CENTER FOR MILITÆRE STUDIER
KØBENHAVNS UNIVERSITET

Cyberkrig

Folkeretten og computer network operations

Anders Henriksen

April 2012

Denne rapport er en del af Center for Militære Studiers forskningsbaserede myndighedsbetjening af Forsvarsministeriet. Formålet med rapporten er at belyse, hvorledes computer network operations reguleres i den del af folkeretten, der regulerer interstatslig magtanvendelse, samt hvilke udfordringer reguleringen skaber for forsvaret og Danmark. Rapporten indeholder i den forbindelse en række anbefalinger til, hvorledes Danmark kan bidrage til at skabe større retlig klarhed i cyberspace, samtidig med at nationale danske interesser fremmes. Det påpeges endvidere, at de relevante danske myndigheder bør udarbejde klare retningslinjer for, hvordan vi fra dansk side reagerer, hvis Danmark rammes af større cyberangreb.

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

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

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

Forfatteren:
Lektor i folkeret Anders Henriksen, Det Juridiske Fakultet, Københavns Universitet.

ISBN: 978-87-7393-663-4

Abstract

It is hard to predict the legality under international law governing the use of force – *jus ad bellum* – of individual cyber attacks. In part this is due to the lack of specifically tailored legal instruments governing cyber attacks; the lack of relevant case law, such as case law from international courts, as well as the current lack of certainty with regard to the perception among states of the legality of cyber attacks. This paper nonetheless concludes that cyber attacks which constitute a form of coercion violate the ban on intervention in the domestic affairs of other states if they target areas of inviolable state sovereignty, where no foreign intervention is tolerated. It similarly concludes that cyber attacks may occasionally constitute 'force', and thereby also potentially violate the prohibition on the use of force in Article 2 (4) of the UN Charter, and in theory also constitute 'armed attacks' that trigger a right to self-defence under Article 51 of the Charter by the state that is the victim of the attacks. In light of the existing legal uncertainty surrounding cyber attacks the paper contains a number of recommendations. Firstly, Denmark should try to introduce greater legal clarity in cyberspace by considering and subsequently advocating a number of non-legally binding norms of behaviour. Furthermore, those considerations should be grounded in an overall strategic assessment of Denmark's interests in cyberspace. To that end, the paper argues, Denmark should consider cyberspace a so-called 'global common'. Secondly, guidelines should be established in the event that Denmark is made the target of extensive cyber attacks. This would require establishing an assessment of 'critical infrastructure' and drafting guidelines as to how Denmark, including the armed forces, should respond to individual cyber attacks.

Dansk resumé

Det er vanskeligt at udtale sig meget kategorisk om cyberangrebs forenelighed med de dele af folkeretten, der regulerer staters brug af international magtanvendelse – *jus ad bellum*. Det hænger bl.a. sammen med, at der endnu ikke findes folkeretlige instrumenter, der er specifikt beregnet på reguleringen af cyberangreb, at der ikke findes relevante retslige afgørelser, såsom domme fra internationale domstole, på området, og at det indtil videre er uklart, hvorledes stater forholder sig retligt til brugen af cyber. Det konkluderes imidlertid ikke desto mindre i papiret, at et cyberangreb krænker det folkeretlige forbud mod intervention, hvis det udgør en form for pression, der har til formål at påvirke en anden stats politik på et område, hvor staten ikke skal tåle international indblanding. Det konkluderes også, at det ej heller kan udelukkes, at i hvert fald nogle cyberangreb vil kunne krænke det folkeretlige magtforbud og – efter omstændighederne – sågar vil kunne udgøre væbnede angreb, der i henhold til pagtens artikel 51 udløser en ret til selvforsvar for den stat, der er udsat for angrebet. I lyset af den retlige uklarhed anbefales det i papiret, at Danmark tager de fornødne initiativer til at skabe en højere grad af retlig klarhed i cyberspace, og at der i den forbindelse indledes overvejelser om, hvilke ikke-retligt bindende *normer for adfærd* vi fra dansk side ønsker i cyberspace. Disse overvejelser bør tage afsæt i en grundlæggende analyse af Danmarks strategiske interesser i cyberspace, og det bør overvejes, om cyberspace med fordel kan betragtes som en såkaldt 'global common'. Endelig anbefales det, at der udarbejdes retningslinjer for, hvordan vi fra dansk side reagerer, hvis vi rammes af større cyberangreb. Dels bør de relevante danske myndigheder gøre sig overvejelser om, hvilke dele af den danske infrastruktur der er af særlig betydning ikke kun for et effektivt forsvar af nationen, men også for myndighedernes muligheder for at løse væsentlige samfundsopgaver. Og dels bør der udarbejdes retningslinjer for, hvordan Danmark, herunder forsvaret, reagerer på konkrete cyberangreb. Dette kunne passende tage form af udarbejdelsen af en 'cyberforholdsordre'.

Indholdsfortegnelse

Anbefalinger

Den folkeretlige regulering af cyberangreb er uklar, og dette udfordrer på en række punkter Danmark, herunder Forsvarsministeriet. I lyset af den eksisterende uklarhed indeholder dette papir følgende anbefalinger.

1. De relevante danske myndigheder bør identificere og kortlægge Danmarks strategiske interesser i cyberspace. Hvad betyder cyberspace for Danmark, og hvilke interesser har vi i cyberspace?

2. På baggrund af den strategiske analyse bør forsvaret påbegynde arbejdet med at skabe en højere grad af folkeretlig klarhed om reguleringen af CNO. Det er endnu for tidligt at gå efter egentlige bindende folkeretlige regler på området, og indtil videre må mindre derfor gøre det. Det anbefales derfor, at Danmark forsøger at opnå en højere grad af retlig klarhed ved at forsøge at påvirke de igangværende internationale bestræbelser på at opstille ikke-retligt bindende *normer for adfærd* i cyberspace, der er forenelige med Danmarks strategiske interesser. Det bør i den forbindelse overvejes, om cyberspace med fordel kan betragtes som en såkaldt 'global common'.

3. I tilknytning til bestræbelserne på at opnå international klarhed over spilleregler i cyberspace bør de relevante danske myndigheder fastlægge nogle klare retningslinjer for, hvordan vi fra dansk side reagerer, hvis Danmark rammes af større cyberangreb. Forsvaret bør i den forbindelse overveje, hvornår cyberangreb er så alvorlige, at de bør udløse danske modforanstaltninger, herunder egentlige selvforsvarshandlinger. For at lette disse overvejelser bør de relevante danske myndigheder identificere de dele af vores infrastruktur, der er særlig kritiske, og hvis destruktion og/eller lammelse må anses som særlig alvorlige angreb på Danmark. Forsvaret bør også udarbejde klare operationelle retningslinjer for, hvordan Danmark reagerer på konkrete cyberangreb. Der bør med andre ord udarbejdes en form for 'cyberforholdsordre', der kan tjene som grundlag for en indledende dansk reaktion på igangværende cyberangreb på Danmark. En sådan ordre vil endvidere bidrage til at afskrække potentielle fjender fra at gøre alvor af eventuelle planer om at udsætte Danmark for cyberangreb.

Baggrund

Det blev ved forsvarsforliget for 2010-2014 besluttet, at der oprettes en cyberkapacitet inden for 'Forsvarsministeriets område med henblik på at *forsvare egen brug af og forhindre modstanderes udnyttelse af cyberspace*.'

Dette papir er blevet udarbejdet til Forsvarsministeriets departement, der med henblik på arbejdet med at opbygge en sådan kapacitet har anmodet Center for Militære Studier ved Institut for Statskundskab på Københavns Universitet om en analyse af foreneligheden af såkaldte computer network-operationer – i det følgende benævnt 'CNO' eller 'cyberangreb' – med visse dele af folkeretten.

Der findes ingen autoritativ og universel anerkendt definition af 'CNO' eller 'cyberangreb', men den mest citerede definition stammer fra det amerikanske militær, der i 2006 definerede 'computer network attacks' (CNA) – der må anses som stort set synonymt med 'computer network-operationer' (CNO) – som værende: 'operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers or networks themselves.'[1] Denne definition fungerer som en fin arbejdsdefinition for analysen i dette papir.

Der er til brug for udarbejdelsen af dette papir blevet afholdt to møder med repræsentanter for Forsvarsministeriet, der havde til formål at klarlægge de nærmere rammer for den ønskede retlige analyse. Der har endvidere været afholdt et kortere studiebesøg i Washington, D.C., USA, hvor der var lejlighed til at drøfte centrale problemstillinger med repræsentanter for det amerikanske forsvarsministeriums nyligt oprettede Cyber Command. Der blev ved samme lejlighed også holdt møder med forskellige ressourcepersoner på George Washington University og i sikkerhedspolitiske tænketanke. Som led i den afsluttende del af arbejdet blev der endelig aflagt et besøg på NATO's Cooperative Cyber Defence Centre Of Excellence (CCDCOE) i Tallinn, Estland.

Efter ønske fra Forsvarsministeriet koncentreres analysen i papiret om de dele af folkeretten, der vedrører reguleringen af staters brug af international magtanvendelse – også betegnet *jus ad bellum*. Notatet forholder sig på den baggrund hverken til foreneligheden af CNO med de dele af folkeretten, der regulerer væbnede konflikter (den humanitære folkeret) – *jus in bello* – eller til CNO's eventuelle overensstemmelse med de internationale menneskerettigheder, herunder Danmarks forpligtelser i henhold til Den Europæiske Menneskerettighedskonvention. Det er imidlertid værd at understrege, at der (også) på disse områder er stor retlig uklarhed, og at der derfor synes at være al mulig grund til, at Forsvarsministeriet tager de fornødne initiativer til at belyse retsgrundlaget. Det kan i den forbindelse til orientering oplyses, at der på foranledning

af det ovennævnte CCDCOE efter planen skal udkomme en manual for CNO's forenelighed med den humanitære folkeret i løbet af 2012.

Notatet er bygget op om den ønskede konkrete retlige analyse af foreneligheden af CNO med *jus ad bellum*, men da der på nuværende tidspunkt hersker en vis grad af uklarhed om den folkeretlige retsstilling på området, suppleres den retlige analyse med en opregning af nogle af de udfordringer – men også muligheder – der er forbundet med denne uklarhed.

Papiret afspejler, at de fleste akademiske bidrag på området indtil videre stammer fra amerikanske folkeretsforfattere. Det skyldes det helt simple forhold, at debatten om foreneligheden af cyber med folkeretten er mere udviklet i USA. Det er ikke desto mindre blevet tilstræbt at gengive et repræsentativt udpluk af opfattelser i den folkeretlige litteratur.

Papiret indledes nedenfor med bestræbelserne på at vurdere foreneligheden af CNO med *jus ad bellum*. Herefter vender gennemgangen sig mod nogle af de udfordringer og muligheder, der er forbundet med den aktuelle retlige usikkerhed. Notatet rundes af med en kort opsummering af de centrale konklusioner og et par konkrete anbefalinger til brug for det videre arbejde med udviklingen af en cyberkapacitet i Forsvarsministeriet.

CNO og jus ad bellum

Indledning

I dette afsnit vil det blive vurderet, hvorledes CNO reguleres af den del af folkeretten, der regulerer staters brug af international magt – *jus ad bellum*. Den materielle analyse af dette spørgsmål er delt op i fem afsnit. I afsnit 3 gives der et bud på, om – og i givet fald under hvilke omstændigheder – cyberangreb strider mod det folkeretlige forbud mod 'intervention' i andre staters indre anliggender. I afsnit 4 diskuteres det, hvorvidt CNO udgør brug af 'magt' i henhold til magtforbudsreglen i FN-pagtens artikel 2, stk. 4, inden det i afsnit 5 vurderes, om cyberangreb kan udgøre et 'væbnet angreb', der udløser en ret til selvforsvar i henhold til pagtens artikel 51. I afsnit 6 rettes opmærksomheden mod de foranstaltninger, som en stat kan iværksætte, når den gøres til genstand for ulovlige handlinger, såsom cyberangreb, inden der i afsnit 7 til sidst vil blive gjort et forsøg på at anvende de retlige konklusioner i papiret på en række konkrete eksempler på cyberangreb fra virkelighedens verden. Inden den materielle gennemgang gøres der imidlertid indledningsvis umiddelbart nedenfor i afsnit 2 en række betragtninger om, hvorfor det på nuværende tidspunkt er vanskeligt at udtale sig meget skråsikkert om cyberangrebs forenelighed med folkeretten.

CNO og den retlige uklarhed

Ny teknologi og nye former for krigsførelse skaber ofte forvirring om det retlige grundlag, og der er derfor intet mærkværdigt i, at fremkomsten af cyber er omgærdet af retlig uklarhed. Et klassisk eksempel på vanskelighederne ved at forene ny teknologi med eksisterende folkeretlige normer var den folkeretlige usikkerhed, der i 1920'erne og 1930'erne omgærdede reguleringen af den nye brug af luftmagt, og et nyere eksempel er diskussionerne i det seneste årti om reguleringen af anvendelsen af droneteknologi.[2] Cyber passer med andre ord ind i et historisk mønster, hvor nye teknologier med mellemrum udfordrer det folkeretlige system. Som Matthew C. Waxman bemærker om de aktuelle retlige udfordringer forbundet med reguleringen af cyber:

> … these fundamental issues are not entirely new or unique to cyber-technology, even if they have new dimensions that make them harder to solve or navigate. Modes and technologies of conflict change, and the law adjusts with varying degrees of success to deal with them. Throughout the U.N. Charter regime's sixty-plus years of development, the means by which states and international actors wage conflict have changed so dramatically that every so often major international legal figures debate whether the Charter's most basic tenets are "dead". Cyber-warfare capabilities and vulnerabilities will strain the Charter and its basic prohibition on force once again … [3]

Alt dette ændrer imidlertid ikke på, at det på nuværende tidspunkt *er* særdeles vanskeligt at udtale sig med nogen nævneværdig grad af sikkerhed om cyberangrebs forenelighed med centrale dele af folkeretten.

Usikkerheden skyldes først og fremmest, at der (endnu) ikke findes folkeretlige instrumenter, der er *specifikt* beregnet på reguleringen af staters cyberangreb. Der findes ganske vist en konvention vedrørende

samarbejde staterne imellem på området for bekæmpelse af *cyberkriminalitet*[4], men denne konvention er ikke umiddelbart relevant for vurderingen af, hvornår CNO krænker de dele af folkeretten, der regulerer staters brug af international magt.

