis rimelighed kan sige, at der ligger en indirekte anerkendelse af, at ikke-statslige aktører kan krænke folkeretten i due diligence-princippet. På grund af de ikke-statslige aktørers centrale rolle i cyberspace kunne en udvikling mod direkte forpligtelser for disse aktører reducere behovet for at arbejde med indirekte modeller for ansvar, som henregnelse og due diligence er udtryk for. En sådan retlig udvikling forudsætter imidlertid etablering af en folkeretlige retssædvane med et sådant indhold, eller indgåelse af en traktat mellem relevante stater herom.

Endelig har rapporten behandlet de udfordringer, der er forbundet med at afgrænse modforanstaltninger over for henholdsvis lovlige (men uvenlige) handlinger og magtanvendelse, som ikke kan anses som lovlige modforanstaltninger. I den forbindelse fremhæver rapporten, at de eksisterende tvivlsspørgsmål inden for dette tema skaber en risiko for, at forskellige stater og folkeretseksperter vil kategorisere konkrete handlinger forskelligt, hvilket kan have væsentlige implikationer bl.a. for forståelsen af de rettigheder og forpligtelser, der følger med sådanne handlinger.

Som det fremgår, har rapporten identificeret en række uklarheder ved såvel modforanstaltningsbegrebet som sådan som en række relaterede folkeretlige spørgsmål. Der synes på denne baggrund at være et udtalt behov for at klargøre den folkeretlige regulering på området med henblik på at skabe forøget stabilitet og forudsigelighed i cyberdomænet. Det er vores vurdering, at Danmark har en interesse i at bidrage til en sådan udvikling, både på grund af Danmarks generelle interesse i at fastholde og styrke den regelbaserede verdensorden – også i cyberspace – men også fordi Danmark netop nu har mulighed for at påvirke den retlige udvikling i den retning, som måtte findes ønskelig.

Det anbefales derfor, at Danmark fortsat indgår aktivt i relevante fora og processer, der har til formål at afklare folkerettens rolle i cyberspace, og som potentielt kan føre til fællesudtalelser eller lignende resultater. Det omfatter de to parallelle FN-spor baseret henholdsvis på *Group of Governmental Experts* (GGE) modellen og den såkaldte *Open-Ended Working Group* (OEWG) proces – i det omfang Danmark, direkte eller indirekte, har adgang til disse processer, og i det omfang der vurderes at være mulighed for reel og effektiv indvirken på processen.[202]

Det anbefales herudover, at Danmark bidrager til den retlige udvikling ved at fremlægge den danske holdning til de områder af folkeretten, der behandles i denne rapport. Da en sådan tilkendegivelse nødvendigvis vil involvere stillingtagen til en række grundlæggende

folkeretlige problemstillinger, vil et ideelt format være en eksplicit, samlet og overskuelig analyse af Danmarks syn på, hvordan centrale dele af folkeretten mere generelt finder anvendelse i cyberspace. Med denne anbefaling lægger vi os i slipstrømmen af lignende anbefalinger fra tilsvarende rapporter om folkerettens rolle i cyberspace.[203]

Som rapporten understreger, har kun få stater på nuværende tidspunkt fremlagt samlede og eksplicitte juridiske analyser af folkerettens rolle i cyberspace, hvilket både illustrerer behovet for yderligere bidrag samt effekten af de enkelte staters bidrag. Det har således vist sig, at også små stater har været i stand til at påvirke den juridiske debat – og dermed potentielt påvirke den retlige udvikling. Det er en mulighed, som også Danmark kan udnytte.[204]

Noter

[1] Der var dog henvisninger til bl.a. propagandavirksomhed på internettet i forbindelse med udspredelsen af global jihadisme. Se Forsvarets Efterretningstjeneste, *Efterretningsmæssig risikovurdering 2004* (december 2004), s. 20.

[2] Forsvarets Efterretningstjeneste, *Efterretningsmæssig risikovurdering 2010* (august 2010), s. 51.

[3] *Ibid.*

[4] NATO, *Cyber Defence Factsheet* (februar 2018).

[5] Beredskabsstyrelsen, *Danskernes Risikoopfattelse – Spørgeskemaundersøgelse: Rapport 2019*, s. 6.

[6] For blot at nævne nogle eksempler: Det er omstridt, hvorvidt 'magtanvendelsesbegrebet' i FN-pagtens artikel 2(4) kun dækker cyberangreb, der medfører fysisk skade, eller om begrebet er bredere. Dette spørgsmål berøres i rapportens kapitel 6. Det er desuden behæftet med tvivl, hvordan suverænitetsprincippet finder anvendelse i forbindelse med cyberoperationer, ligesom der er uklarheder om, hvorvidt 'digitale objekter' er omfattet af krigens loves beskyttelse af civile 'objekter'. Se herom i M. N. Schmitt (red.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, Cambridge, 2017) ('*Tallinn-manualen 2.0*'), s. 17-27 og 435-437.

[7] M. N. Schmitt (red.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, Cambridge, 2013) ('*Tallinn-manualen 1.0*').

[8] H. Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention,* Chatham House (december 2019).

[9] *Ibid,* s. 58.

[10] Dette er ikke isoleret til den juridiske debat. Se eksempelvis en nyligt udgivet gennemgang af emnet i T. Liebetrau, *Dansk offensiv cybermagt mellem angreb, spionage og forsvar: en komparativ analyse på tværs af Europa*, Center for Militære Studier (maj 2020).

