FORSVARSAKADEMIET

Brief

7. MARTS 2017

HVAD ER RAMMERNE FOR ET LOVLIGT CYBERFORSVAR?

Af Studielektor Dorthe Bach Nyemann, Institut for Strategi

FORSVARET

Hvad er rammerne for et lovligt cyberforsvar?

København marts 2017
Forsvarsakademiet
Svanemøllens Kaserne
Ryvangs Allé 1
2100 København Ø
Tlf.: +45 728 17000
Ansvarshavende redaktør: Anja Dalgaard-Nielsen, chef for Institut for Strategi
Layout: FAK
ISBN: 978-87-7147-181-6

INDHOLDSFORTEGNELSE

INDLEDNING

Når Danmark konfronteres med et stigende antal cyberangreb rettet mod både enkeltpersoner, virksomheder, statens vitale infrastruktur, samt i de institutioner, der udgør fundamentet for vores nationale sikkerhed, må det afføde overvejelser af både politisk og juridisk art. De seneste år er der derfor taget en række initiativer som for eksempel oprettelsen af Center for Cybersikkerhed i 2012 under Forsvarsministeriet, og senest har vi, som del af det sidste danske forsvarsforlig, set oprettelsen af en Computer Network Operations (CNO) kapacitet, der skal kunne forsvare egen digital infrastruktur, men også gennemføre militære angreb på en fjendtlig aktørs digitale infrastruktur (Redegørelse for den tværministerielle arbejdsgruppe om Folketingets inddragelse ved anvendelse af den militære Computer Network Attack (CNA) - kapacitet, 2015-16).Internationalt ser vi ligeledes en kraftig vækst i initiativer til beskyttelse af staterne og formulering af strategier til bekæmpelse af cyberangreb, både i staterne selv og i organisationer som NATO (Lin, 2016) (The White House, 2011) (NATO, 2014) (Regeringen, 2014). Tiltagene har i første omgang drejet sig om identifikation af sårbarheder i cyberspace og i den fysiske infrastruktur, der understøtter dette og efterfølgende til opbyggelse af kapabiliteter til forsvar i forbindelse med cyberangreb. I de senere år er det desuden i tiltagende grad blevet legitimt at tale om, at staterne også opbygger offensive cyberkapabiliteter (Lewis, 2015). Udviklingen af cyberkapabiliter kan i et strategisk perspektiv anskues i forhold til den generelle magtbalance mellem stater, og kan her være med til at udfordre den klassiske forståelse af deterence. Det har også en betydning for opfattelsen af asymmetrisk krigsførelse, kapabilitetens særlige rolle i hybrid krigsførelse etc. Dette brief vil imidlertid ikke udfolde de strategiske implikationer, men i stedet fokusere på de folkeretlige udfordringer, der gør sig gældende, når cyberangreb og modangreb bringes i anvendelse.

Der er allerede mange forskere, der har beskæftiget sig med udfordringerne for folkeretten og særligt med udarbejdelsen af Tallinn Manualen og de mange publikationer op til og efter dennes udgivelse, må der siges at være en rig juridisk diskussion på området (Heinegg, 2012) (Allan, 2013) (Henriksen, 2014) (Schmitt M. N., 2013) (Sklerov, 2009). Imidlertid er staternes praksis og fortolkninger af handlinger begået i dette nye domæne helt afgørende for, hvordan folkeretten vil udvikle sig. Her er det afgørende, at Danmark bidrager med en adfærd og en dertil knyttet retsopfattelse, som tjener vores interesser i en international retsorden, der er til fordel for småstater og som samtidig giver os de handlemuligheder, der er nødvendige til lovligt at kunne imødegå de nye trusler som cyberangreb af forskellig art udgør. I dette brief søger jeg, at sætte lys på to helt centrale spørgsmål omkring *adfærd* og *retsopfattelse* i cyberspace.