Fraværet af mere specifikke regler gør, at der ikke er noget alternativ til at forsøge at anvende de eksisterende *generelle* regler på cyberangreb, men det er desværre lettere sagt end gjort. Det mest centrale folkeretlige instrument på området er FN-pagten, der har som sit primære formål at sikre opretholdelsen af international fred og sikkerhed. Pagten udgør den folkeretlige rygrad i det internationale samfunds forsøg på at regulere staters internationale brug af magt, men pagten er fra 1945 og dermed også fra en tid, hvor computeren endnu ikke var opfundet, og hvor man derfor ikke gjorde sig tanker om, hvorledes staters aktiviteter i cyberspace skulle reguleres. På tidspunktet for oprettelsen af pagten var fokus i det internationale samfund rettet mod den netop afsluttede verdenskrig, og bestræbelserne på at undgå endnu en verdensomspændende blodig konflikt tog derfor også først og fremmest afsæt i et forsøg på at regulere de former for (konventionel) interstatslig magtanvendelse, såsom luftbombardementer og troppefremrykninger, der netop havde taget livet af millioner af mennesker.

Fokuseringen på traditionel – kinetisk – magtanvendelse i FN-pagten gør det naturligvis vanskeligt at vurdere, hvorledes man folkeretligt skal forholde sig til nye og mere 'ikke-konventionelle' våbenteknologier, såsom cyber. Som Daniel T. Kuehl formulerer det:

> Our existing paradigm for war requires kinetic actions, destroying things, or crossing of physical boundaries with physical objects such as airplanes or tanks. What are the political and legal regimes for actions that do not cross the physical limits of territorial sovereignty or cause kinetic destruction, but still have serious impact on the national security of the "attacked" State? Where are the lines of sovereignty in cyberspace, and how does the State respond to the provocations and intrusions of what may be a shadowy and virtual opponent?[5]

Problemerne har til dels at gøre med karakteren af cyberangreb, der, som Michael N. Schmitt formulerer det, udfordrer

> … the prevailing paradigm, for its consequences cannot easily be placed in a particular area along the community values threat continuum. The dilemma lies in the fact that CNA spans the spectrum of consequentiality. Its effects freely range from mere inconvenience … to physical destruction … to death … It can affect economic, social, mental, and physical well-being, either directly or indirectly, and its potential scope grows almost daily, being capable of targeting everything from individual persons or objects to entire societies.[6]

En anden årsag til den aktuelle retlige uklarhed er, at der endnu ikke findes retslige afgørelser eller domme, der tager stilling til foreneligheden af cyberangreb med folkeretten. Den Internationale Domstol tog i en vejledende udtalelse i 1996 stilling til, om anvendelsen af atomvåben var foreneligt med folkeretten, og domstolen bidrog ved samme lejlighed til at skabe større retlig klarhed over et område, der i årtier havde

været genstand for massiv folkeretlig debat. En tilsvarende udtalelse om cyberangreb findes imidlertid (endnu) ikke.

Det er også svært at udtale sig skråsikkert om foreneligheden af cyberangreb med folkeretten, fordi vi mangler viden om, hvordan staterne i det internationale samfund forholder sig retligt til brugen af cyber. Det er i den forbindelse værd at huske på, at det først og fremmest er *stater*, der skaber og udvikler folkeretten, og at det derfor også først og fremmest er op til stater at vurdere, om konkrete cyberangreb er forenelige med centrale folkeretlige principper. Udviklingen af cyberspace er (formentlig) fortsat på et meget tidligt stadium, og verden har kun været vidne til relativt få (offentliggjorte) cyberangreb, der har givet stater anledning til at forholde sig konkret til lovligheden af denne type angreb. Så mens vi ved, hvordan staterne forholder sig retligt til affyringen af missiler eller fremrykningen af kampvogne, så ved vi endnu ikke særlig meget om, hvordan de forholder sig til brugen af cyber.

I en rapport fra 1999 noterede det amerikanske forsvarsministerium sig da også følgende om anvendelsen af de eksisterende folkeretlige principper på cyberangreb:

> There is no way to be certain how these principles of international law will be applied by the international community to computer network attacks. As with other developments in international law, much will depend on how the nations and international institutions react to the particular circumstances in which these issues are raised for the first time.[7]

På nuværende tidspunkt er det med andre ord særdeles vanskeligt at udtale sig om, hvorvidt – og i givet fald under hvilke omstændigheder – cyberangreb strider mod folkeretten.

I det følgende vil der ikke desto mindre alligevel blive gjort et forsøg. Det skal i den forbindelse bemærkes, at der primært er tre måder, hvorpå cyberangreb kan iværksættes. Cyberangreb kan iværksættes enten 1) *uden forbindelse* til et konventionelt angreb, 2) som led i *forberedelserne* til et konventionelt angreb eller 3) som led i et *igangværende* konventionelt angreb.

I det følgende er fokus først og fremmest rettet mod den første type cyberangreb og altså mod at afklare, hvorledes cyberangreb, der iværksættes uden forbindelse til et konventionelt angreb, reguleres. Det skal i den forbindelse bemærkes, at gennemgangens primære fokus er rettet mod at afklare, hvornår *staters* brug af cyber er uforenelig med folkeretten.[8]

Forbuddet mod intervention

Det første – og laveste – niveau af folkeretsstridig interstatslig 'indblanding' kommer til udtryk i det såkaldte 'ikke-interventionsprincip'[9], der udspringer af det folkeretlige princip om, at alle suveræne stater er berettigede til at udvikle sig uden fremmed indblanding.[10] Ikke-interventionsprincippet genfindes ikke udtrykkeligt i FN-pagten[11], men det er opregnet i en lang række deklarationer fra FN's Generalforsamling, hvoraf den væsentligste er deklarationen om venskabelige forbindelser fra 1970. Denne lyder bl.a.:

> No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.
> No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it advantages of any kind.[12]

Princippet genfindes endvidere i afgørelser fra Den Internationale Domstol, herunder i afgørelsen i *Nicaragua*, hvor domstolen bl.a. henviste til ovennævnte resolution og ved samme lejlighed konkluderede, at ikke-interventionsprincippet har karakter af folkeretlig sædvane.[13]

Det præcise omfang af ikke-interventionsprincippet er omtvistet, og det hænger bl.a. sammen med, at mange af de Generalforsamlingsresolutioner, hvori der henvises til princippet, ikke er retligt bindende for staterne og næppe udtrykker bindende sædvaneret.[14]

Princippet består i praksis af to delelementer. Det første er et krav om, at der skal være en konkret *intervention*, og det andet er en betingelse om, at denne intervention skal være rettet mod *forhold, som alle stater er berettigede til at bestemme selv uden fremmed indblanding.*[15]

Det er uklart, hvilke handlinger der udgør en 'intervention' i ikke-interventionsprincippets forstand, og der er formentlig grund til at være lidt tilbageholdende med at tillægge forbuddet en meget stor rækkevidde.[16] Skillelinjen synes under alle omstændigheder formentlig at gå ved *pression* ('coercion'), og hvis en handling ikke er et forsøg på at presse en anden stat, så kan handlingen næppe udgøre en 'intervention'.[17]

Der er en tæt forbindelse mellem ikke-interventionsforbuddet og det folkeretlige forbud mod brug af egentlig magt (se herom nedenfor), men begrebet 'intervention' dækker utvivlsomt bredere end magtbegrebet, der kun udtrykker en del af et mere vidtgående forbud mod indblanding i andre staters anliggender. Interventionsforbuddet er eksempelvis ikke begrænset til væbnet pression, og også andre former for pression, såsom økonomisk eller politisk pression, vil efter omstændighederne kunne falde ind under forbuddet.

Det andet element i interventionsforbuddet er kravet om, at interventionen skal være rettet mod

forhold, som alle stater er berettigede til at bestemme selv uden fremmed indblanding. Interventionen skal have til formål at *ændre politikken* i en anden stat, og kun de handlinger, der sigter mod at påvirke de valg, som en anden stat foretager, udgør folkeretsstridig intervention. Også denne betingelse er imidlertid vanskelig at anvende i praksis, da det ofte kan være særdeles vanskeligt at vurdere motiver bag staters handlinger og undladelser.

Det kan på baggrund af det ovennævnte udledes, at cyberangreb vil kunne krænke forbuddet mod intervention, hvis de udgør en form for pression, der har til formål at påvirke en anden stats politik på et område, hvor staten ikke skal tåle international indblanding.[18]

Foreneligheden af konkrete CNO-angreb med interventionsforbuddet vil altid afhænge af en konkret vurdering, men inkluderingen af økonomisk pression inden for rammerne af interventionsforbuddet øger chancen (eller risikoen, om man vil) for, at cyberangreb mod andre staters økonomiske infrastruktur, såsom den finansielle sektor eller elektroniske betalingssystemer, vil være at anse som ulovlig indblanding.

Det skal dog understreges, at det formentlig tillægges betydning, om et cyberangreb mod en stats elektroniske infrastruktur krydser den territoriale grænse og rettes mod mål *inde i* staten, eller om angrebet alene rettes mod mål *uden for* statens territorium, såsom mod den elektroniske trafik, der går ind i og ud af staten. Handlinger mod mål, der geografisk befinder sig i den stat, der er mål for angrebet, vil efter en umiddelbar betragtning nemmere kunne komme i konflikt med ikke-interventionsforbuddet.

Forbuddet mod trussel om magtanvendelse eller brug af magt

Interventioner i andre stater, der involverer brug af egentlig 'magt', falder potentielt set ikke bare ind under forbuddet mod intervention, men også under FN-pagtens magtforbudsregel i artikel 2, stk. 4:

> Alle medlemmer skal i deres mellemfolkelige forhold afholde sig fra trussel om magtanvendelse eller brug af magt; det være sig mod nogen stats territoriale integritet eller politiske uafhængighed eller på nogen anden måde, der er uforenelig med de Forenede Nationers formål.

Som så mange andre bestemmelser i pagten har også artikel 2, stk. 4, været genstand for massiv international debat siden oprettelsen af FN i 1945[19], og i relation til analysen i dette papir er det relevante spørgsmål naturligvis først og fremmest, hvad der ligger i begrebet 'magt'.

Der har fra starten været forskellige fortolkninger af magtbegrebet i artikel 2, stk. 4, men den traditionelle opfattelse har været, at 'magt' forudsætter brugen af militære eller i det mindste *væbnede* virkemidler, og at ikke-væbnede virkemidler, såsom økonomisk og politisk pression, ikke er omfattet.[20]

Til støtte herfor taler, at det af forarbejderne til pagten fremgår, at der ikke var opbakning til et forslag fra Brasilien om at udvide magtbegrebet til at inkludere økonomiske virkemidler[21], og at det ej heller i forbindelse med forhandlingerne om vedtagelsen af efterfølgende resolutioner og deklarationer var muligt at opnå enighed i FN om at udvide begrebet til økonomisk pression.[22]

Det hører også med til historien, at Den Internationale Domstol endnu ikke har fundet, at økonomisk pression skulle kunne være omfattet af magtforbuddets rækkevidde. I *Nicaragua* gjorde Nicaragua gældende, at det var udsat for massivt økonomisk pres fra USA, der bl.a. blev beskyldt for at yde økonomisk støtte til oprørere, der søgte at vælte den siddende regering, men domstolen fandt ikke, at de amerikanske handlinger – til trods for deres uforenelighed med interventionsforbuddet – udgjorde magt.

Den traditionelle opfattelse af, at ikke-væbnede handlinger, såsom økonomisk og politisk pression, ikke hører under magtforbuddet i artikel 2, stk. 4, betyder, at mange cyberangreb må forventes at falde uden for forbuddets rammer.

Der bør ikke desto mindre udvises en vis forsigtighed på dette punkt. I sin vejledende udtalelse i *Nuclear Weapons* bemærkede Den Internationale Domstol nemlig følgende om pagtens regler om magtanvendelse:

> These provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons used. The Charter neither expressly prohibits, nor permits, the use of any specific weapon …[23]

Domstolen åbnede herved også mulighed for, at der muligvis anlægges en *effektbaseret* tilgang til magtbegrebet, hvorefter det afgørende ikke er, *hvilket våben* der anvendes, men derimod om *virkningen* af en handling er kinetisk.[24] Og det vil i så fald følge heraf, at det ikke nødvendigvis er afgørende for vurderingen, om en handling rettet mod en anden stat udføres med en computer eller et missil, men derimod i stedet hvilken *effekt* handlingen har på staten. Eller som Jason Barkham formulerer det: ”If an action kills people or destroys property, it is a use of force.”[25]

Det er da også den generelle antagelse, at eksempelvis biologiske og kemiske våben har karakter af ’magtanvendelse’ i henhold til artikel 2, stk. 4, selvom disse våben adskiller sig fra konventionelle (kinetiske) våben.

Det er endnu for tidligt at konkludere med sikkerhed, *om* stater vil anlægge en effektbaseret tilgang til vurderingen af, om cyberangreb er forenelige med FN-pagtens regler om magtanvendelse, men det

forekommer sandsynligt. Som det amerikanske forsvarsministerium bemærkede i sin rapport fra 1999, så er 'the consequences … likely to be more important than the means used.'[26]

Det er i den forbindelse også værd at hæfte sig ved, at flere stater, såsom USA, Storbritannien og Rusland, allerede *har* bekendtgjort, at de betragter cyberangreb som en form for magtanvendelse.[27]

Den internationale reaktion på terrorangrebene mod USA den 11. september 2001 indikerer også, at stater undertiden lægger større vægt på effekterne af en handling end på de midler, hvormed handlingen blev effektueret. Inden terrorangrebene i USA var det nemlig den overvejende opfattelse i det internationale samfund, at private terrororganisationer ikke kunne stå bag et 'væbnet angreb', der udløste en ret til selvforsvar (se herom nedenfor). Denne opfattelse var baseret dels på en antagelse om, at kun stater – og ikke private aktører – kan stå for 'væbnede angreb', og dels på, at terrorisme som middel er væsensforskellig fra de (mere konventionelle) former for magtanvendelse, der kan udløse en ret til selvforsvar. Opfattelsen ændrede sig imidlertid efter alt at dømme på grund af omfanget – og dermed *effekten* – af angrebene den 11. september, og i dag hælder de fleste til den antagelse, at private terrorangreb – hvis de er voldsomme nok – vil kunne udløse en ret til selvforsvar.[28]

En effektbaseret tilgang har naturligvis stor betydning for, om cyberangreb må forventes at kunne krænke pagtens regler om magtanvendelse, herunder magtforbudsreglen i artikel 2, stk. 4. For, som Yoram Dinstein bemærker om cyberangreb (som han betegner 'CNA'):

> The crux of the matter is not the medium at hand (a computer server in lieu of, say, an artillery battery), but the violent consequences of the action taken. If there is a cause and effect chain between the CNA and these violent consequences, it is immaterial that they were produced by high rather than low technology.[29]

Eller som Jason Barkham skriver:

> As long as the method of computer attack seems to work like a weapon by causing damage instantaneously and in a manner analogous to a conventional weapon, it is relatively easy to consider at least some types of Informational Warfare attacks uses of force.[30]

Spørgsmålet er selvfølgelig, hvornår cyber så har tilstrækkelig 'lighed' med kinetisk magt.