[11] President of Estonia, *President of the Republic at the opening of CoCon 2019* (2019), tilgået 19 maj 2020; Ministère Des Armées, *Droit International Appliqué Aux Opérations Dans le Cyberspace* (2019), tilgået 19 maj 2020.

[12] J. Crawford, *State Responsibility: The General Part* (Cambridge University Press, Cambridge, 2013), s. 685. Det bemærkes dog, at emneområdet for ARSIWA's kapitel om modforanstaltninger beskrives som 'measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation.' Se Den Internationale Lovkommission, 'Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentary', *Yearbook of the International Law Commission* (2001) Vol. II, Part Two, as corrected ('*ARSIWA med kommentarer*'), s. 125.

[13] Se eksempelvis D. Alland, 'The Definition of Countermeasures', i J. Crawford, A. Pellet & S. Olleson (red.), *The Law of International Responsibility* (Oxford University Press, Oxford, 2010), s. 1135. Se desuden beskrivelsen af begrebet 'non-forcible countermeasures' i *ARSIWA med kommentarer* (n 12), s. 75.

[14] Forsvarets Efterretningstjeneste, *Efterretningsmæssig risikovurdering 2019* (november 2019) ('*FE vurdering 2019*'), s. 31.

[15] Center for Cybersikkerhed, *Trusselssvurdering: Cybertruslen mod Danmark 2019* (marts 2019) ('*CTV 2019*'), s. 3. Se lignende i *Ibid.*, s. 8.

[16] *FE vurdering 2019* (n 14), s. 32; Center for Cybersikkerhed, *Trusselsvurdering: Cybertruslen mod Danmark 2020* (juni 2020) ('CTV 2020'), s. 3.

[17] *Ibid.*, s. 32.

[18] *CTV 2020* (n 16), s. 15.

[19] Se bl.a. J. Kish og D. Turns, *International Law and Espionage* (Martinus Nijhoff Publishers, The Hague, Boston, 1995; S. Chesterman, 'The Spy Who Came in from the Cold War: Intelligence and International Law.' 27:4 *Michigan Journal of International Law* (2006); A. J. Radsan, 'The Unresolved Equation of Espionage and International Law', 28:3 *Michigan Journal of International Law* (2007). Se dog et modargument til den traditionelle opfattelse i R. Buchan, *Cyber Espionage and International Law* (Hart Publishing, Oxford, 2019).

[20] *FE vurdering 2019* (n 14), s. 34; *CTV 2019* (n 15), s. 13; *CTV 2020* (n 16), s. 19.

[21] *FE vurdering 2019* (n 14), s. 34.

[22] *Ibid.*

[23] *Ibid.*

[24] *Ibid.*

[25] *Tallinn-manualen 2.0*. (n 6), s. 342. Eksperterne var enige om, at angrebet udgjorde "brug af væbnet magt" efter FN-pagtens artikel 2(4), men de kunne ikke blive enige om, hvorvidt angrebet også udgjorde et "væbnet angreb" efter FN-pagtens artikel 51.

[26] *FE vurdering 2019* (n 14), s. 33. Se også *CTV 2019* (n 15), s. 6.

[27] *FE vurdering 2019* (n 14), s. 36; *CTV 2019* (n 15), s. 5-6.

[28] *FE vurdering 2019* (n 14), s. 34.

[29] *Ibid*., s. 36.

[30] *Ibid*.

[31] Forsvarets Efterretningstjeneste, *Efterretningsmæssig risikovurdering 2011* (oktober 2011), s. 17.

[32] A. Henriksen, *Cyberkrig: Folkeretten og computer network operations*, Center for Militære Studier (april 2012).

[33] A. Henriksen, *Folkeretten og modreaktioner i cyberspace*, Center for Militære Studier (februar 2014).

[34] *Ibid.,* s. 2.

[35] Rapportens afsnit 4 indeholder konkrete eksempler på situationer, hvor stater har hævdet at være ansvarsfri for brud på folkeretlige regler med henvisning til, at der var tale om lovlige modforanstaltninger.

[36] I forbindelse med det langstrakte arbejde med statsansvarsreglerne blev modforholdsregler af Lovkommissionen selv omtalt som 'perhaps the most difficult and controversial aspect of the whole regime of State responsibility'. Se Den Internationale Lovkommission, *Yearbook of the International Law Commission (1996) Vol. II, Part. 2*, (UN Doc. A/CN.4/SER.A/1996/Add.l (Part 2)), s. 66.

[37] *Gabčíkovo-Nagymaros Project* (Hungary v. Slovakia), Judgment, I.C.J. Reports 1997, s. 7, præmis 83 (vores understregning).