Det første spørgsmål omhandler selve definitionen af et væbnet angreb i cyberspace, og hvorvidt statspraksis kan eller bør være med til at udvide denne *definition i forhold til den vi har i dag.*

Det andet spørgsmål handler om, hvorvidt stater lovligt kan modsvare cyberangreb med forskellige midler, uden at de gældende regler for attribution af statsansvar finder anvendelse.

Briefet her vil søge at etablere disse spørgsmåls relevans og betydning for staters fremtidige lovlige handlemuligheder. Det må efterfølgende kalde på yderligere analyser af de to spørgsmåls omfang og implikationer for at finde mere dybdegående svar på, hvor staternes praksis med fordel kan udvikle sig.

Samtidig afventer vi endnu med spænding Tallinn Manualens efterfølger, der er lige på trapperne, og som gerne skal give spændende indspark til den meget afgørende juridiske diskussion af de situationer, hvor cyberangreb, netop *ikke* er væbnede, og hvor modforanstaltningerne og en eventuel international regulering derfor kræver noget helt andet.

OM KILDER

Cyberaktiviteter kan ud over helt normal adfærd i cyberspace enten anskues som grænseoverskridende kriminalitet, spionage eller andre uvenlige handlinger samt som et væbnet angreb. Fortolkningen vil være afhængigt af den kontekst cyberaktiviteten indgår i, og de konsekvenser det har for enten staten, en privat gruppe af borgere eller en virksomhed samt i det omfang, det lader sig afdække, hvilke *intentioner*, der lå bag handlingen og *de aktører*, der gennemførte dem.

Anskuer vi aktiviteten som cyberkriminalitet, skal det behandles via de nationale retsinstanser. Herudover findes der en konvention om cyberkriminalitet, den såkaldte Budapest Konvention, der kriminaliserer en række handlinger i cyberspace, hvis formål er at harmonisere de nationale lovgivninger, således at grænseoverskridende cyberkriminalitet bedre kan håndteres i fællesskab (Convention on Cybercrime, Budapest, 2001). Omkring 50 stater har ratificeret denne traktat.

Anskues handlingen i stedet som spionage er den kriminaliseret i de nationale retssystemer, men er ikke i sig selv ulovlig efter international ret. (Schmitt, 2013, rule 10, para 8). Der findes ikke nogen traktat, der forbyder spionage og adfærden ses som et nødvendigt onde, om end den kan opfattes som værende i strid med de folkeretlige grundprincipper. Spioner mister derfor også deres kombattantstatus ved pågribelse under en væbnet konflikt og kan udvises i fredstid, selvom vedkommende har diplomatstatus. Kontinuummet af uvenlige handlinger mellem stater bevæger sig fra "*the fair game of spying on each others institutions, [to] making data public – in true or altered form – [in order] to influence [e.g.] an election [which] is a new level of malicious activity*" som John O. Brennan, director of the Central Intelligence Agency, USA udtrykker det (Sanger, 2016).

Selvom der kun har været ganske lidt statspraksis eller *opinio juris* i forhold til, hvornår en handling i cyberspace kan opfattes som angreb mod staten og ikke "bare" grænseoverskridende kriminalitet, spionage eller andre uvenlige handlinger, er der fornyligt begyndt at komme udmeldinger, der kan anvendes i fremtidige fortolkninger af den internationale ret på området. Disse vil blive inddraget i analysen af udviklingen i vores forståelse af cyberangreb.

Ved vurdering af lovligheden af handlinger i cyberspace tages her udgangspunkt i Tallinn Manualen. Tallinn Manualen er en ekspertgruppes bud på at skabe konsensus om, i hvilket omfang og i hvilken udstrækning folkeretten, og herunder også den internationale humanitære folkeret, er gældende i relation til en række forskellige incidenter i cyberspace. Den er derfor alene en god indikator på, hvordan stater vil fortolke og anvende folkeretten. Tallinn Manualen vil med sikkerhed præge den sædvaneretlige udvikling og kan indeholde gældende ret, men har altså hverken status af sædvaneret eller traktat. Herudover inddrages FN-pagten og centrale domme fra internationale domstole.