Ifølge Daniel B. Silver vil det være tilfældet, når den *direkte* og *forudsigelige* effekt af et cyberangreb er *fysisk* skade på personer eller ejendom, der svarer til den skade, der opstår ved brugen af konventionelle våben. Herudover bør det ifølge Silver blive tillagt betydning, hvis cyberangrebet udføres af en stats væbnede styrker.[31] Endelig vil et cyberangreb, der alene forårsager økonomisk eller politisk skade, ifølge

Silver formentlig falde uden for rækkevidden af artikel 2, stk. 4, og det gælder også, selvom et angreb måtte føre til omfattende uro i den stat, der er mål for angrebet.[32]

Christopher C. Joyner og Catherine Lotrionte lader til at være af en tilsvarende opfattelse:

> The argument seems persuasive that cyber-based activities that *directly and intentionally* result in non-combatant deaths and destruction – such as the premeditated disruption of an air traffic control system that result in the crash of a civilian airliner or the corruption of a medical database that causes civilians or wounded soldiers to receive transfusions of the wrong blood type – breach modern prohibitions on the use of force. Less clear is the case of other cyber-based activities, for example the disruption of a financial or social security system or the disclosure of confidential personal information, which produces no human injuries or property damage. These activities clearly intrude into the internal affairs of another state, but do not exceed any visible threshold of harm against which customary international law protects civilians (min kursivering).[33]

Et andet spørgsmål er, om begrebet 'ejendom' ('property') udelukkende skal forstås som ejendom i fysisk forstand, såsom fysisk infrastruktur, eller om også elektronisk 'ejendom', såsom elektroniske data, er omfattet. Dækker begrebet eksempelvis destruktion eller beskadigelse af elektroniske data, såsom data i offentlige registre, patientjournaler eller banker?

Det er endnu for tidligt at svare på dette spørgsmål, men svaret vil formentlig afhænge af en meget konkret vurdering af omstændighederne omkring og virkningerne af et givent cyberangreb.

Det skal understreges, at en betoning af effekt betyder, at det i stigende grad kan blive vanskeligt at opretholde den klassiske sondring mellem væbnede handlinger – der er omfattet af magtforbuddet – og ikke-væbnede handlinger, såsom økonomisk pression – der falder uden for.[34]

Det er imidlertid også i denne forbindelse værd at bemærke, at der som berørt i afsnit 3 formentlig sondres mellem de handlinger, der iværksættes ind over grænsen til en stat, og dem, der ikke gør. Virkemidler, der *ikke* rettes mod mål *inde* i en stat, vil kun rent undtagelsesvis kunne udgøre magt som beskrevet i artikel 2, stk. 4, og anerkendelsen af en effektbaseret tilgang til magtbegrebet betyder derfor heller ikke nødvendigvis, at eksempelvis handelssanktioner og anden form for økonomisk pression hermed også vil krænke magtforbudsreglen.[35]

Selvom en effektbaseret tilgang til magtbegrebet i artikel 2, stk. 4, betyder, at i hvert fald nogle cyberangreb vil falde ind under magtforbuddet, er det tilsyneladende ikke tilstrækkeligt til at tilfredsstille i hvert fald dele af den akademiske litteratur, der lader til at være af den opfattelse, at magtforbuddet bør underkastes en helt ny – og mere vidtrækkende – fortolkning.

Denne opfattelse er særlig tydelig i amerikanske akademiske kredse, hvor man ellers historisk har udlagt indholdet af magtforbuddet relativt snævert.[36] Som Christopher C. Joyner og Catherine Lotrionte skriver:

> The Age of Information Warfare invites reconsideration of the restrictive scope of this prohibition. The fact that one government today can use Information Warfare instruments transnationally through cyberspace to inflict damage on cyber-based facilities in another state suggests the need to reconsider a broader interpretation of the prohibition of the use of force.[37]

Enkelte amerikanske jurister er villige til at gå så langt som til at gøre gældende, at *ethvert* cyberangreb, der forsætligt forårsager *enhver form* for ødelæggelse på en anden stats territorium, er at anse som magtanvendelse i henhold til artikel 2, stk. 4.[38]

Det må imidlertid anses som meget tvivlsomt, om stater vil tilslutte sig en så vidtrækkende fortolkning af magtbegrebet, og der er derfor al mulig grund til – indtil videre i hvert fald – at holde fast i, at ønsket i den amerikanske litteratur om at underkaste magtforbuddet en ny fortolkning er et bud på, hvordan folkeretten bør være (*de lege ferenda*), frem for en udlægning af, hvordan den rent faktisk er (*de lege lata*).

Retten til selvforsvar mod et væbnet angreb

Det tredje og mest kvalificerede niveau af folkeretsstridig 'indblanding' findes i artikel 51 i FN-pagten, der regulerer staters ret til selvforsvar. Den centrale del af bestemmelsen lyder:

> Intet i nærværende pagt skal indskrænke den naturlige ret til individuelt eller kollektivt selvforsvar i tilfælde af et væbnet angreb mod et medlem af de Forenede Nationer, indtil Sikkerhedsrådet har truffet de fornødne forholdsregler til opretholdelse af mellemfolkelig fred og sikkerhed.

Hvis en stat er udsat for et 'væbnet angreb', kan den altså gribe til selvforsvar.

Men på samme måde, som det er uklart, hvad der konkret er indeholdt i begreberne 'intervention' og 'magt', er det også behæftet med vanskeligheder at vurdere, hvad der præcist menes med et 'væbnet angreb'.

Den Internationale Domstol bemærkede i sin afgørelse i *Nicaragua*, at der skal sondres mellem 'the most grave forms of the use of force' og 'other less grave forms'[39], og at 'a mere frontier incident' falder uden for begrebet væbnet angreb.[40] Det betyder, at der under alle omstændigheder eksisterer en *de minimis*-regel på området, ifølge hvilken mindre alvorlige former for magtanvendelse undtages fra begrebet væbnet angreb. Det stemmer også overens med FN's Generalforsamlings definition af aggression fra 1974.[41]

I *Nicaragua* konkluderede domstolen også, at der ikke nødvendigvis er identitet mellem den magtanvendelse, der er at anse som 'magt', og den magtanvendelse, der udgør et 'væbnet angreb'. Så ikke al

ulovlig magtanvendelse udløser altså en ret til selvforsvar[42], og der eksisterer altså en gråzone, inden for hvilken en stat nægtes ret til at forsvare sig mod ulovlig magtanvendelse, der ikke opfylder betingelserne for at udgøre et væbnet angreb.

I bestræbelserne på at definere, hvad der ligger i begrebet 'væbnet angreb', kan man med fordel skele til indholdet af definitionen af aggression, hvorefter et væbnet angreb bl.a. vil kunne være en realitet, hvis en stats væbnede styrker angriber (litra a) eller bombarderer en anden stats territorium (litra b), blokerer en anden stats havne eller kyster (litra c), angriber en anden stats land-, sø- eller luftstyrker eller "marine and air fleet" (litra d) eller befinder sig på en anden stats territorium i strid med en indgået aftale med værtsstaten herom (litra e), hvis en stat lader en anden stat bruge sit territorium til at foretage aggression mod en tredje stat (litra f), eller hvis en stat står bag udsendelsen af væbnede grupper, der foretager væbnede handlinger mod en anden stat, eller er "substantially" involveret heri (litra g).[43]

Enkelte folkeretsforfattere har herudover forsøgt at give løsere bud på, hvad der konkret ligger i et væbnet angreb, og ifølge Yoram Dinstein er væbnede angreb karakteriseret ved at være:

> use of force producing (or liable to produce) serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property. When no such results are engendered by (or reasonably expected from) a recourse to force, Article 51 does not come into play.[44]

Spørgsmålet er naturligvis, om cyberangreb kan udgøre væbnede angreb, der udløser en ret til selvforsvar. Svaret er uklart, for som Joyner og Lotrionte kort og godt bemærker: "Computer-generated intrusions and cyber-communication disruptions elude easy classification as being 'attacks'".[45] Ifølge enkelte forfattere hælder NATO åbenbart til den opfattelse, at cyberangreb ikke umiddelbart kan udgøre væbnede angreb.[46]

Som berørt i afsnit 4 er det imidlertid sandsynligt, at stater vil anlægge en *effektbaseret* tilgang til cyberangreb, og det kan derfor principielt heller ikke udelukkes, at særligt voldsomme cyberangreb vil kunne opfylde betingelserne for at udgøre 'væbnede angreb'. Som Yoram Dinstein bemærker:

> From a legal perspective there is no reason to differentiate between kinetic and electronic means of attack. A premeditated destructive CNA can qualify as an armed attack just as much as a kinetic attack bringing about the same – or similar results.[47]

Dinstein forsøger også at give en række eksempler på, hvornår konkrete cyberangreb efter hans opfattelse må forventes at udgøre væbnede angreb:

> Fatalities caused by loss of computer-controlled life-support systems, an extensive power-grid outage (electricity black-out) creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating thereby floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers), etc. The most

> egregious case is the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighbouring areas are densely populated.[48]

Et andet bud kom i 1999 fra det amerikanske forsvarsministerium:

> It might be hard to sell the notion that an unauthorized intrusion into an unclassified information system, without more, constitutes an armed attack. On the other hand, if a coordinated computer network attack shuts down a nation's air traffic control system *along with* its banking and financial system and public utilities, *and* opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack (mine kursiveringer).[49]

En nærlæsning af sidstnævnte citat viser, at det amerikanske forsvarsministerium i hvert fald på daværende tidspunkt anlagde en temmelig tilbageholdende tilgang, i den forstand at det formentlig kun var rent undtagelsesvist, at cyberangreb efter USA's opfattelse ville være tilstrækkelig alvorlige til at kunne kvalificere sig som 'væbnede angreb', der udløser en amerikansk ret til selvforsvar.

En tidligere højtstående juridisk rådgiver fra den amerikanske regering gav imidlertid i en tale i marts 2011 udtryk for, at USA sidenhen kan have ændret holdning og i dag anlægger en mindre restriktiv tilgang. Den juridiske rådgiver bemærkede i hvert fald, at cyberangreb, der (blot) 'inflict significant physical destruction *or* loss of life by causing the failure of critical infrastructure, like a dam or water supply system … would justify a full military response.'[50]

Sikkert er det i hvert fald, at der flere steder i den amerikanske litteratur opereres med en ganske lav tærskel for, hvornår cyberangreb udløser en ret til selvforsvar. Ifølge Horace B. Robertson, Jr., vil et cyberangreb eksempelvis kunne være et 'væbnet angreb', selvom der ikke sker tab af menneskeliv. Ifølge Robertson skal konsekvenserne af angrebet (blot) være 'major damage to or destruction of vital military or civilian infrastructure *or* the loss of life' (min kursivering).[51] En tilsvarende – lempelig – opfattelse spores hos Christopher C. Joyner og Catherine Lotrionte, der går så langt som til at mene, at tyveri eller destruktion af følsomme militære oplysninger bør være tilstrækkeligt til at klassificere handlingerne som et væbnet angreb.[52]

Også her er der imidlertid grund til at være varsom, og det er langtfra oplagt, at stater vil bakke op om sådanne ganske vidtrækkende fortolkninger af begrebet 'væbnet angreb'.

En af årsagerne til, at det i praksis kan være kompliceret at vurdere, hvornår cyberangreb kan udgøre 'væbnede angreb', er, at det ikke altid er tydeligt, hvor stor retlig betydning *målet* for angrebet skal tillægges.

Det er som en indledende betragtning oplagt, at visse mål anses som mere vitale og vigtige end andre mål, og at cyberangreb mod sådanne mål, såsom militære installationer og regeringsinfrastruktur, nemmere vil kunne udgøre væbnede angreb end angreb mod mindre betydningsfulde mål, men det kan ikke desto mindre ofte være behæftet med vanskeligheder at vurdere, præcis hvilke mål der skal tillægges størst betydning.

En løsning er at gøre som USA[53], Storbritannien[54], Australien[55] og EU[56] og forsøge at definere og klassificere de dele af staternes infrastruktur, der anses for at være særlig betydningsfulde – eller 'kritiske' – og hvis destruktion – eller midlertidige lammelse – derfor også nemmere vil kunne anses som et væbnet angreb på staten end angreb på andre mål.[57]

Endelig kompliceres spørgsmålet af, at dele af staters kritiske infrastruktur som regel er ejet og drevet af aktører på det private marked, såsom store multinationale selskaber, og ikke af staten. Det er ikke en betingelse, at et angreb mod en anden stat skal rette sig mod statslige mål, før det kan udgøre et 'væbnet angreb', og angreb på civile mål, såsom udenlandsk ejede virksomheder, vil derfor efter omstændighederne også kunne udløse en ret til selvforsvar.[58] Det forekommer ikke desto mindre også nærliggende at antage, at angreb på statslige mål i højere grad vil kunne udgøre væbnede angreb end angreb på civile mål.

Selvforsvar og andre typer af modforanstaltninger mod cyberangreb

Vi har indtil nu set, at cyberangreb efter omstændighederne vil kunne udgøre en ulovlig 'intervention' i andre staters indre anliggender, 'magtanvendelse', der er uforenelig med magtforbudsreglen i FN-pagtens artikel 2, stk. 4, eller – i særligt alvorlige tilfælde – sågar 'væbnede angreb' i henhold til pagtens artikel 51. Det rejser det spørgsmål, hvilke foranstaltninger den stat, der gøres til genstand for det pågældende cyberangreb, kan iværksætte for at beskytte sig selv og sin elektroniske infrastruktur.