[38] Se dog nedenfor om 'indirect or collateral' effects.
[39] *ARSIWA med kommentarer* (n 12), 128.
[40] Se mere detaljeret herom i afsnit 5.
[41] Se også *Tallinn-manualen 2.0* (n 6), regel nr. 21, s. 116ff.
[42] *Ibid.*, s. 134.
[43] *ARSIWA med kommentarer* (n 12), s. 130. Se også *Ibid.*, s. 118.
[44] Se *Tallinn-manualen 2.0* (n 6), s. 119.
[45] Se også *Ibid.*, s. 123.
[46] Se også *Ibid.*, s. 128.
[47] *ARSIWA med kommentarer* (n 12), s. 129.
[48] *Tallinn-manualen 2.0* (n 6), s. 128.
[49] Se hertil ARSIWA, artikel 43.
[50] Se også *Tallinn-manualen 2.0* (n 6), s. 120.
[51] Se desuden Crawford (n 12), s. 706.
[52] Se ARSIWA, artikel 49(1), 52(1), 52(1) og 54.
[53] ARSIWA, artikel 49(1).
[54] *ARSIWA med kommentarer* (n 12), s. 119.
[55] *Ibid.*
[56] *Ibid.*
[57] *Ibid.*
[58] Se mere om processen og denne debat i J. Crawford, J. Peel & S. Olleson, 'The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: Completion of the Second Reading', 12:5 *European Journal of International Law* (2001). Se særligt artiklens s. 980-982 om kollektive modforanstaltninger.
[59] Begrebet er lånt og oversat fra James Crawfords arbejde som *special rapporteur* for statsansvar. Det bør bemærkes, at begrebet ikke er universelt anvendt, og at andre begreber ofte anvendes i litteraturen. Der er i det hele taget en del forvirring om terminologien. Se mere herom i M. Dawidowicz, *Third-Party Countermeasures in International Law* (Cambridge University Press, Cambridge, 2017), s. 33-34.
[60] Denne skepsis kommer ofte til udtryk igennem en formodning eller et udgangspunkt om, at kollektive modforanstaltninger ikke er tilladt. Se en 'hård' udgave af denne skepsis hos M. N. Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law', 54:3 *Virginia Journal of International Law* (2014), s. 728-729, og en lidt 'blødere' udgave hos N. Tsagourias, 'The Law Applicable to Countermeasures against Low-Intensity Cyber Operations', 14:1 *Baltic Yearbook of International Law* (2014), s. 120-121. For en mere grundlæggende skeptisk tilgang se f.eks. D. Alland, 'Countermeasures of General Interest', 13:5 *European Journal of International Law* (2002), s. 1230-1233.
[61] *Tallinn-manualen 2.0* (n 6), s.132.
[62] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, I.C.J. Reports 1986 ('Nicaragua'), s. 14.
[63] *Ibid*, s.132.
[64] *Ibid*.

[65] Se særligt C. Tams, *Enforcing Obligations Erga Omnes in International Law* (Cambridge University Press, Cambridge, 2005); E. K. Proukaki, *The Problem of Enforcement in International Law: Countermeasures, the Non-injured State and the Idea of International Community* (Routledge, New York, 2010); Dawidowicz, (n 59). Disse studier behandles kort nedenfor.

[66] *President of Estonia* (n 11).

[67] *Ministère Des Armées* (n 11).

[68] *Ibid.*

[69] *Nicaragua* (n 62), præmis 228 og 292.

[70] *Ibid*., præmis 160, 164 og 230-231.

[71] *Ibid*., præmis 165-166 og 232-234.

[72] *Ibid*., præmis 199.

[73] *Ibid*., præmis 249.

[74] Se f.eks. Schmitt (n 60), s. 728.

[75] Se desuden *Nicaragua* (n 62), præmis 210, som også peger i denne retning.

[76] Crawford (n 12), s. 704.

[77] J. Charney 'Third State Remedies in International Law', 10:1 *Michigan Journal of International Law* (1989), s. 74-75.

[78] S. Haataja 'Cyber Operations and Collective Countermeasures under International Law', 25:1 *Journal of Conflict and Security Law* (2020), s. 48; P. Roguski 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?', *12th International Conference on Cyber Conflict: 20/20 Vision – The Next Decade* (2020).

[79] *ARSIWA med kommentarer* (n 12), s. 139; *Tallinn-manualen 2.0* (n 6), s. 132.

[80] Se *ARSIWA med kommentarer* (n 12), s. 137-139.

[81] J. Crawford, *Third report on State responsibility, by Mr. James Crawford, Special Rapporteur* (2000) (UN Doc. A/CN.4/507), para. 386-406.

[82] *Ibid.,* para. 392.

[83] *Ibid.,* para. 401.

[84] J. M. Petman, 'Resort to Economic Sanctions by Not Directly Affected States', i L. P. Forlati & L. A. Sicilianos (red.), *Les sanctions économiques en droit international/Economic Sanctions in International Law* (Hague Academy of International Law & Martinus Nijhoff Publishers, Leiden, Boston, 2004), s. 376.

[85] C. Tams (n 65), s. 231.

[86] *Ibid.*

[87] *Ibid.*

[88] Proukaki (n 65).

[89] *Ibid.*, s. 103.

[90] Dawidowicz (n 59).

[91] *Ibid.*, s. 242.

[92] *Ibid.*

[93] *Ibid.*, s. 244.

[94] *Ibid.*, s. 283.