ANONYMITET OG ANARKI SOM JURIDISK UDFORDRING

De juridiske diskussioner omkring cyberangreb har indtil nu kredset meget omkring vanskelighederne omkring attribution og regulering af aktiviteter i cyberspace. Umiddelbart synes en af de helt store problemstillinger i den forbindelse at omhandle anonymitet. Hvis vi ikke ved, hvor handlingen stammer fra, er det vanskeligt at afgøre, hvilke intentioner, der ligger bag og derfor også vanskeligt at afgøre, om der er tale om kriminalitet eller et angreb. Det er ligeledes vanskeligt, at etablere tilstrækkelig bevisbyrde til, at vi kan stille stater til ansvar for handlinger, der oftest alene falder tilbage på de patriotiske hackergrupper, som den umiddelbare afsender. Uden klar attribution til staten bliver det ikke muligt at gå til Den Internationale Domstol eller bruge de sanktioner, der opregnes i Draft articles on Responsibility of States for Internationally Wrongful Acts, fra 2001. Det giver helt nye muligheder for at føre proxy krig, og ”plausible deniability” for stater.(Henriksen & Ringsmose, 2014,10, s. 36,37).

Muligheden for at være anonym har betydet en eksplosiv vækst i mindre alvorlige cyberhændelser, men det har imidlertid kun ført til nogle ganske få tilfælde med mere vidtrækkende konsekvenser (Henriksen & Ringsmose, 2014,10, s. 24,25). Mindre cyberoperationer, der indebærer spionage eller disruption frem for egentlige væbnede angreb, er en velegnet metode til at balancere stærkere magter i et domæne, hvor der lettere opstår en ”lige konkurrence”, samt til at genere svagere magter, der ikke har ressourcer til at gennemføre undersøgelser af, hvor angrebet kommer fra og heller ikke kan etablere et modsvar (Valeriano & Maness, 2015, s. 190). Såfremt angrebet bliver voldsomt nok, menes staterne faktisk i dag at have de ressourcer og metoder der skal til for finde ud af, hvem der stor bag et givent angreb. En af årsagerne er, at når det gælder anvendelsen af mere avancerede cybervåben, er det kun ganske få statslige aktører, der har ekspertise og midler til at udvikle og anvende disse, og herved er det ”nemt” at finde frem til mulige afsender bag et angreb samt at sandsynliggøre, hvilke stater der har støttet en eventuel ikke-statslig aktør(Henriksen & Ringsmose, 2014,10, s. 25). Når det gælder væbnede angreb er anonymitet i cyberspace derfor i høj grad en illusion. Det er dog slet ikke det samme som at kunne fremlægge tilstrækkelige beviser til at etablere attribution til staten.

Den væsentligste årsag til cyberaktiviteternes tilsyneladende anonymitet er, at staterne selv har en række strategiske grunde til ikke at afsløre, i hvor høj grad de er under angreb eller af hvem. Herved afslører de nemlig deres egne systemers sårbarhed og et mangelfuldt forsvar

på cyberområdet. Hertil kommer, at især de mest magtfulde stater, der både har defensive og offensive cyberkapabiliteter, og samtidig har de bedste muligheder for at forme og præge folkeretten, kun i begrænset omfang er interesserede i at regulere cyberspace. Det skyldes først og fremmest, at der ikke eksisterer særligt store fælles interesser i, hvordan og med hvilket formål en sådan regulering skal finde sted(Henriksen & Ringsmose, 2014,10, s. 35) (The White House, 2011, s. 9-10).