Hvis et cyberangreb mod en stat opfylder betingelserne for at være et 'væbnet angreb' i henhold til artikel 51, vil staten som berørt i afsnit 5 være berettiget til at gøre brug af magt for at forsvare sig mod angrebet.[59]

FN-pagtens artikel 51 foreskriver, at retten til selvforsvar udløses, når et væbnet angreb 'occurs', og det er derfor også fast antaget, at det først er fra det tidspunkt, hvor et væbnet angreb *er* indledt, at en stat lovligt kan indlede sit selvforsvar.

Den umiddelbare konsekvens af dette helt klare udgangspunkt kan dog i ekstraordinære tilfælde forekomme mindre rimelig, da det kan være svært at kræve, at en stat altid skal forholde sig passiv, hvis en fjende er i de sidste stadier af iværksættelsen af et større væbnet angreb. Det antages derfor, at en stat i henhold til et princip om såkaldt *anticiperet selvforsvar* rent undtagelsesvis kan være berettiget til at gribe til våben og

selvforsvar mod en *overhængende trussel* om et forestående angreb, i tidsrummet umiddelbart *før* angrebet materialiserer sig.[60]

Det er under alle omstændigheder vigtigt at understrege, at det ikke står en stat fuldstændig frit for at bruge væbnet magt i selvforsvar, og at lovlige selvforsvarshandlinger skal være både nødvendige og proportionale med det angreb, der udløste retten til selvforsvar.[61]

Kravet om *nødvendighed* ligger i naturlig forlængelse af staternes generelle pligt til at afstå fra at anvende væbnet magt i deres internationale relationer og i stedet søge at løse deres fredstruende konflikter med fredelige midler eller alternativt indbringe dem til kollektiv behandling i FN's Sikkerhedsråd. Det er derfor også kun naturligt, at løsningsmodeller, der ikke indebærer brug af international væbnet magt, skal foretrækkes. Selvforsvar mod et cyberangreb forudsætter med andre ord, at der ikke er andre og mere fredelige måder, hvorpå angrebet kan standses.

Unødvendig magtanvendelse betegnes ofte som et *repressalie*, der ellers som udgangspunkt er en folkeretsstridig handling, som en stat kan være berettiget til at foretage som en konsekvens af en anden stats retsstridige handling for at få oprejsning og for at afskrække denne fra lignende retsstridige handlinger.[62] Det er den generelle antagelse, at *væbnede repressalier* er uforenelige med retten til selvforsvar.[63]

Kravet om *proportionalitet* betyder, at selvforsvarshandlinger skal stå i rimeligt forhold til det angreb, som selvforsvaret har til formål at imødegå, så det er altså kun de handlinger, der er nødvendige for at standse det væbnede angreb, der er forenelige med retten til selvforsvar.[64]

Kravet bevirker imidlertid ikke, at en forsvarende stat per definition er afskåret fra at gøre brug af mere magt for at standse et angreb end den magt, der blev anvendt i det væbnede angreb, der udløste retten til selvforsvar, da 'the action needed to halt and repulse the attack may … have to assume dimensions disproportionate to those of the attack suffered.'[65]

Der gælder heller ikke noget krav om, at selvforsvarshandlinger skal udøves på samme måde og med samme midler som angrebet, og der er derfor principielt heller ikke noget til hinder for, at en stat forsvarer sig mod et cyberangreb, der udgør et 'væbnet angreb', med traditionelle væbnede midler.[66]

Hvis et cyberangreb ikke er tilstrækkelig alvorligt til at udgøre et 'væbnet angreb', der udløser en ret til selvforsvar, er en stat ikke berettiget til at gøre brug af magtanvendelse som beskrevet i artikel 2, stk. 4, for at forsøge at bringe det pågældende angreb til standsning.

Det betyder imidlertid ikke, at staten af den grund er henvist til at se passivt til. Folkeretten anerkender nemlig, at en stat kan være berettiget til at iværksætte *modforanstaltninger* mod den stat, der udsætter staten for en folkeretsstridig handling. Det fremgår bl.a. af de folkeretlige principper for statsansvar[67], hvori det også bemærkes, at formålet med modforanstaltninger alene må være at få modparten til at indstille sine retsstridige handlinger, og at de iværksatte modforanstaltninger skal være proportionale.[68]

I praksis betyder dette, at en stat som udgangspunkt altid er berettiget til at besvare et cyberangreb med de nødvendige modforanstaltninger. Hvis angrebet er tilstrækkelig alvorligt til at udgøre et 'væbnet angreb', kan staten gribe til selvforsvar, og i mindre alvorlige tilfælde vil staten som regel være berettiget til at gengælde angrebet efter principperne om lovlige modforanstaltninger. Kun i de tilfælde, hvor et cyberangreb ikke er tilstrækkelig alvorligt til at udgøre et væbnet angreb, men dog alvorligt nok til at udgøre 'magt' i henhold til artikel 2, stk. 4, vil en stat ikke være berettiget til at svare igen med et angreb af samme styrke.[69] I disse situationer må staten derfor 'nøjes' med at iværksætte modforanstaltninger, der falder under tærsklen for magtanvendelse i artikel 2, stk. 4, og/eller eventuelt indbringe det igangværende cyberangreb for FN's Sikkerhedsråd med anmodning om, at rådet tager de fornødne skridt til at bringe angrebet til ophør.[70]

Det vil altid afhænge af en konkret vurdering, om en stats selvforsvarshandlinger eller øvrige modforanstaltninger opfylder betingelserne om nødvendighed og proportionalitet, men det er som en generel antagelse svært at være uenig med det amerikanske forsvarsministerium i, at en stat som udgangspunkt altid er berettiget til at standse 'any unauthorized intrusion into a nation's computer systems' og at sikre systemet mod nye forsøg på uautoriseret indtrængen.[71]

Analysen i denne rapport har indtil nu været baseret på den antagelse, at det er en stat, der står bag et cyberangreb, men det vil langtfra altid være tilfældet. Faktisk er cyberangreb netop kendetegnede ved at være en form for 'krigsførelse', som relativt nemt vil kunne udføres af *private aktører*, såsom 'patriotiske' hackergrupper. Som det bemærkes i en Chatham House-rapport om cyberwarfare:

> Unlike diplomacy, military force and economic warfare, it challenges the traditionalist view of the state as the principal actor in the international system and the decisive influence on warfare. Although nation-states have far greater access to the capabilities, resources and budgets needed to carry out substantial and well-directed cyber attacks and are the most likely to employ cyber ways and means to achieve their ends, cyberspace has made it possible for non-state actors, commercial organizations and even individuals to acquire the means and motivation for warlike activity.[72]

Dette rejser flere spørgsmål af potentielt stor betydning for staters mulighed for at imødegå cyberangreb.

Det følger af principperne for statsansvar, at en stat er ansvarlig for de handlinger, der udøves af statsansatte personer[73] og af andre personer, der handler på statens vegne.[74] En stat er med andre ord ikke kun ansvarlig for de cyberangreb, som den selv foretager, men også for de angreb, som andre udfører på statens vegne.

Det interessante spørgsmål er derfor, hvor tæt forbindelsen mellem en stat og private personer skal være, før sidstnævnte kan siges at handle 'på statens vegne'.

I henhold til principperne for statsansvar kan private personers handlinger henregnes til en stat, når de private personer handler efter *ordre* fra staten ("*instructions of*"), eller når staten kan *styre* ("*the direction of*") eller *kontrollere* ("*control of*") personerne.[75] Den Internationale Domstol konkluderede i *Nicaragua*, at der med begrebet 'kontrollere' henvises til, at en stat skal være i stand til at udøve *effektiv kontrol over de private personer under de operationer, hvor handlingerne blev begået*.[76]

Domstolens restriktive vendinger og begrebet 'effektiv kontrol' er i de seneste årtier blev kritiseret for at gøre det for nemt for stater at undgå at ifalde et folkeretligt ansvar for de handlinger, som de i en eller anden forstand bifalder, og kritikerne fik en smule medhold af appelretten for Krigsforbrydertribunalet for det tidligere Jugoslavien, der i en afgørelse fra 1999 – *Tadic* – konkluderede, at kravene om kontrol ikke altid er så høje, som Den Internationale Domstol lagde op til i *Nicaragua*.[77]

I en række nyere afgørelser har Den Internationale Domstol imidlertid afvist, at de restriktive krav i *Nicaragua* skulle have ændret sig[78], og i *Genocide* cementerede domstolen, at en stat (fortsat) kun er ansvarlig for private personers handlinger, når den er i stand til at udøve effektiv kontrol over personerne 'in respect of each operation in which the alleged violations occurred'.[79]

Konklusionen må derfor også (fortsat) være, at en stat kun er ansvarlig for private personers cyberangreb, når staten har været i stand til at udøve 'effektiv kontrol' over personerne under de operationer, hvor cyberangrebene finder sted.

De skrappe krav til statsansvar skaber særlige problemer for de stater, der udsættes for cyberangreb, som de mistænker andre stater for at stå bag, for det kan nemlig være endog meget vanskeligt at afgøre, om det er en stat eller en gruppe private personer, der står bag et cyberangreb. Som det bemærkes i rapporten fra Chatham House:

> One of the main attractions of cyberspace is the shield of anonymity it offers, at least in the short term. Operating behind false IP addresses, foreign servers and aliases, attackers can act with almost complete anonymity and relative impunity. In the case of suspected state-sponsored actions it is difficult to

> establish beyond any doubt that the order to attack originated in the executive or presidential office, let alone a capital city. Furthermore, the difficulty of attribution allows a degree of plausible deniability.[80]

Fremkomsten af cyber har derfor fået nogle forfattere af juridisk litteratur til at argumentere for, at der er behov for at gentænke de retlige rammer for staters muligheder for at imødegå cyberangreb og åbne mulighed for, at stater i langt højere grad kan indlede selvforsvarshandlinger mod cyberangreb, der udgår fra ukendte aktører. En af disse forfattere er Matthew Hoisington:

> To address the unique nature of cyberwarfare, international law should afford protection for states who initiate a good-faith response to an attack, thus acting in cyber self-defense, without first attributing and characterizing the attack.[81]

Indtil videre må det imidlertid konkluderes, at et sådant udsagn savner et solidt grundlag i folkeretten, og det er svært at være uenig med Yoram Dinsteins udlægning af gældende folkeret, når han bemærker, at en stat ikke må:

> … rush headlong to hasty action predicated on reflexive impulses and unfounded suspicions; it has no choice but to withhold forcible response until hard evidence is collated and the state of affairs is clarified, lest the innocent be endangered.[82]

En stat må med andre ord ikke indlede selvforsvarshandlinger mod en anden stat, hvis ikke staten er sikker på, at det er en fremmed stat, der står bag et konkret angreb. Det er i den forbindelse værd at huske på, at FN-pagten jo netop har til formål at lægge hindringer i vejen for staters potentielle overdrevne brug af international væbnet magt. Som Jason Barkham formulerer det:

> A rule permitting wide-ranging responses would allow targeted states too much latitude in determining the extent of the appropriate response and would eviscerate Article 51's purpose of limiting the times where self-defense actions would be appropriate.[83]

Det hører også med til historien, at det jo ikke kun er i forbindelse med cyberangreb, at det kan være forbundet med problemer for en stat at vurdere, hvem der står bag et angreb. Samme problem findes på området for bekæmpelse af terrorisme, hvor det ikke er noget særsyn, at der er tvivl om, hvem der stod bag konkrete terrorangreb, og om en eller flere stater eventuelt har været involveret.

Det skal også bemærkes, at en konkret usikkerhed om, hvem der står bag et cyberangreb, jo ikke nødvendigvis varer ved. Dels er det muligt, at cyberangreb udføres som et led i en mere konventionel militær konfrontation – eventuelt som det første led heri (se herom nedenfor) – hvor det derfor ganske hurtigt fremstår klart, hvem der har iværksat angrebet, og dels kan fremtidige teknologiske fremskridt gøre det nemmere at identificere bagmændene bag konkrete cyberangreb.[84]

På nuværende tidspunkt er det under alle omstændigheder ikke muligt at nå nogen anden konklusion, end at stater kun er ansvarlige for de cyberangreb, som de selv udfører, eller som udføres af personer, som staten er i stand til at udøve effektiv kontrol over under de operationer, hvor cyberangrebene udføres.

Det rejser naturligvis spørgsmålet om, hvorvidt det gør en forskel for en stats ret til at iværksætte modforanstaltninger, herunder selvforsvarshandlinger, at et cyberangreb udføres af en privat aktør, såsom en hackergruppe, og ikke af en stat.

Det folkeretlige udgangspunkt er ganske klart: Angreb fra private aktører udløser ikke en ret til selvforsvar eller andre former for modforanstaltninger på en anden stats territorium.

Det er imidlertid et omdiskuteret spørgsmål, om der ikke i ganske særlige tilfælde kan gøres undtagelser fra dette udgangspunkt. Den internationale reaktion på terrorangrebene i USA den 11. september 2001 viste, at det formentlig vil være tilfældet.[85]

I *Corfu Channel* konkluderede Den Internationale Domstol i 1949, at en stat ikke 'knowingly' må lade sit territorium blive brugt til handlinger, der krænker andre staters rettigheder.[86] Det følger heraf, at en stat skal tage de nødvendige forholdsregler for at sikre, at private aktører ikke bruger dens territorium til at angribe mål i andre stater.

Hvis en stat ikke lever op til sin folkeretlige forpligtelse til at forhindre, at private aktører på dens territorium angriber mål i andre stater, vil den stat, der er mål for den private aktørs angreb, efter omstændighederne kunne være berettiget til at iværksætte modforanstaltninger, herunder eventuelt egentlige selvforsvarshandlinger, for at bringe angrebene til ophør. Der vil derfor også efter omstændighederne være grundlag for, at en stat, der er udsat for cyberangreb fra en privat aktør, kan være berettiget til at iværksætte modforanstaltninger mod den private aktør.

To forbehold skal dog knyttes hertil.

Det første er, at retten til at iværksætte modforanstaltninger mod en privat aktør er subsidiær i forhold til værtsstatens ret til at standse de angreb, der udgår fra den private aktør. Det betyder i praksis, at modforanstaltningerne først kan iværksættes, fra det tidspunkt hvor værtsstaten har vist sig at mangle enten den fornødne vilje eller evne til at standse angrebene fra den private aktør. Den stat, der udsættes for cyberangreb fra en privat aktør, må altså indledningsvis forsøge at få værtsstaten til at gribe ind over for den

private aktør, og først hvis dette viser sig ikke at være muligt, vil staten kunne iværksætte sine egne modforanstaltninger.