[95] *Joint statement by the Governments of the Ten States members of the European Community concerning the Falkland Islands issued at Brussels on 10 April 1982* (14. April 1982) (UN Doc. S/14976).
[96] Se detaljer i Dawidowicz (n 59), s. 141.
[97] *Trade Restrictions Affecting Argentina Applied For Non-Economic Reasons* (5. maj 1982) (L/5319), para. 1(b).
[98] Den Internationale Lovkommission, *Report of the International Law Commission*, Fifty-Second Session, Supp. No. 10 (2010) (U.N. Doc. A/55/10), artikel 54. A/5/19.
[99] J. Crawford, *Fourth report on State responsibility, by Mr. James Crawford, Special Rapporteur* (2001) (UN Doc. A/CN.4/517), para. 74.
[100] *Ibid.*, para. 72.
[101] Den Internationale Lovkommission, *Report of the International Law Commission on the work of its fifty-second session (2000): Topical summary of the discussion held in the Sixth Committee of the General Assembly during its fifty-fifth session prepared by the Secretariat* (2000) (UN Doc. A/CN.4/513), para. 175.
[102] Crawford (n 99), para. 74.
[103] *Ibid.*
[104] Det skal dog bemærkes, at spørgsmålet ikke var i fokus dengang, bl.a. fordi der syntes at være en vis forvirring omkring forståelsen af den foreslåede regulering. Se nærmere i Tams (n 65), s. 242-244.
[105] *Ibid.*, s. 246.
[106] *Ibid.*, s. 246-247.
[107] *Ibid.*, s. 247.
[108] Den Internationale Lovkommission, *State responsibility — Comments and observations received from Governments* (2001) (UN Doc. A/CN.4/515 and Add. 1-3), ('Comments and observations'), s. 83.
[109] Den Internationale Lovkommission, *Sixth Committee, Summary of Record of Meetings*, (9. November 2001) (UN Doc. A/C.6/56/SR.11), para. 30.
[110] *Ibid.*, para. 33.
[111] Dawidowicz (n 59), s. 283.
[112] Se f.eks. de britiske udtalelser herom i *Comments and observations* (n 108), s. 94. Se desuden den japanske tilgang i samme, s. 94.
[113] Se lignende i *Tallinn-manualen 2.0* (n 6), s. 130; Schmitt (n 60), s. 727-728.
[114] Efter omstændighederne kan national lovgivning naturligvis være relevant.
[115] Se lignende i *Tallinn-manualen 2.0* (n 6), s. 130. Se endvidere om afsnit 5.2 om 'due diligence'-princippet.
[116] Spørgsmålet om henregnelse af ikke-statslige aktører til staten handlinger behandles i afsnit 5.1.
[117] Article 51 i *Draft Articles on the Responsibility of International Organizations* ('ARIO') har samme ordlyd som ARSIWA, artikel 22, bortset fra, at det i artikel 51, stk. 4, tilføjes, at '[c]ountermeasures shall, as far as possible, be taken in such a way as to limit their effects on the exercise by the responsible international organization of its functions.'
[118] Se ARSIWA, artikel 5 for så vidt angår tilfælde, hvor ikke-statslige aktører handler på baggrund af en retlig bemyndigelse fra staten. Se desuden afsnit 4.3.
[119] *ARSIWA med kommentarer* (n 12), s. 47.

[120] *Nicaragua* (n 62), s. 14, præmis 115. Se også *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, s. 43 ('Genocide'), præmis 389ff.

[121] Se for eksempel *Tallinn-manualen 2.0* (n 6), s. 96; M. N. Schmitt and S.Watts, 'Beyond State-Centrism: International Law and Non-state Actors in Cyberspace', 21:3 *Journal of Conflict & Security Law* (2016), s. 604.

[122] Schmitt and Watts (n 121), s. 604-605. Den ikke-statslige aktørs *ultra vires*-handlinger henregnes med andre ord ikke til staten.

[123] *United States Diplomatic and Consular Staff in Tehran, Judgment*, I.C.J. Reports 1980, s. 3.

[124] *ARSIWA med kommentarer* (n 12), s. 53.

[125] *Tallinn-manualen 2.0* (n 6), s. 99; Schmitt and Watts (n 121), s. 605.

[126] Således kan eksempelvis 'bevæbning' af en oprørsgruppe med malware efter omstændighederne udgøre magtanvendelse, jf. *Tallinn-manualen 2.0* (n 6), s. 331-332.

[127] Der er ikke krav om, at den pågældende cyber-infrastruktur skal befinde sig på statens eget territorium. Det afgørende er, om staten kan udøve 'governmental control' over den. Se hertil *Tallinn-manualen 2.0* (n 6), s. 32-33.

[128] Se bl.a. R. Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 *Journal of Conflict & Security Law* (2016), s. 431.

[129] Det bemærkes, at visse traktater pålægger stater at forhindre bestemte handlinger. Dette gælder eksempelvis *Folkedrabskonventionens* artikel 1, som fortolket af ICJ i *Genocide* (n 120), præmis 430. Indtil videre er der imidlertid ikke vedtaget sådanne specifikke traktatbestemmelser vedrørende cyberoperationer.

[130] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*, Judgment (Merits), I.C.J. Reports 1949, s. 4, s. 22. Vores understregning.

[131] *Tallinn-manualen 2.0* (n 6), s. 37.

[132] *Ibid.,* s. 37-38.

[133] *Corfu Channel* (n 130), s. 18. Se også ICJ's udtalelse i *Genocide* (n 120), præmis 432: 'to incur responsibility on this basis it is enough that the State was aware, or should normally have been aware, of the serious danger that acts of genocide would be committed.'

[134] *Tallinn-manualen 2.0* (n 6), s. 41.

[135] Dette synes at svare til de fleste staters holdning. Se hertil P. Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program for Cyber Norms Policy Brief (marts 2020), s. 11-12.

[136] *Tallinn-manualen 2.0* (n 6), s. 42.

[137] *Ibid.*, regel 7.

[138] *Ibid.*, s. 40 og 43.

[139] *Genocide* (n 120), præmis 431.

[140] *Tallinn-manualen 2.0* (n 6), 47.

[141] Buchan (n 128), s. 446.

[142] Sådanne krav stilles eksempelvis i artikel 14 i *Konvention af 23. november 2001 om IT-kriminalitet*.