Det andet forbehold er, at der skal sondres mellem modforanstaltninger mod *den private aktør*, der står bag cyberangrebet, og foranstaltninger mod *myndighederne* i den stat, hvori den private aktør opholder sig (værtsstaten).[87] Hvis et cyberangreb fra en privat aktør ikke kan henregnes til en stat, vil modforanstaltningerne nemlig alene kunne rettes mod den private aktør og ikke mod værtsstatens myndigheder, herunder myndighedernes elektroniske infrastruktur.

En måde at anskue problemstillingen på er at anlægge den betragtning, at den stat, der iværksætter modforanstaltninger, såsom selvforsvar, mod en privat aktør, der står bag et cyberangreb, i princippet blot opfylder den forpligtelse, som de lokale myndigheder i den stat, hvori den private aktør befinder sig, er underlagt, til at sikre, at statens territorium ikke benyttes til at angribe andre stater.[88]

Praksis for cyberangreb

Indledning

Med henblik på at illustrere, hvorledes den folkeretlige regulering af international magtanvendelse kan finde anvendelse på cyberangreb, redegøres der i det følgende for en række af de cyberangreb, der har ramt stater i løbet af de seneste par år. Der sondres i den forbindelse mellem de tre måder, hvorpå cyberangreb kan iværksættes. Det drejer sig som tidligere berørt om angreb, der iværksættes 1) *uden forbindelse* til et konventionelt angreb, 2) som led i *forberedelserne* til et konventionelt angreb eller 3) som led i et *igangværende* konventionelt angreb.

Cyberangreb uden forbindelse til konventionelle angreb – Estland, Litauen og Iran

Den første type cyberangreb iværksættes uden nogen forbindelse til konventionel magtanvendelse. Det formentlig kendteste angreb af denne type ramte Estland i løbet af en treugers periode i april og maj 2007 i form af såkaldte 'Distributed Denial Of Service-angreb (DDOS-angreb)', der bl.a. rettede sig mod officielle hjemmesider for ministerier, nyhedsmedier, telefonselskaber og banker.[89] Angrebet var efter alt at dømme motiveret af en estisk beslutning om at flytte et russisk krigsmonument fra centrum af hovedstaden Tallinn til en militær kirkegård uden for byen – en beslutning, der blev mødt med massive protester fra såvel det russiske mindretal i Estland som den russiske regering i Moskva. Estland har efterfølgende beskyldt Rusland og/eller patriotiske russiske hackergrupper for at stå bag angrebet, men Rusland har aldrig taget ansvaret.

Lidt over et år efter cyberangrebet på Estland blev et andet baltisk land også udsat for et cyberangreb, om end i mindre målestok. I juni 2008 blev ca. 300 offentlige og private litauiske hjemmesider hacket, og indholdet af hjemmesiderne blev erstattet med bl.a. prosovjetiske og kommunistiske symboler eller antilitauiske slogans.[90] Angrebet indledtes, få dage efter at det litauiske parlament havde vedtaget en lov, der forbød offentlig fremvisning af symboler fra bl.a. Sovjettiden, såsom hammer og sejl. Den nye litauiske lov blev kritiseret af især Rusland, og der blev gennemført en mindre demonstration foran den litauiske ambassade i Rusland. Selvom repræsentanter for den litauiske regering efterfølgende har udtalt, at der efter deres opfattelse var en forbindelse mellem vedtagelsen af den nye lovgivning og cyberangrebet, og at angrebet udgik fra et område 'øst for Litauen', har Litauen aldrig officielt beskyldt Rusland for at stå bag angrebet. Ifølge flere kilder kan angrebet meget vel have været udført af patriotiske russiske hackergrupper.[91]

Hvis det *var* det officielle Rusland, der stod bag angrebene, og hvis disse havde til formål at presse henholdsvis de estiske og de litauiske myndigheder til at ændre deres beslutninger om at flytte det pågældende krigsmonument og vedtage den konkrete lovgivning, var de uforenelige med Ruslands forpligtelser i henhold til det folkeretlige forbud mod intervention.

Angrebene var imidlertid næppe tilstrækkelig intense til at krænke magtforbuddet i FN-pagtens artikel 2, stk. 4. Angrebet på Estland var det mest omfattende af angrebene, og selvom det ganske vist lagde diverse regeringshjemmesider ned, ligesom estiske nyhedsmedier, telefonselskaber og banker blev berørt af angrebene, var der ingen, der mistede livet, og angrebene førte heller ikke efter det oplyste til reel skade på ejendom.

Det forekommer under alle omstændigheder sikkert, at ingen af angrebene var tilstrækkeligt alvorlige til at udgøre et væbnet angreb, der kunne have udløst henholdsvis en estisk og en litauisk ret til selvforsvar. Dertil var effekterne af angrebene for begrænsede. Det hører da også med til historien, at ikke engang Estland selv på noget tidspunkt under det tre uger lange angreb overvejede at påberåbe sig NATO's 'musketered' i Washington, dvs. traktatens artikel 5, hvorefter et 'væbnet angreb' på et enkelt medlem af NATO skal anses som et angreb på alliancen som helhed.[92]

Som berørt har Rusland aldrig officielt taget ansvaret for angrebene på Estland og Litauen, og angrebene illustrerer, hvor vanskeligt det kan være at få klarlagt, om det er en stat eller private hackergrupper, der står bag et cyberangreb[93], herunder om hackergrupper handler på vegne af en stat. Hvis angrebene på Estland og Litauen blev udført af private hackergrupper, som de russiske myndigheder ikke var i stand til at udøve effektiv kontrol over, på de tidspunkter hvor angrebene blev udført, følger det af de folkeretlige principper for staters ansvar, at Rusland ikke var internationalt ansvarlig for angrebene.

Det følger imidlertid også, at Rusland, som andre stater, er underlagt en generel forpligtelse til at sikre, at dets territorium ikke anvendes af personer, der angriber mål i andre stater, og hvis Rusland ikke lever op til denne forpligtelse, vil det efter omstændighederne være nødsaget til at acceptere, at den stat, der er mål for de private personers angreb, selv forsøger at bringe angrebene til ophør ved at gøre brug af passende modforanstaltninger mod den private aktør.

Estland og Litauen er ikke de eneste stater, der efter alt at dømme er blevet gjort til genstand for cyberangreb, der er blevet iværksat uden nogen forbindelse til et konventionelt angreb. Ifølge flere kilder inficerede en computervirus ved navn 'Stuxnet' i sommeren 2010 et stort antal computere rundt omkring i verden, herunder Siemens' centrifuger på det iranske atomanlæg ved Natanz. Ifølge kilderne fik virussen centrifugerne til at selvdestruere, hvorved der skete alvorlig skade på et påstået iransk atomvåbenprogram.[94]

Hvis cyberangrebet mod anlægget i Natanz blev iværksat af en fremmed stat, er det svært ikke at drage den konklusion, at denne stat overtrådte interventionsforbuddet, og det er også nærliggende at antage, at angrebet

meget vel kan have krænket magtforbuddet i FN-pagtens artikel 2, stk. 4. Effekterne af angrebet er i hvert fald umiddelbart at sammenligne med den skade, der forårsages af kinetiske våben.

Det mest interessante spørgsmål synes derfor også at være, om det pågældende cyberangreb på Iran kan have været tilstrækkelig alvorligt til, at det kunne kvalificeres som et egentligt væbnet angreb, der i teorien kunne udløse en iransk ret til selvforsvar.

Det taler imod dette, at angrebet efter det oplyste kun forårsagede materiel skade. Omvendt er det svært at forestille sig mål i Iran, der er af lige så stor betydning for det iranske styre som dets eventuelle atomvåbenprogram, og det taler selvsagt for, at angrebet bør sidestilles med et væbnet angreb.

Cyberangreb som forberedelse til konventionelle angreb – Syrien og Libyen

Der findes tilsyneladende i hvert fald to eksempler på, at stater enten *har* anvendt eller har *overvejet* at anvende cyberangreb med henblik på at bane vejen for konventionelle angreb. Det første eksempel stammer fra september 2007, hvor det israelske luftvåben efter alt at dømme gennemførte et konventionelt luftangreb på et bygningskompleks i Syrien, der ifølge amerikanske og israelske kilder var mistænkt for at rumme et hemmeligt syrisk atomprogram.[95] Luftangrebet blev ifølge flere kilder muliggjort af, at et israelsk cyberangreb havde sat radarer og andre sensorer i det syriske luftforsvar midlertidigt ud af kraft, hvorved det var muligt for de israelske kampfly at trænge ind i og flyve ud af syrisk luftrum uden at blive opdaget. Det andet eksempel er de påståede amerikanske overvejelser om at indlede luftoperationen mod Libyen i marts 2011 med et omfattende cyberangreb, der ville have haft til formål at lamme det libyske luftforsvarssystem.[96]

Konventionelle luftangreb som det påståede israelske luftangreb på Syrien og det amerikanske på Libyen er *i sig selv* tilstrækkeligt intense til at blive kvalificeret som egentlige væbnede angreb, der udløser en ret til selvforsvar.[97] Det interessante spørgsmål på dette sted er imidlertid, hvordan folkeretten forholder sig til et *forberedende* cyberangreb mod en stats radarsystem og luftforsvar.

Det vil afhænge af en konkret vurdering, om den midlertidige lammelse af en stats radarsystemer og luftforsvarssystemer er tilstrækkelig alvorlig til at udgøre henholdsvis magtanvendelse og et væbnet angreb i FN-pagtens forstand, men det forekommer imidlertid som en generel betragtning oplagt, at en stat, der oplever, at dens luftforsvarssystem sættes ud af kraft, som udgangspunkt vil være i sin gode ret til at antage, at der er en overhængende (’imminent’) fare for, at et konventionelt angreb er umiddelbart forestående, og at staten derfor også i udgangspunktet vil være berettiget til at gribe til selvforsvarshandlinger mod den aktør, der har angrebet dens luftforsvarssystem. Det betyder i praksis, at det næppe spiller nogen rolle, om et

forberedende cyberangreb mod en stats luftforsvarssystem *i sig selv* er tilstrækkelig alvorligt til at udgøre et væbnet angreb, da cyberangrebet under alle omstændigheder må forventes at blive fulgt op af et konventionelt angreb, der vil være tilstrækkelig alvorligt, og som under alle omstændigheder udløser en ret til selvforsvar.

Cyberangreb under konventionelle angreb – Georgien

Den tredje og sidste form for cyberangreb er de angreb, der iværksættes under igangværende konventionelle angreb. Et eksempel herpå var det cyberangreb, der ramte Georgien under den kortvarige væbnede konflikt mellem Rusland og Georgien i august 2008.[98]

Konflikten mellem Rusland og Georgien indledtes natten til den 8. august 2008, da georgiske styrker indledte en større militær operation i den demilitariserede zone i Sydossetien. Rusland reagerede på den georgiske operation ved at indlede en modoffensiv ikke bare mod de fremrykkende georgiske tropper i Sydossetien, men også mod mål i selve Georgien. Den 8. august 2008 blev et stort antal officielle og private georgiske hjemmesider endvidere ramt af cyberangreb, der satte siderne ud af kraft, og den 11. august 2008 udsendte det georgiske udenrigsministerium en pressemeddelelse, hvori man erklærede, at Georgien var udsat for et storstilet russisk cyberangreb.[99] Der er ifølge flere kilder ikke nogen tvivl om, at angrebene udgik fra Rusland, men som i forbindelse med angrebene på Estland i 2007 og Litauen i 2008 er det ikke bevist, at det var det officielle Rusland og ikke private patriotiske hackergrupper, der stod bag angrebet på Georgien. Den russiske regering har da også benægtet, at den stod bag.[100]

Vurderingen af, om cyberangrebet på Georgien var foreneligt med *jus ad bellum*, er i praksis uden betydning, fordi Georgien og Rusland allerede på tidspunktet for angrebet var begyndt at anvende international væbnet magt mod hinanden.

Isoleret betragtet mindede cyberangrebet mod Georgien om de tilsvarende angreb på Estland og Litauen, og angrebet på Georgien udgjorde næppe *i sig selv* magtanvendelse i FN-pagtens forstand. Det var under alle omstændigheder ikke tilstrækkelig alvorligt til at udgøre et væbnet angreb, der kunne udløse en georgisk ret til selvforsvar.

Udfordringer og anbefalinger

Gennemgangen i forrige afsnit viste, at det kan være vanskeligt at udtale sig med sikkerhed om, hvordan de folkeretlige regler og principper for international magtanvendelse regulerer konkrete cyberangreb. I dette afsnit skal vi se lidt nærmere på de udfordringer – men også muligheder – der er forbundet hermed.

For det første er det oplagt, at den aktuelle retlige uklarhed betyder, at Danmark, herunder det danske forsvar, må indstille sig på, at cyberområdet er omgærdet af stor retlig usikkerhed.

For det andet er det lige så oplagt, at Danmark bør forholde sig til den aktuelle retlige uklarhed. For er den at foretrække, eller ville det tjene Danmarks interesser bedre, hvis der kunne opnås en højere grad af folkeretlig klarhed?

Som et lille, åbent samfund, der ikke bare er afhængigt af moderne teknologi, og i særdeleshed informationsteknologi, men også er sårbart over for andre staters offensive anvendelse af sådanne teknologier, forekommer det oplagt, at det er i Danmarks interesse, at der skabes klarhed om de retlige normer i cyberspace.

Det anbefales derfor også i denne rapport, at Danmark tager de fornødne initiativer til at skabe en højere grad af retlig klarhed i cyberspace.

Det ville i den forbindelse være nærliggende at anlægge den betragtning, at Danmark skulle arbejde for, at det internationale samfund fik skabt et bindende folkeretligt regelsæt, der er specifikt målrettet reguleringen af cyberangreb, og det skorter da heller ikke på forfattere af folkeretlig litteratur, der argumenterer for behovet for nye, egentlige regler på området.[101] Mulige perspektiver for en egentlig cyberkonvention blev endvidere diskuteret under World Economic Forum i Davos, Schweiz, i 2010.[102]

Det *ville* da også på mange måder være at foretrække med en egentlig 'cyberkonvention', der regulerede cyberangreb. Dels skaber konventioner (som regel) tiltrængt retlig klarhed over staternes forpligtelser på et givent område, og dels indeholder de ofte også konkrete mekanismer, der kan sikre håndhævelsen af de retlige forpligtelser, som konventionen pålægger de kontraherende stater.

Der er ikke desto mindre i hvert fald tre grunde til, at det hverken er sandsynligt eller nødvendigvis særlig hensigtsmæssigt, at man fra det internationale samfunds side, herunder fra dansk side, på nuværende tidspunkt tager initiativ til at få vedtaget en bindende konvention til brug for reguleringen af cyberangreb.

For det første er vi – som berørt tidligere – formentlig fortsat i de tidlige stadier af udviklingen af cyberspace, og det er derfor også indtil videre temmelig usikkert, hvordan staterne forholder sig retligt til en række meget centrale spørgsmål, såsom spørgsmålene om, hvornår cyberangreb bør anses for at udgøre krænkelser af forbuddet mod 'intervention' eller 'magtanvendelse', og hvornår cyberangreb bør sidestilles med 'væbnede angreb', der udløser en ret til selvforsvar. Der har været for få konkrete sager, hvor staterne har skullet tage retlig stilling til cyberangreb, og vi mangler derfor også fortsat konkret viden om, hvordan staterne mener, at cyberspace bør forenes med den eksisterende folkeret. Og indtil vi ved mere herom, giver det ikke mening at forsøge at udarbejde bindende retningslinjer for, hvordan stater må opføre sig i cyberspace.

For det andet ved vi endnu heller ikke så meget om, hvad cyber egentlig kan udrette. Vi ved, hvad mere traditionelle våbentyper kan gøre af skade, men vi ved endnu ikke særlig meget om de effekter, der er forbundet med brugen af cyber som våbentype. Og fordi vi ikke ved det, så er det hverken realistisk eller formålstjenligt at bede stater lægge sig endegyldigt fast på, hvordan de må anvende cyber, og hvordan de ikke må.

Endelig er der for det tredje det forhold, at der formentlig er ganske stor forskel på, hvilke retlige normer stater egentlig ønsker i cyberspace. Stater ser forskelligt på fordelene og ulemperne ved cyberspace,[103] og derfor har stater også forskellige opfattelser af, i hvor høj grad de eksisterende retlige begreber figurer, såsom magtbegrebet og begrebet 'væbnet angreb', bør finde anvendelse på cyberangreb.

Stater med stærke offensive cyberkapaciteter og en lav grad af national sårbarhed over for cyberangreb vil foretrække én form for folkeretlig regulering, mens stater med en svag offensiv kapacitet og en høj grad af national sårbarhed vil ønske en anden. Som Matthew Waxman bemærker om USA's aktuelle ønsker om at regulere cyber:

> With these relationships between law and power in mind, the United States has an interest in regulating cyber-attacks, but it will be difficult to achieve such regulation through international use-of-force law or through new international agreements to outlaw types of cyber-attacks. That is because the distribution of emerging cyber-capabilities and vulnerabilities … is unlikely to correspond to the status quo distribution of power built on traditional measures like military and economic might.[104]

Herudover må det forventes, at også mere ideologisk betingede forskelle staterne imellem vil gøre det vanskeligt at finde fælles folkeretligt fodslag. For mens vestlige stater som USA og staterne i EU, herunder Danmark, bl.a. ser cyberspace som et forum for udbredelsen af 'vestlige' værdier, såsom informationsfrihed og ytringsfrihed, er stater som Rusland og især Kina og stater i Mellemøsten opsat på at forhindre, at internettet udvikler sig til et sted, hvor regeringskritik og andre 'undergravende' aktiviteter kan florere.

Det forhold, at der for tiden næppe vil kunne opnås international enighed om bindende folkeretlige regler, er imidlertid ikke ensbetydende med, at Danmark bør læne sig tilbage og passivt afvente udviklingen i cyberspace og virkningerne af og reaktioner på kommende cyberangreb.

Det er nemlig ikke kun ved hjælp af bindende retlige regler, at vi kan opnå en højere grad af klarhed over spillereglerne i cyberspace. Indtil vi har en egentlig cyberkonvention, må mindre gøre det, og det anbefales derfor i dette papir, at vi fra dansk side begynder at overveje, hvilke ikke-retligt bindende *normer for adfærd* vi fra det internationale samfunds, og hermed også fra dansk, side ønsker i cyberspace. For selvom stater som berørt har forskellige interesser i cyberspace, er det ikke umuligt, at staterne trods alt ville kunne nå til enighed om relativt basale ikke-retlige forventninger til, hvordan stater og private aktører bør opføre sig i cyberspace. Opbygningen af normer for adfærd er som regel også det første skridt på vejen mod en eventuel udvikling af egentlige bindende retlige forpligtelser på et givent område.[105]

Der er flere grunde til, at ikke-retligt bindende normer undertiden kan være at foretrække frem for bindende retlige normer. Det er for det første nemmere at få stater til at bakke op om normer på et nyt område, hvis de netop ikke er retligt bindende, for når brud på normer ikke følges op af egentlige sanktioner, er den pris, som stater skal betale for ikke at efterleve normerne, ofte til at leve med.

For det andet er ikke-retligt bindende normer ofte ikke særlig præcise, og det betyder, at de som regel vil have nemmere ved at ændre sig i takt med den almindelige udvikling end retlige normer, der er nedfældet i en konvention. Det er især af stor betydning inden for cyberområdet, der er under hastig udvikling.

Herudover skal det også med, at selv ikke-retlige normer under alle omstændigheder er bedre end den aktuelle høje grad af uklarhed om spillereglerne i cyberspace. Som chefen for den amerikanske Cyber Command har udtalt:

> When all countries can come up and say: 'This is going to be the way we're going to operate and the way we're going to defend and the way we're going to do this', and we all agree to it, that will go a long way.[106]

Et blik på andre staters tilgang til den aktuelle retlige usikkerhed, der omgærder cyberspace, afslører da også, at normopbygning synes at være 'the name of the game'. USA lader i hvert fald til at være helt på det rene med, at det bliver svært at opnå enighed om bindende regler i cyberspace, og at det derfor – indtil videre – først og fremmest handler om at påvirke staters adfærd i cyberspace. I den amerikanske cyberspacestrategi fra maj 2011 bemærkes det eksempelvis bl.a.:

> The United States will work with like-minded states to establish an environment of expectations, or *norms of behaviour*, that ground foreign and defense policies and guide international partnerships. The last two decades have seen … increasing evidence that governments are seeking to exercise traditional national power through cyberspace. These events have not been matched by clearly agreed-upon norms for acceptable state behaviour in cyberspace. To bridge that gap, we will work to build a consensus on what constitutes *acceptable behaviour*, and a partnership among those who view the functioning of these systems as essential to the national and collective interest (mine kursiveringer).[107]

NATO's Cyber Center of Excellence (CCDCOE) offentliggjorde da også i maj 2011 '10 Rules of Behaviour for Cyber Security'[108], og i FN-regi er de internationale bestræbelser på at opnå enighed om basale normer for adfærd i cyberspace også så småt begyndt. På Ruslands initiativ blev 15 af de mest betydningsfulde cyberstater, såsom Rusland, USA, Kina og Frankrig, i 2010 enige om at bede FN om at arbejde på at udvikle netop normer for adfærd i cyberspace.[109]

Danmark bør begynde at gøre sig overvejelser om, hvilken adfærd vi ønsker at stater anlægger i cyberspace.

Det er som en helt generel betragtning i den forbindelse vigtigt, at vi fra dansk side forstår – og accepterer – at udviklingen af normer for adfærd og eventuelt også egentlige retlige normer i høj grad handler om strategi og dermed om fremme af nationale interesser. Opgaven består med andre ord ikke kun i at lade jurister kigge ud i en tåge af retlig uklarhed med besked på at identificere det mest 'korrekte' retlige svar på en given problemstilling, men i lige så høj grad i at bistå juristerne med at finde de retlige løsninger, der stemmer bedst overens med Danmarks strategiske interesser.

Det er værd at huske på, at normer for adfærd og egentlige retlige normer jo ikke opstår ud af den blå luft, men derimod udgår fra politiske valg og politiske prioriteringer. Jura hænger uløseligt sammen med politik, og det kan derfor ikke undre, at staterne i det internationale samfund altid har anvendt folkeretten og folkeretlige fortolkninger af centrale principper og begreber, såsom magtbegrebet, til at fremme deres respektive politiske og strategiske dagsordener. Svage stater har forsøgt at opnå fælles fodslag om vidtrækkende fortolkninger af magtforbudsreglen, mens stærke stater har forsøgt det modsatte. Eller som Matthew Waxman formulerer det:

> Competing interpretations of Article 2(4) and 51 have always reflected distributions of power. As a corollary, efforts to revise legal boundaries and thresholds may have re-allocative effects on power by raising and lowering the costs of using resources and capabilities that are unequally apportioned.[110]

Det er ikke anderledes, for så vidt angår cyberspace, og det er selvfølgelig også i det lys, at vi skal se de aktuelle amerikanske bestræbelser på dels at udvikle 'restriktive' normer for adfærd og dels at fortolke magtforbuddet bredt. USA er opmærksom på, at brugen af cyber kan være en måde, hvorpå mindre

magtfulde stater kan forsøge at kompensere for deres konventionelle militære og økonomiske underlegenhed i forhold til USA. Som Waxman bemærker om de amerikanske forsøg på at påvirke folkeretten:

> … U.S. legal interpretations and declaratory postures that define prohibited force in ways that narrow Charter interpretations to take account of cyber-warfare may be seen as part of an effort to sustain a legal order in which anticipated U.S. military and economic moves and countermoves against potential adversaries fit quite comfortably – that is, a legal order that preserves U.S. comparative advantages. In extending the foundational U.N. Charter prohibition on the use of force to cyber-attacks by emphasizing their comparable effects to conventional military attacks, such interpretations help deny that arsenal to others by raising the costs of its use.[111]

Det fremstår hermed også klart, at den aktuelle uklarhed om den folkeretlige regulering af cyber ikke kun repræsenterer en udfordring – eller et problem, om man vil – for Danmark og det danske forsvar, men i høj grad også en *mulighed* for, at vi fra dansk side kan forsøge at fremme vores strategiske interesser ved at forsøge at skabe de normer for adfærd og skabe lydhørhed for den fortolkning af den gældende folkeret, der er mest i overensstemmelse med Danmarks interesser. For når juraen er uklar – som den er på cyberområdet – så handler det i høj grad om strategi.

Det er værd at huske på, at Danmark i de seneste år faktisk *har* gjort sig erfaringer på området for normudvikling. Udenrigsministeriet påbegyndte i 2007 den såkaldte 'Copenhagen Process', der har til formål at identificere 'best practices' på området for fangehåndtering under internationale operationer.[112] Ligesom på cyberområdet er også den folkeretlige regulering af håndtering af fanger under moderne væbnede konflikter nemlig uklar, og Copenhagen Process er et forsøg fra dansk side på at få opbygget nogle basale normer for, hvordan stater bør/skal forholde sig til behandlingen af tilbageholdte personer.

De danske bestræbelser på at afklare, hvilke normer for adfærd Danmark gerne ser i cyberspace, bør derfor naturligvis tage afsæt i en mere grundlæggende analyse af, hvad vores strategiske interesser er, og hvordan cyberspace bedst kan forenes hermed. Så for at kunne svare på, hvilke normer for adfærd vi gerne vil have i cyberspace, må vi starte med at spørge os selv, hvad vi egentlig skal bruge cyberspace til. Hvad er Danmarks interesser i cyberspace? Det er i den forbindelse værd at bemærke, at Danmark, i modsætning til stater som USA[113], Storbritannien[114], Australien[115], Frankrig[116], Tyskland[117] og Holland[118], endnu ikke har udarbejdet en cyberstrategi.

Det forekommer oplagt, at Danmark tænker reguleringen af cyber ind i en større strategisk ramme, og en mulighed er at betragte cyberspace som en 'global common' på linje med det ydre rum og det åbne hav[119], hvor vi fra dansk side arbejder for, at reguleringen af cyberspace i store træk bør følge principperne for reguleringen af de andre 'commons of mankind'.[120] Og det ville i så fald i udgangspunktet betyde, at reguleringen skulle udformes i overensstemmelse med fem grundlæggende principper.

For det første følger det af præmissen om, at cyberspace er en 'common', at der ikke kan etableres et egentligt ejerskab over cyberspace. Den fysiske infrastruktur vil være ejet og drevet af stater og private virksomheder, men ingen af disse vil 'eje' den elektroniske trafik, der flyder gennem cyberspace.

En 'global commons'-parallel vil for det andet betyde, at det ikke blot vil være op til et par stater at udforme spillereglerne i cyberspace, men at normfastlægningen bør overlades til et eller andet internationalt organ.

Det vil for det tredje også betyde, at det ej heller vil være få heldige stater – men derimod hele det internationale samfund – der vil kunne høste frugterne af fordelene ved cyberspace.

For det fjerde vil det betyde, at cyberspace bevares og beskyttes til brug for fremtidige generationer.[121]

Og for det femte og sidste vil det betyde, at cyberspace kun må bruges til fredelige og ikke-militære formål.

Det sidste princip gør, at det ikke er realistisk med en traditionel global commons-tilgang til reguleringen af cyber. Stater har valgt at anvende cyberspace til militære formål, og en egentlig afmilitarisering er derfor næppe mulig. Cyberspace er – og bliver – med andre ord ikke som Arktis.

De facto-militariseringen af cyberspace betyder, at den aktuelle udfordring ved reguleringen af cyberspace består i at finde en balance mellem bevarelsen af cyberspace som en (fredelig) global common og de legitime militære hensyn, der følger af enhver form for militarisering af ny teknologi.

Hvordan denne balance skal se ud, er et strategisk og politisk spørgsmål, men det forekommer under alle omstændigheder oplagt, at staterne bør udnytte, at dele af cyberspace er koblet op på staters jurisdiktion, og at det derfor også i vidt omfang er muligt for staterne selv at forhindre i hvert fald mange cyberangreb.[122]

Det er endvidere på dette sted også værd at henlede opmærksomheden på det banale forhold, at vi fra dansk side skal være opmærksomme på, at rammerne for tilladelig opførsel jo går begge veje. Så hvis vi fra dansk side vil arbejde for, at en given adfærd i cyberspace skal være tilladelig, skal vi også være opmærksomme på, at vi i så fald risikerer, at det er en adfærd, som vores potentielle fjender lovligt vil kunne bruge mod os.