[143] N. Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', 21:3 *Journal of Conflict & Security Law* (2016).

[144] Se for eksempel *Tallinn-manualen 2.0* (n 6), s. 35-36 og 175; Schmitt and Watts (n 121), s. 600.

[145] Det er ikke, som eksempelvis Nicholas Tsagourias giver udtryk for, en generel forudsætning for folkeretlig regulering af ikke-statslige aktører, at de opfylder bestemte betingelser vedrørende effektiv kontrol over territorium eller lignende, jf. Tsagourias (n 143), s. 467ff. Men en eventuel regulering af ikke-statslige aktørers adfærd i cyberdomænet ville naturligvis skulle tage højde for relevante eksisterende folkeretlige, herunder menneskeretlige, regler. For så vidt angår individers og andre ikke-statslige aktørers rolle i folkeretlige system, se A. Kjeldgaard-Pedersen, *The International Legal Personality of the Individual* (Oxford University Press, Oxford, 2018).

[146] Et kort overblik over diskussionen og den relevante praksis findes eksempelvis i G. Hernandez, *International Law* (Oxford University Press, Oxford, 2019), s. 355-357. Blandt andre nylige udgivelser om emnet kan nævnes M. E. O'Connell, C. Tams & D. Tladi (red.), *Self-Defence against Non-State Actors* (Cambridge University Press, Cambridge, New York, 2019).

[147] Se *ARSIWA med kommentarer* (n 12), s. 75.

[148] Det kan efter omstændighederne være i strid med ARSIWA. Se ARSIWA, artikel 49, stk. 2 og 3.

[149] Det kan skabe udfordringer med ARSIWA, artikel 52, stk. 1.

[150] Se *Nicaragua* (n 62), præmis 205.

[151] Se bl.a. Roguski (n 135), s. 7-8.

[152] Den Faste Voldgiftsret, *Island of Palmas (Neth. v. U.S.)* 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

[153] Se M. N. Schmitt & L. Vihul, 'Respect for Sovereignty in Cyberspace', 95:7 *Texas Law Review* (2016).

[154] Se herom i Roguski (n 135), s. 4-7.

[155] Se Schmitt & Vihul (n 153), s. 1641-1642; M. N. Schmitt, 'Grey Zones in the International Law of Cyberspace', 42:2 *Yale Journal of International Law Online* (2017), s. 4-5.

[156] United Kingdom Attorney General's Office, *Cyber and International Law in the 21st Century* (tale afholdt 23. maj 2018), tilgået 23. juni 2020.

[157] United States Department of Defense, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference*, (tale afholdt 2. marts 2020), tilgået 23. juni 2020.

[158] Se også Roguski (n 135), s. 4-7.

[159] Netherlands Ministry of Foreign Affairs, *Appendix: International law in cyberspace* (2019) ('Nederlandene MFA'), s. 2, tilgået 23. juni 2020; *Ministère Des Armées* (n 11), s. 6-8.

[160] *Nederlandene MFA* (n 159), s. 2.

[161] N. Riedel, *"Cyber Security as a Dimension of Security Policy". Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office* (tale afholdt 18. maj 2015) ('Riedel'), tilgået 23. juni 2020.

[162] Se Schmitt & Vihul (n 153).

[163] Se f.eks. den østriske og tjekkiske tilgang beskrevet i P. Roguski, *The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States*, Just Security (11. maj 2020), tilgået 23. juni 2020. Se desuden forskellige sydamerikanske staters primært støttende tilgang til

spørgsmålet i D. B. Hollis, *International Law and State Cyber Operations: Improving Transparency, Fourth Report* (5. maj 2020) (OEA/Ser.Q, CJI/doc 603/20 rev.1), s. 18–20.

[164] Se f.eks. W. Banks, 'State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0', 95:7 Texas Law Review (2016); J. D. Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', 95:7 *Texas Law Review* (2016); M. N. Schmitt, '"Virtual" Disenfranchisement: Cyber Election Meddling in the Gray Zones of International Law', 19:1 *Chicago Journal of International Law* (2018); N. Tsagourias, 'Electoral Cyber Interference, Self-Determination and The Principle of Non-Intervention in Cyberspace', i D. Broeders & B. van den Berg (red.), *Governing Cyberspace: Behavior, Power and Diplomacy* (Rowman & Littlefield Publishers, Lanham, London, 2020).

[165] Se *Nicaragua* (n 62), præmis 191 and 211.

[166] Se f.eks. A. Randelzhofer & O. Dörr, 'Article 2 (4)', i B. Simma et al (red.), *The Charter of the United Nations: A Commentary*, (Oxford University Press, Oxford, 2012), s. 208.

[167] *Nicaragua* (n 62), præmis 228.

[168] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, s. 226.

[169] *Ibid.*, para. 39.

[170] Se bl.a. *Nicaragua* (n 62), præmis 183-195. Se også C. Gray, *International Law and the Use of Force* (Oxford University Press, Oxford, 2018), s. 12.

[171] Randelzhofer & Dörr (n 166), s. 208-210.

[172] *Ibid.*, s. 210.

[173] Group of Governmental Experts, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2015) (UN Doc. A/70/174), s. 12; M. Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, Oxford, 2014), s. 53; *Tallinn-manualen 2.0* (n 6), s. 330; Roguski (n 135), s. 9.