Afslutningsvis skal det med, at de relevante myndigheder i Danmark skal sørge for at have planer for, hvordan vi fra dansk side reagerer over for eventuelle cyberangreb, som vi måtte blive udsat for. Hvad gør Danmark, hvis vi bliver ramt?

Der synes i den forbindelse at være behov for, at der udvikles nogle relativt klare retningslinjer for, hvornår cyberangreb mod Danmark har karakter af henholdsvis ulovlig intervention, ulovlig magtanvendelse eller sågar egentlige væbnede angreb, der udløser en dansk ret til selvforsvar. Hvornår mener vi eksempelvis fra dansk side, at cyberangreb bliver så voldsomme, at de udløser en dansk ret til selvforsvar?

To tiltag synes i den forbindelse at være særlig presserende.

For det første bør de relevante danske myndigheder gøre sig overvejelser om, hvilke dele af den danske infrastruktur der er af særlig betydning ikke kun for et effektivt forsvar af nationen, men også for myndighedernes muligheder for at løse væsentlige samfundsopgaver. Som så mange andre stater har vi med andre ord også i Danmark behov for at identificere den del af vores infrastruktur, der er særlig kritisk. Det anbefales derfor i dette papir, at de relevante danske myndigheder påbegynder dette arbejde.

For det andet – og i forlængelse heraf – bør der udarbejdes nogle klare retningslinjer for, hvordan Danmark, herunder forsvaret, skal reagere på konkrete cyberangreb. Der findes allerede retningslinjer, såsom en kongelig forholdsordre fra 1954[123], for, hvordan de danske styrker skal reagere på traditionelle kinetiske angreb, men der findes ikke noget tilsvarende på cyberområdet. Ligesom det i midten af det forrige århundrede blev skønnet nødvendigt at udarbejde en forholdsordre om, hvordan de danske styrker skulle forholde sig i tilfælde af et angreb på Danmark, har vi her i starten af det 21. århundrede behov for en ny 'ordre', der fastslår, hvordan forsvaret og de danske styrker skal forholde sig i tilfælde af omfattende cyberangreb på Danmark.

Hvis krigsførelse i stigende grad sker med elektroniske midler, så skal vi have retningslinjer for elektronisk krigsførelse, og det anbefales derfor også i denne rapport, at der udarbejdes en form for 'cyberforholdsordre', der gør det klart for det danske forsvar, hvordan det skal forholde sig i tilfælde af cyberangreb.

Det er i den forbindelse også værd at bemærke, at en eventuel 'cyberforholdsordre' vil bidrage til bestræbelserne på at afskrække potentielle fjender fra at iværksætte cyberangreb mod Danmark.[124]

Konklusion

Det er behæftet med store vanskeligheder at vurdere foreneligheden af CNO med den del af folkeretten, der regulerer, hvornår stater må gøre brug af væbnet magt mod hinanden.

Det konkluderes ikke desto mindre – forsøgsvis – i dette papir, at cyberangreb vil kunne krænke det folkeretlige forbud mod intervention, hvis det udgør pression, der har til formål at påvirke en anden stats politik på et område, hvor staten ikke skal tåle international indblanding. Hvorvidt det vil være tilfældet, afhænger af en konkret vurdering, men inkluderingen af økonomisk pression inden for rammerne af interventionsforbuddet øger sandsynligheden for, at cyberangreb mod økonomisk infrastruktur, såsom finansiel infrastruktur, vil være at anse som ulovlig indblanding.

Det konkluderedes også, at der sandsynligvis skal anlægges en effektbaseret tilgang til vurderingen af, om cyberangreb kan udgøre magtanvendelse i henhold til FN-pagtens artikel 2, stk. 4, og at det derfor også må konkluderes, at i hvert fald visse typer CNO vil kunne krænke FN-pagtens magtforbud. Og den effektbaserede tilgang betyder også, at særligt alvorlige cyberangreb endvidere vil kunne udgøre væbnede angreb, der udløser en ret til selvforsvar i henhold til FN-pagtens artikel 51.

Dersom et cyberangreb opfylder betingelserne for at udgøre et væbnet angreb, vil den stat, der gøres til genstand for angrebet, være berettiget til at iværksætte de væbnede handlinger, der måtte være nødvendige for at forsvare sig mod angrebet. Det er i den forbindelse værd at hæfte sig ved, at der ikke gælder noget krav om, at selvforsvarshandlinger skal udøves på samme måde og med samme midler som angrebet, og at en stat derfor efter omstændighederne kan være berettiget til at forsvare sig mod et cyberangreb med traditionelle væbnede midler.

Hvis et cyberangreb ikke er tilstrækkelig alvorligt til at udgøre et 'væbnet angreb', der udløser en ret til selvforsvar, er en stat ikke berettiget til at gøre brug af magtanvendelse som beskrevet i artikel 2, stk. 4, for at forsøge at bringe det pågældende angreb til standsning. Staten vil imidlertid som udgangspunkt være berettiget til at iværksætte passende modforanstaltninger.

Stater er kun ansvarlige for de cyberangreb, der udføres af statsansatte personer eller af andre personer, som staten er i stand til at udøve effektiv kontrol over, på det tidspunkt hvor angrebene udføres. Det kan i praksis skabe problemer for de stater, der udsættes for cyberangreb, som de mistænker andre stater for at stå bag.

Det konkluderes imidlertid også, at en stat, der er mål for en privat aktørs cyberangreb, efter omstændighederne kan være berettiget til at iværksætte modforanstaltninger, herunder eventuelt egentlige

selvforsvarshandlinger, for at bringe angrebene til ophør. Retten til at iværksætte modforanstaltninger mod en privat aktør er imidlertid subsidiær i forhold til værtsstatens ret til at standse de pågældende angreb, og retten til at iværksætte modforanstaltninger udløses med andre ord også først på det tidspunkt, hvor værtsstaten har vist sig at mangle enten den fornødne vilje eller evne til at standse angrebene fra den private aktør.

Det er i Danmarks interesse, at der skabes klarhed om de retlige normer i cyberspace, og den aktuelle uklarhed kalder derfor på en stillingtagen fra Danmark, herunder fra Forsvarsministeriet.

Der er flere grunde til, at det ville være nærliggende at mene, at Danmark skulle arbejde for, at man i det internationale samfund fik skabt et folkeretligt regelsæt, der er specifikt målrettet reguleringen af cyberangreb.

Det er imidlertid ikke anbefalingen i dette papir. Dels er vi formentlig fortsat i de tidlige stadier af udviklingen i cyberspace, og dels er der efter alt at dømme stor forskel på, hvilke retlige normer stater egentlig ønsker i cyberspace.

Det anbefales i stedet, at Danmark gør sig overvejelser om, hvilke ikke-retligt bindende *normer for adfærd* vi fra dansk side ønsker i cyberspace. Det er i den forbindelse vigtigt, at Danmark holder sig for øje, at udvikling af normer i høj grad handler om strategi, og at vi derfor også er på det rene med, at den aktuelle uklarhed om den folkeretlige regulering af cyber ikke kun er et problem, men i høj grad også en mulighed for Danmark og det danske forsvar for at søge at fremme vores strategiske interesser.

Det anbefales også, at Danmark indleder bestræbelserne på at afklare, hvilke normer for adfærd vi gerne ser i cyberspace, med en mere grundlæggende analyse af Danmarks strategiske interesser og en efterfølgende vurdering af, hvordan cyberspace kan forenes hermed.

En mulighed er, at Danmark betragter cyberspace som en såkaldt ’global common’, og at vi fra dansk side arbejder for, at reguleringen af cyberspace i store træk bør følge principperne for reguleringen af de andre ’commons of mankind’.

Endelig er det oplagt, at de relevante myndigheder i Danmark skal sørge for at have planer for, hvordan vi fra dansk side skal reagere over for eventuelle cyberangreb, som vi måtte blive udsat for. Der synes i den forbindelse at være behov for, at der udvikles nogle retningslinjer for, hvornår vi fra dansk side mener, at cyberangreb mod Danmark bliver så voldsomme, at de potentielt set kan udløse en dansk ret til selvforsvar.

Som så mange andre stater har Danmark i den forbindelse behov for at identificere den del af vores infrastruktur, der er særlig kritisk. Herudover bør der udarbejdes nogle klare retningslinjer for, hvordan Danmark, herunder forsvaret, skal reagere på konkrete cyberangreb. En mulighed er at udarbejde en form for 'cyberforholdsordre', der gør det klart for det danske forsvar, hvordan det skal forholde sig i tilfælde af cyberangreb.

Noter

[1] *United States National Military Strategy for Cyberspace Operations,* GL-1
[2] Se bl.a. diskussionen i *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston*, 28 May 2010, A/HRC/14/24/Add. 6
[3] Matthew C. Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), *Yale Journal of International Law*, vol. 36 (2011), s. 425. Se også Yoram Dinstein, 'Computer Network Attacks and Self-Defense', i *Computer network attack and international law; Symposium on Computer Network Attack and International Law*, 1999, Naval War College, s. 114: 'The novelty of a weapon – any weapon – always baffles statesmen and lawyers, many of whom are perplexed by technological innovations … In reality, after a period of gestation, it usually dawns on belligerent parties that there is no insuperable difficulty in applying the general principles and rules of international law to the novel weapon.'
[4] Convention on Cybercrime, ETS no. 185 (2001).
[5] Daniel Kuehl, 'Information Operations, Information Warfare, and Computer Network Attack', i *Computer network attack and international law; Symposium on Computer Network Attack and International Law*, 1999, Naval War College, s. 54.
[6] Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law – Thoughts on a Normative Framework', *Columbia Journal of Transnational Law*, vol. 37 (1999), s. 912
[7] DoD, Office of Legal Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, s. 18.
[8] Det skal for en god ordens skyld bemærkes, at det er et generelt folkeretligt princip, at stater er ansvarlige for de retsstridige handlinger, som de foretager sig mod andre stater, og en stat vil derfor som det helt klare udgangspunkt også være folkeretligt ansvarlig, herunder eventuelt erstatningsansvarlig, for de retsstridige cyberangreb, som staten foretager mod andre stater.
[9] Se præamblen til Wienerkonventionen om traktater, hvor 'non-interference in the domestic affairs of States' er at finde blandt folkeretlige principper 'embodied in the Charter of the United Nations.'
[10] Se hertil FN-pagtens artikel 2, stk. 1.
[11] Det tætteste er artikel 2, stk. 7, der beskytter medlemsstaterne mod organisationens indblanding i staternes indre anliggender.
[12] *The Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations (1970)*, UN Doc. A/RES/2625 (XXV). En anden central resolution er *Declaration on the Inadmissibility of Intervention into the Domestic Affairs of States (1965)*, GA res. 2131 A/6014.
[13] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA)*, Judgment, ICJ Rep. (1986) 14, præmis 202. Se også domstolens tidligere afgørelse i *Corfu Channel (United Kingdom v. Albania)*, Judgment, ICJ Rep. (1949) 4, præmis 35 og *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, ICJ Rep. (2005) 000, præmis 164-5.
[14] Se gennemgangen i Maziar Jamnejad & Michael Wood, 'The Principle of Non-intervention', *Leiden Journal of International Law*, 22 (2009), s. 351-357. Det drejer sig bl.a. om *Declaration on the Inadminissiblity of Intervention and Interference in the Internal Affairs of States*, se Jamnejad & Wood i referencen ovenfor, s. 355.
[15] Se også *Nicaragua* (note 13) præmis 205 ('matters in which each State is permitted, by the principle of State sovereignty, to decide freely').
[16] Jamnejad & Wood (se note 14) s. 349.
[17] Ibid. s. 348. Se også resolutionen vedrørende venskabelige relationer (note 12) ('No State may use or encourage the use of economic, political or any other type of measures to *coerce* (min kursivering) another State …'). Se også *Nicaragua* (note 13) præmis 205 ('The element of *coercion* (min kursivering), which defines, and indeed forms the very essence of, prohibited intervention …') og ('Intervention is wrongful when it uses methods of *coercion* (min kursivering) in regard to such choices, which must remain free ones …')
[18] For støtte i litteraturen til konklusionen om, at CNO kan krænke interventionsforbuddet, se bl.a. Christopher C. Joyner & Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework', *European Journal of International Law* (2001), vol. 12, no. 5, s. 849; Marco Roscini, 'World Wide Warfare – Jus ad bellum and the Use of Cyber Force', *Max Planck UNYB*, 14 (2010), s. 102-3 og Joanna Kulesza, 'State responsibility for cyber-attacks on international peace and security', *Polish Yearbook on International Law* (2009), s. 6-7.