[174] I den forbindelse er det værd at minde om, at det ikke er mange år siden, at den daværende Legal Adviser for det amerikanske udenrigsministerium, Harold Koh, indledte en tale med at spørge sig selv, om de grundlæggende folkeretlige principper overhovedet finder anvendelse i cyberspace. Selv om Koh svarede "ja", er det påfaldende, at det for så kort tid siden blev fundet nødvendigt overhovedet at bringe spørgsmålene på banen. Se H. H. Koh, 'International Law in Cyberspace Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012' 54 *Harvard International Law Journal* (2012), s. 2-3.

[175] Bemærk, at da Anders Henriksen i 2012 udgav *Cyberkrig: Folkeretten og computer network operations* blev det understreget, at det var for tidligt at konkludere på, om stater ville anlægge denne tilgang. Se Henriksen (n 32), s. 13.

[176] Se bl.a. Koh (n 174), s. 4; *United Kingdom Attorney General's Office* (n 156); *President of Estonia* (n 11); *Ministère Des Armées* (n 11), s. 7; *Nederlandene MFA* (n 159), s. 3; Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (oktober 2017), s. 90, tilgået 23. juni 2020; *Riedel* (n 161). Se om den akademiske tilgang i Roscini (n 173), s. 47-49 (Roscini anvender dog en modificeret udgave af tilgangen); C. Kress, 'On the Principle of Non-Use of Force in Current International Law', Just Security (30. September 2019), tilgået 23. juni 2020. Der er desuden

bemærkelsesværdigt, at tilgangen øjensynlig modtog enstemmig opbakning blandt eksperterne bag *Tallinn-manualen 2.0*. Se *Tallinn manualen 2.0* (n 6)*,* regel 69 med bemærkninger.

[177] Se *Nicaragua* (n 62), præmis 195.

[178] R. Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', 17:2 *Journal of Conflict and Security Law* (2012), s. 212. Se en gentagelse af dette grundlæggende synspunkt i Buchan (n 19), s. 65-68.

[179] Roscini (n 173), s. 55.

[180] Se S. Haataja, *Cyber Attacks and International Law on the Use of Force: the Turn to Information Ethics* (Routledge, Abingdon, New York, 2019), s. 95; Haataja (n 78), s. 7.

[181] Kress (n 176).

[182] International Law Association, Committee on the Use of Force (2010-2018), *Final Report on Aggression and the Use of Force*, Sydney Conference (2018), s. 26.

[183] *Tallinn-manualen 2.0* (n 6), regel nr. 69.

[184] *Nicaragua* (n 62), præmis 195.

[185] *Tallinn-manualen 2.0* (n 6), s. 333.

[186] *Ibid*, s. 334-336.

[187] *Nederlandene MFA* (n 159), s. 3-4.

[188] *Ibid.,* s. 4.

[189] *Ministère Des Armées* (n 11), s. 7.

[190] *Commonwealth of Australia* (n 176), s. 90.

[191] *Ibid.,* s. 90.

[192] *Riedel* (n 161).

[193] *Ibid.*

[194] *President of Estonia* (n 11).

[195] *Ibid.*

[196] *United Kingdom Attorney General's Office* (n 156).

[197] Koh (n 174), s. 4-5.

[198] United States Department of Defense (n 157).

[199] Se bl.a. Y. Dinstein, 'Computer Network Attacks and Self-Defence' 76 *International Law Studies Series US Naval War College* (2002), s. 105; H. H. Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, Cambridge, 2012), s. 68 og 74.

[200] Se bl.a. D. B. Silver, 'Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter' 76:1 *International Law Studies Series US Naval War College* (2002), s. 85; S. J. Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' 27:1 *Berkeley Journal of International Law* (2009), s. 231; C. Joyner and C. Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' 12:5 *European Journal of International Law* (2001), s. 849-850; og *Tallinn-manualen 2.0* (n 6), s. 333-337.

[201] Se bl.a. M. N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', 37:3 *Columbia Journal of Transnational Law* (1999), s. 885-938; J. Barkham, 'Information Warfare and International Law on the Use of Force', 34 *New York University Journal of*

International Law and Politics (2001), s. 88-91; E. T. Jensen, 'Computer Attacks on Critical State Infrastructure: A Use of Force Invoking the Right of Self-Defence', 38 *Stanford Journal of International Law* (2002), s. 222–29; H. S. Lin, 'Offensive Cyber Operations and the Use of Force', 4:63 *Journal of National Security Law and Policy* (2010), s. 63-86; N. Tsagourias, 'Cyber attacks, self-defence and the problem of attribution', 17:2 *Journal of Conflict & Security Law* (2012), s. 229-244; Roscini (n 173), s. 55.

[202] Det bemærkes, at Danmark bl.a. i arbejdet under OEWG har udtalt sig om pre-drafts og taget del i fællesinitiativer, der omfatter indsamling af statsudtalelser. Se Permanent Mission of Denmark to the United Nations, *Denmark's response to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security* (16. april 2019), tilgået 23. juni 2020; Australien et al, *Open Ended Working Group Developments in the field of information and telecommunications in the context of international security, Joint Proposal* (16. april 2020), tilgået 23. juni 2020.

[203] Se bl.a. Moynihan (n. 8), s. 58, anbefaling ii; Roguski (n 135), s. 24.

Referencer

Alland, D., 'Countermeasures of General Interest', 13:5 *European Journal of International Law* (2002)

Alland, D., 'The Definition of Countermeasures' i J. Crawford, A. Pellet & S. Olleson (red.), *The Law of International Responsibility* (Oxford University Press, Oxford, 2010)

Australien et al, *Open Ended Working Group Developments in the field of information and telecommunications in the context of international security, Joint Proposal* (16. april 2020)

Banks, W., 'State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0', 95:7 *Texas Law Review* (2016)

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

Beredskabsstyrelsen, *Danskernes Risikoopfattelse – Spørgeskemaundersøgelse, Rapport 2019* (2019)

Buchan, R., 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', 17:2 *Journal of Conflict and Security Law* (2012)

Buchan, R., 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21 *Journal of Conflict & Security Law* (2016)

Buchan, R., *Cyber Espionage and International Law* (Hart Publishing, Oxford, 2019)

Center for Cybersikkerhed, *Trusselssvurdering: Cybertruslen mod Danmark 2019* (marts 2019)

Center for Cybersikkerhed, *Trusselssvurdering: Cybertruslen mod Danmark 2020* (juni 2020)

Charney, J. I., 'Third State Remedies in International Law', 10:1 *Michigan Journal of International Law* (1989)

Chesterman, S., "The Spy Who Came in from the Cold War: Intelligence and International Law." 27:4 *Michigan Journal of International Law* (2006)

Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy* (oktober 2017)

Crawford, J., *Third report on State responsibility, by Mr. James Crawford, Special Rapporteur* (2000) (UN Doc. A/CN.4/507)

Crawford, J., *Fourth report on State responsibility, by Mr. James Crawford, Special Rapporteur* (2001) (UN Doc. A/CN.4/517)

Crawford, J., *State Responsibility: The General Part* (Cambridge University Press, Cambridge, 2013)

Crawford, J., Peel, J. & Olleson, S., 'The ILC's Articles on Responsibility of States for Internationally Wrongful Acts: Completion of the Second Reading', 12:5 *European Journal of International Law* (2001)

Dawidowicz, M., *Third-Party Countermeasures in International Law* (Cambridge University Press, Cambridge, 2017)

Den Faste Voldgiftsret, *Island of Palmas (Neth. v. U.S.)*, 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928)

Den Internationale Domstol, *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*, Judgment (Merits), I.C.J. Reports 1949, s. 22

Den Internationale Domstol, *United States Diplomatic and Consular Staff in Tehran*, Judgment, I.C.J. Reports 1980, s. 3

Den Internationale Domstol, *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)*. Merits, Judgment, I.C.J. Reports 1986, s. 14

Den Internationale Domstol, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, s. 226

Den Internationale Domstol, *Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)*, Judgment, I.C.J. Reports 1997, s. 7

Den Internationale Domstol, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, s. 43

Den Internationale Lovkommission, *Yearbook of the International Law Commission (1996), Vol. II, Part. 2* (1996) (UN Doc. A/CN.4/SER.A/1996/Add.l (Part 2))

Den Internationale Lovkommission, *Report of the International Law Commission on the work of its fifty-second session (2000): Topical summary of the discussion held in the Sixth Committee of the General Assembly during its fifty-fifth session prepared by the Secretariat* (2000) (UN Doc. A/CN.4/513)

Den Internationale Lovkommission, *Report of the International Law Commission*, Fifty-Second Session, Supp. No. 10 (2000) (U.N. Doc. A/55/10)

Den Internationale Lovkommission, 'Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries', *Yearbook of the International Law Commission* (2001) Vol. II, Part Two, as corrected

Den Internationale Lovkommission, *Sixth Committee, Summary of Record of Meetings*, (9. November 2001) (UN Doc. A/C.6/56/SR.11)

Den Internationale Lovkommission, *State responsibility — Comments and observations received from Governments* (2001) (UN Doc. A/CN.4/515 and Add. 1-3)

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

Dinstein, Y., 'Computer Network Attacks and Self-Defense', 76 *International Law Studies Series US Naval War College* (2002)

Forsvarets Efterretningstjeneste, *Efterretningsmæssig risikovurdering 2004* (december 2004)

Forsvarets Efterretningstjeneste, *Efterretningsmæssig risikovurdering 2010* (august 2010)

Forsvarets Efterretningstjeneste, *Efterretningsmæssig risikovurdering 2011* (oktober 2011)

Forsvarets Efterretningstjeneste, *Efterretningsmæssig risikovurdering 2019* (november 2019)

Group of Governmental Experts, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2015) (UN Doc. A/70/174)

Gray, C., *International Law and the Use of Force* (Oxford University Press, Oxford, 2018)

Haataja, S., *Cyber Attacks and International Law on the Use of Force: the Turn to Information Ethics,* (Routledge, Abingdon, New York, 2019)

Haataja, S., 'Cyber Operations and Collective Countermeasures under International Law', 25:1 *Journal of Conflict and Security Law* (2020)

Henriksen, A., *Cyberkrig: Folkeretten og computer network operations*, Center for Militære Studier (april 2012)

Henriksen, A., *Folkeretten og modreaktioner i cyberspace*, Center for Militære Studier (februar 2014)

Hernandez, G., *International Law* (Oxford University Press, Oxford, 2019)

Hollis, D. B., *International Law and State Cyber Operations: Improving Transparency, Fourth Report* (5. Maj 2020) (OEA/Ser.Q, CJI/doc 603/20 rev.1)

International Law Association, Committee on the Use of Force (2010-2018), *Final Report on Aggression and the Use of Force*, Sydney Conference (2018)

Jensen, E. T., 'Computer Attacks on Critical State Infrastructure: A Use of Force Invoking the Right of Self-Defence', 38 *Stanford Journal of International Law* (2002)