[19] For en oversigt over noget af debatten, se Anders Henriksen, *Krigens folkeret – og international væbnet terrorbekæmpelse*, Jurist- og Økonomforbundets forlag, 2010, s. 31-40.
[20] Albrecht Randelzhofer, 'Article 2(4)', i *The Charter of the United Nations: A Commentary* (Bruno Simma, ed., 2nd ed.) (2002), s. 117 ('limited to armed force'). Se også D.W. Bowett, Self-Defence in International Law, Frederick A. Prager, 1958, s. 148, Ian Brownlie, *International Law and the Use of Force by States*, Oxford University Press, 1963, s. 361.
[21] *Documents of the United Nations Conference on International Organization*, 1945, vol. VI, 559, 720-721.
[22] Se hertil bl.a. gennemgangen i Daniel B. Silver, 'Computer Network Attack as a Use of Force under Article 2(4)', i *Computer network attack and international law; Symposium on Computer Network Attack and International Law*, 1999, Naval War College s. 81.
[23] *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, ICJ Rep. (1996) 226, præmis 39.
[24] Jason Barkham, 'Information Warfare and International Law on the Use of Force', *New York University Journal of International Law and Politics*, vol. 34, 2001-2002, s. 79. Se også Julie J.C.H. Ryan, Daniel J. Ryan & Eneken Tikk, 'Cyber Security Regulation: Using Analogies to Develop Frameworks for Regulation', i *International Cyber Security: Legal & policy Proceedings*, CCDCOE, 2010, s. 94.
[25] Barkham (note 24) s. 72. Se også Roscini (note 18) s. 104-7.
[26] DoD (note 7) s. 18.
[27] Roscini (note 18) s. 108-9.
[28] Se hertil Henriksen (note 19) s. 123.
[29] Dinstein (note 3) s. 103.
[30] Barkham (note 24) s. 80.
[31] Silver (note 22) s. 85. Se også Roscini (note 18) s. 107 ('The fact that several states have included cyber technology in their military doctrines, refer to it as "cyber warfare" and have set up military units with specific cyber expertise supports the view that Trojan horses, worms, viruses and so on are indeed regarded as "just another weapons system ...')
[32] Silver (note 22) s. 85.
[33] Joyner & Lotrionte (note 18) s. 850. Et andet bud på at vurdere, hvornår CNO er at anse som magt i henhold til artikel 2, stk. 4, kommer fra Michael N. Schmitt, der opstiller en række kriterier for, hvornår CNO falder henholdsvis inden for og uden for begrebet 'magt'. Det drejer sig om 'severity', 'immediacy', 'directness', 'invasiveness', 'measurability' og 'presumptive legitimacy', se Schmitt (note 6) s. 915. Se også Thomas C. Wingfield, 'CNA and the Jus ad Bellum: An Introduction', i *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law* (2004), Stockholm, s. 91-92.
[34] Se også Barkham (note 24) s. 59.
[35] Det grænseoverskridende element overses imidlertid ofte i litteraturen, se bl.a. Barkham (note 24) s. 87 & 89 og Matthew Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to the Right to Self-Defense', *Boston College International & Comparative Law Review*, vol. 32 (2009), s. 448-9.
[36] Se også Waxman (note 3) s. 431 ('there is considerable momentum among American scholars and policy experts behind the idea that some cyber-attacks ought to fall within Article 2(4)'s prohibition of "force" …')
[37] Joyner & Lotrionte (note 18) s. 846. Se også Barkham (note 24) s. 94: "The problem with failing to expand Article 2(4) is that it would become underinclusive. IW, like economic sanctions, would become a legal act under international law that many in the international community nonetheless would oppose. That would undermine respect for the prohibition on the use of force …"
[38] Walter Gray Sharp, Sr., *Cyberspace and the Use of Force* (1999), s. 140.
[39] *Nicaragua* (note 13) præmis 191.
[40] Ibid. præmis 195. Se også ICJ *Oil Platform*, ICJ Rep. (2003) 161, præmis 51.
[41] Generalforsamlingsresolution 3314 af 14. december 1974, se art. 2: "The first use of armed force by a state in contravention of the charter shall constitute prima facie evidence of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including *the fact that the acts concerned or their consequences are not of sufficient gravity* (min kursivering)".
[42] *Nicaragua* (note 13) præmis 195: "But the Court does not believe that the concept of "armed attack" includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support. Such assistance may be regarded as a threat or use of force".

[43] Se henvisningen i note 42. Der er ikke fuldkommen identitet mellem begreberne 'væbnet angreb' og 'aggression', men et 'væbnet angreb' må anses for at være en form for aggression, se også Yoram Dinstein, *War, Aggression and Self-Defense*, 4. udg., Cambridge University Press, 2005, s. 184.
[44] Dinstein (note 43) s. 193.
[45] Joyner & Lotrionte (note 18) s. 855.
[46] Ryan (note 24) s. 94-95.
[47] Dinstein (note 3) s. 103. Se også Dinstein (note 43) s. 196.
[48] Dinstein (note 3) s. 105.
[49] DoD (note 7) s. 18.
[50] Steven G. Bradbury, Keynote Address: 'The Developing Legal Framework for Defensive and Offensive Cyber Operations', *Harvard National Security Journal*, vol. 2 (unummereret).
[51] Horace B. Robertson, Jr., 'Self-Defense against Computer Network Attack', i *Computer network attack and international law; Symposium on Computer Network Attack and International Law*, 1999, Naval War College, s. 138. For et andet bud se Sharp (note 38) s. 130
[52] Joyner & Lotrionte (note 18) s. 855.
[53] Se bl.a. *United States National Strategy to Secure Cyberspace,* February 2003, s. 1 og *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets,* February 2003, s. 35.
[54] United Kingdom Government, *United Kingdom Cyber Security Strategy*, June 2009, s. 9.
[55] Australian Government, *Cyber Security Strategy*, 2009, s. 20.
[56] EU Commission, *Green Paper on a European Programme on Critical Infrastructure Protection*, November 2005, s. 20.
[57] FN's Generalforsamling udtalte i 2003, at det er op til hver enkelt stat at 'determine its own critical infrastructure'. A/RES/58/199 af 23. december 2003
[58] Se også Dinstein (note 3) s. 106 og Roscini (note 18) s. 116.
[59] Se også artikel 21 i Den Internationale Lovkommissions retningslinjer for staters ansvar, se hertil Generalforsamlingsresolution 56/83 af 12. december 2001.
[60] Dinstein (43) s. 187, Ole Spiermann, *Moderne Folkeret*, 3. udg., Jurist- og Økonomforbundets Forlag, 2006, s. 433 og Dansk Institut for Internationale Studier, *Nye Trusler og Militær Magtanvendelse*, 2005, s. 79.
[61] Se hertil bl.a. *Nicaragua* (note 13) præmis 176, *Nuclear Weapons* (note 23) præmis 41, *Oil Platforms* (note 40) præmis 76-77 og *Armed Activities* (note 13) præmis 147.
[62] Se hertil også redegørelsen fra Dansk Institut for Internationale Studier (note 60) s. 74. Om repressalier eller modforanstaltninger generelt, se Lovkommissionens retningslinjer for statsansvar (note 59), artikel 22 og 49-51.
[63] *Nuclear Weapons* (note 23) præmis 46. Se også artikel 50, stk. 1, litra a, i Lovkommissionens retningslinjer for statsansvar (note 59) og resolutionen om venskabelige relationer (note 12).
[64] *Nicaragua* (note 13) præmis 237, *Oil Platforms* (note 40) præmis 77 og *Armed Activities* (note 13) præmis 147. I sin vejledende udtalelse i *Nuclear Weapons* (se note 23) bemærkede Den Internationale Domstol i præmis 42, at kravet om proportionalitet også fordrer, at selvforsvar skal udøves inden for rammerne af den humanitære folkeret. Som berørt indledningsvist i dette notat berøres *jus in bello* imidlertid ikke på dette sted.
[65] Roberto Ago, 'Addendum to Eighth Report on State Responsibility', *International Law Commission Yearbook*, vol. 13, 1980, s. 69. Se også Rosalyn Higgins, *Problems and Progress; International Law and How We Use it*, Clarendon Press, 1994, s. 232.
[66] DoD (note 7) s. 18.
[67] Se Lovkommissionens retningslinjer for statsansvar (note 59), artikel 49.
[68] Ibid. artikel 51.
[69] Det er nemlig kun i tilfælde af et 'væbnet angreb' eller et mandat fra FN's Sikkerhedsråd, at en stat må bruge magt i henhold til artikel 2, stk. 4.
[70] FN's Sikkerhedsråd er tillagt det primære ansvar for opretholdelsen af international fred og sikkerhed og er efter kapitel 7 beføjet til at vedtage bindende resolutioner eller om nødvendigt iværksætte de midler, der skønnes nødvendige for at genoprette international fred og sikkerhed.
[71] DoD (note 7) s. 19-20.
[72] Paul Cornish m.fl., *On Cyber Warfare*, Chatham House, November 2010, s. 11.
[73] Se artikel 4 (note 59).

[74] Se hertil også artikel 3 (g) i definitionen af aggression, hvorefter aggression bl.a. kan bestå i 'The sending by or *on behalf of a State* (min kursivering) of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State.'
[75] Se Lovkommissionens retningslinjer for statsansvar (note 59), artikel 8.
[76] *Nicaragua* (note 13) præmis 115. Se også kommentarerne til artikel 8 i Lovkommissionens retningslinjer for statsansvar 2001, gengivet i *Yearbook of the International Law Commission, 2001*, vol. II, Part Two: "(3) … Such conduct will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of was an integral part of that operation. The principle does not extend to conduct which was only incidentally or peripherally associated with an operation and which escaped from the State's direction or control."
[77] ICTY *Tadic, Appeals Chamber, Judgement*, 15. juli 1999, præmis 117 og præmis 137.
[78] Se bl.a. *Armed Activities* (note 13) præmis 160.
[79] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, ICJ Rep. (2007) 43, præmis 400. Det skal også nævnes, at det af artikel 11 i de internationale retningslinjer for statsansvar fremgår, at en stat også vil kunne ifalde et internationalt ansvar for private personers ulovlige handlinger, såsom international terrorisme, hvis staten *efterfølgende* anerkender handlingerne og lader dem indgå i sin politik (*"acknowledges and adopts the conduct in question as its own"*), se hertil også *United States Diplomatic and Consular Staff in Tehran,* ICJ Rep. (1980) 3, præmis 74. Hvor meget der i praksis skal til, før en stat overtager ansvaret for private personers handlinger i henhold til artikel 11, vil i sagens natur altid bero på en konkret vurdering.
[80] Cornish m.fl. (note 72) s. 13.
[81] Hoisington (note 35) s. 453. Se også Joyner & Lotrionte (note 18)
[82] Dinstein (note 3) s. 111. Se også Barkham (note 24) s. 82: "If a target state were to detect an IW attack in progress, traditional international law would require it to wait until damage occurred to know whether or not the action would qualify as an armed attack."
[83] Barkham (note 24) s. 82.
[84] Se også Dinstein (note 3) s. 112.
[85] Se hertil også gennemgangen i Henriksen (note 19) s. 123. Se også konklusionerne i redegørelsen fra DIIS (note 60) s. 71.
[86] *Corfu Channel* (note 13) s. 22.
[87] Se Dinstein (note 43) s. 245. Se også Henriksen (note 19) s. 125-127.
[88] Denne form for selvforsvar er på den baggrund blevet betegnet som en form for 'extra-territorial law-enforcement', se Dinstein (note 43) s. 245.
[89] For faktuelle oplysninger se Eneken Tikk m.fl., *International Cyber Incidents: Legal Considerations*, CCDCOE, 2010, s. 14-34. Se også oversigten i Scott J. Shackelford, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', *Berkeley Journal of International Law*, vol. 25, no. 3, (2009), s. 192-251
[90] Tikk m.fl. (note 89), s. 51-65.
[91] Ibid. s. 55.
[92] Ibid. s. 25-26.
[93] Ibid. s. 31-32.
[94] Se bl.a. Holger Stark, 'Mossad's Miracle Weapon, Stuxnet Virus Opens New Era of Cyber War', *Der Spiegel*, 08/08/2011. Se også William J. Borad m.fl., 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay', *New York Times*, January 15, 2011.
[95] David E. Sanger & Mark Mazetti, 'Israel Struck Syrian Nuclear Project, Analysts Say', *New York Times*, October 14, 2007. Israel har aldrig indrømmet angrebet.
[96] Eric Schmitt & Thom Shanker, 'U.S. Debated Cyberwarfare in Attack Plan on Libya', *New York Times*, October 17, 2011.
[97] Der ses her bort fra det forhold, at luftbombardementerne af Libyen var baseret på en bemyndigelse fra FN's Sikkerhedsråd, se Sikkerhedsrådsresolution 1973 af 17. marts 2011.
[98] For oplysninger se Tikk m.fl. (note 89) s. 66-90
[99] *Georgian Ministry of Foreign Affairs*, 'Cyber Attacks Disable Georgian Websites', 11. august 2011.
[100] Tikk m.fl. (note 89) s. 75.
[101] Se bl.a. Barkham (note 24), s. 95 og Kulesza (note 18) s. 12-13.
[102] Rex Hughes, 'A treaty for cyberspace', *International Affairs*, vol. 86, no. 2 (March 2010), s. 523-541.

[103] Ryan m.fl. (note 24) s. 97.
[104] Waxman (note 3) s. 450.
[105] Om udviklingen af normer i cyberspace se bl.a. Martha Finnemore, 'Cultivating International Cyber Norms', i Center for a New American Security, *America's Cyber Future; Security and Prosperity in the Information Age*, juni 2011, s. 87-101
[106] Cornish m.fl. (note 72) s. 19
[107] *United States International Strategy for Cyberspace; Prosperity, Security, and Openness in a Networked World*, May 2011, s. 9.
[108] De ti regler kan findes i Eneken Tikk, '10 Rules of Behaviour for Cyber Security', *Survival*, vol. 53, issue 3, 2011, s. 119-132. Se også Daniel J. Ryan m.fl., 'International Cyberlaw: A Normative Approach', *Georgetown Journal of International Law*, vol. 42, 2011, s. 1161-1197.
[109] Warwick Ashford, 'US joins UN cyber arms control collaboration', *Computer Weekly*, 20 July 2010.
[110] Waxman (note 3) s. 448.
[111] Ibid. s. 452.
[112] Se Ministry of Foreign Affairs of Denmark, *The Copenhagen Process on the Handling of Detainees in International Military Operations*, december 2007.
[113] Se note 53
[114] Se note 54
[115] Se note 55
[116] *Défense et sécurité des systémes d'information, Stratégie de la France*, februar 2011.
[117] Federal Ministry of the Interior*, Cyber Security Strategy for Germany*, februar 2011.
[118] Ministry of Security and Justice, *The National Cyber Security Strategy (NCSS), Success through cooperation*, februar 2011.
[119] Se også Ryan (note 24) s. 76-99.
[120] For en oversigt over denne regulering, se Ryan (note 24) s. 76-99.
[121] Se hertil Shackelford (note 89) s. 211-212. Se også Jennifer Frakes, Notes and Comments: 'The Common Heritage of Mankind Principle and the Deep Seabed, Outer Space, and Antarctica', *Wisconsin International Law Journal*, vol. 21, 2003, s. 411-413.
[122] Se også Ryan (note 24) s. 92. Se hertil også Jack Goldsmith, *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press, 2006.
[123] *Anordning om forholdsordre for det militære forsvar ved angreb på landet og under krig* af 6. marts 1952 og *Anordning om ændringer i anordning om forholdsordre for det militære forsvar ved angreb på landet og under krig* af 26. april 1961
[124] Om afskrækkelse i cyberspace se bl.a. Bjørn Møller, 'Cyberspace: The New Battlefield? War, Crime and Terrorism: Threats and Protection' (endnu ikke offentliggjort) s. 8.