Joint statement by the Governments of the Ten States members of the European Community concerning the Falkland Islands issued at Brussels on 10 April 1982 (14. April 1982) (UN Doc. S/14976)

Joyner, C. & Lotrionte, C., 'Information Warfare as International Coercion: Elements of a Legal Framework', 12:5 *European Journal of International Law* (2001)

Kish, J. & Turns D., *International Law and Espionage* (Martinus Nijhoff Publishers, The Hague, Boston, 1995)

Kjeldgaard-Pedersen, A., *The International Legal Personality of the Individual* (Oxford University Press, Oxford, 2018)

Koh, H. H., 'International Law in Cyberspace Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012' 54 *Harvard International Law Journal* (2012)

Kress, C., *On the Principle of Non-Use of Force in Current International Law*, Just Security (30. September 2019)

Liebetrau, T., *Dansk offensiv cybermagt mellem angreb, spionage og forsvar: en komparativ analyse på tværs af Europa*, Center for Militære Studier (maj 2020)

Lin, H. S., 'Offensive Cyber Operations and the Use of Force', 4:63 *Journal of National Security Law and Policy* (2010)

Ministère Des Armées, *Droit International Appliqué Aux Opérations Dans le Cyberspace* (2019)

Moynihan, H., *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention*, Chatham House (december 2019)

NATO, *Cyber Defence Factsheet* (februar 2018)

Netherlands Ministry of Foreign Affairs, *Appendix: International law in cyberspace* (2019)

O'Connell, M. E, C. Tams, & D. Tladi (red.), *Self-Defence against Non-State Actors* (Cambridge University Press, Cambridge, New York, 2019)

Ohlin, J. D., 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', 95 *Texas Law Review* (2016)

Permanent Mission of Denmark to the United Nations, *Denmark's response to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security* (16. april 2019)

Petman, J. M., 'Resort to Economic Sanctions by Not Directly Affected States', i L. P. Forlati & L.-A. Sicilianos (red.) *Les sanctions économiques en droit international/Economic Sanctions in International Law* (Hague Academy of International Law & Martinus Nijhoff Publishers, Leiden, Bosten, 2004)

President of Estonia, *President of the Republic at the opening of CoCon 2019* (2019)

Proukaki, E. K., *The Problem of Enforcement in International Law: Countermeasures, the Non-injured State and the Idea of International Community* (Routledge, New York, 2010)

Radsan, A. J., 'The Unresolved Equation of Espionage and International Law', 28:3 *Michigan Journal of International Law* (2007)

Randelzhofer, A. & O. Dörr, 'Article 2 (4)', i B. Simma et al (red.), *The Charter of the United Nations: A Commentary* (Oxford University Press, Oxford, 2012)

Riedel, N. *"Cyber Security as a Dimension of Security Policy". Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office"* (tale afholdt 18. maj 2015)

Roguski, P., 'Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?', *12th International Conference on Cyber Conflict: 20/20 Vision – The Next Decade* (2020)

Roguski, P., *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program for Cyber Norms Policy Brief (marts 2020)

Roguski, P., *The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States*, Just Security (11. maj 2020)

Roscini, M., *Cyber Operations and the Use of Force in International Law* (Oxford University Press, Oxford, 2014)

Schmitt, M. N., 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', 37:3 *Columbia Journal of Transnational Law* (1999)

Schmitt, M. N. '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' 54:3 *Virginia Journal of International Law* (2014)

Schmitt, M. N. (red.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, Cambridge, 2013)

Schmitt, M. N. (red.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, Cambridge, 2017)

Schmitt, M. N., 'Grey Zones in the International Law of Cyberspace', 42:2 *Yale Journal of International Law Online* (2017)

Schmitt, M. N., '"Virtual" Disenfranchisement: Cyber Election Meddling in the Gray Zones of International Law', 19:1 *Chicago Journal of International Law* (2018)

Schmitt, M. N. & L. Vihul, 'Respect for Sovereignty in Cyberspace', 95:7 *Texas Law Review* (2016)

Schmitt, M. N. and Watts, S., 'Beyond State-Centrism: International Law and Non-state Actors in Cyberspace', 21:3 *Journal of Conflict & Security Law* (2016)

Shackelford, S. J., 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', 27:1 *Berkeley Journal of International Law* (2009)

Silver, D. B., 'Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter', 76:1 *International Law Studies Series US Naval War College* (2002)

Tams, C., *Enforcing Obligations Erga Omnes in International Law* (Cambridge University Press, Cambridge, 2005)

Trade Restrictions Affecting Argentina Applied For Non-Economic Reasons (5. maj 1982) (L/5319)

Tsagourias, N., 'Cyber attacks, self-defence and the problem of attribution', 17:2 *Journal of Conflict & Security Law* (2012)

Tsagourias, N., 'The Law Applicable to Countermeasures against Low-Intensity Cyber Operations', 14:1 *Baltic Yearbook of International Law* (2014)

Tsagourias, N., 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', 21:3 *Journal of Conflict & Security Law* (2016)

Tsagourias, N., 'Electoral Cyber Interference, Self-Determination and The Principle of Non-Intervention in Cyberspace', i Dennis Broeders & Bibi van den Berg (red.), *Governing Cyberspace: Behavior, Power and Diplomacy* (Rowman & Littlefield Publishers, Lanham, London, 2020)

United Kingdom Attorney General's Office, *Cyber and International Law in the 21st Century*, (tale afholdt 23. maj 2018)

United States Department of Defense, *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference* (tale afholdt 2. marts 2020)