Anonymiteten og den manglende fælles normdannelse og regulering af cyberaktiviteter dækker altså i nogen grad over nogle helt klassiske interessemodsætninger mellem staterne. Dette udspringer af de vilkår, der definerer det internationale system, herunder anarkiet. Staternes gensidige mistro til andres intentioner skaber en manglende vilje til at ville dele efterretninger og et ønske om at undgå begrænsninger i sine egne handlemuligheder. Det fastholder interessen i at skjule egne sårbarheder såvel som kapabiliteteter. Når det kommer til de folkeretlige udfordringer i cyberspace, er det faktisk i mindre grad domænets egenskaber, der skaber problemer, og i højere grad anvendelsen af ikke-statslige aktører til at gennemføre cyberangrebene, der er afgørende og skal håndteres i staters praksis og i fortolkning af folkeretten. Herved kommer de folkeretlige udfordringer i cyberspace til at ligne dem, vi kender fra andre domæner, hvor ikke-statslige aktører spiller en stadig større rolle.

ET VÆBNET ANGREB I CYBERSPACE?

Når vi skal indkredse, hvornår der er tale om et væbnet angreb i cyberspace, er det oplagt at se på to forskellige artikler i FN-pagten, nemlig 2,4 om "Use of force" og så artikel 51, der taler om "an armed attack". Use of force angiver, hvornår staternes suverænitet er blevet krænket. Hvorvidt en sådan krænkelse også er nok til at udgøre et væbnet angreb, der giver ret til selvforsvar i henhold til FN-pagten er et andet spørgsmål, som der er delte meninger om. Den internationale domstol har angivet en "de minimis" tærskel, som betyder, at der kan konstateres brug af væbnet magt over f.eks. en grænse (altså Use of force) uden at dette kommer til at udgøre et væbnet angreb i artikel 51s forstand (International Court of Justice, 1986, s. rep 14, 101, 103). Omvendt tilslutter flere sig teorien om akkumulering, hvor et mindre alvorligt tilfælde af voldsudøvelse i sammenhæng med andre tilfælde tilsammen kan opfattes som et væbnet angreb ifølge FN-pagten (Ruys, 2008, s. 7). Vi kan opstille nogle kriterier for, hvornår noget er "Use of force", men må ud fra en casebaseret betragtning afgøre, hvornår dette også er nok til at nå tærsklen for et væbnet angreb i henhold til artikel 51 i FN-pagten. Herudover er det også væsentligt at holde sig for øje, at retten til selvforsvar ikke bare reguleres af FN-pagten, men er en sædvaneretlig bestemmelse, der har videre rammer end ordlyden i artikel 51 favner. Det er derfor også muligt at sædvaneretten, i forhold til hvad der udgør et væbnet angreb med ret til selvforsvar, er ved at blive udvidet i takt med, at vi konstaterer forskellige typer af cyberangreb som nedenstående diskussion også vil pege på.

Ifølge Henriksen og Ringsmose kan vi forstå et angreb i cyberspace som handlinger:

> *"der er politisk og/eller strategisk motiverede, og som tager sigte mod at* ødelægge, manipulere eller nægte afgangen *til information lagret på en anden aktørs computere eller computernetværk. Det umiddelbare mål med et sådant angreb kan eksempelvis være at begrænse en modstanders evne til at kommunikere med egne militære styrker eller at ødelægge kritisk infrastruktur med henblik på at svække og destabilisere en fremmed stat. Hensigten kan også være at påføre en modstander civile eller militære tab ved eksempelvis at afspore tog, overbelaste nukleare reaktorer, forurene drikkevandsreservoirer eller afbryde strømforsyninger* (Henriksen & Ringsmose, 2014,10, s. 13).

Et angreb kan indenfor den forståelse altså indebære fysisk ødelæggelse, men kan også ske ved grov manipulation af data eller nægtet adgang til uundværlig information. Tallinn Manualen er mere snæver i sin præmis og knytter begrebet *angreb* sammen med anvendelsen af vold mod en modstander. I Tallinn Manualen arbejdes der med en *forventet effektbaseret* definition, hvor cyberaktiviteter alene kan blive til angreb "whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt, 2013, rule 30). Det skal altså være sammenligneligt med et væbnet angreb med konventionelle midler (Boothby, 2012, s. 384). Denne ret snævre fortolkning hænger sammen med det "mandat" Tallinn Manualens eksperter har givet sig selv; nemlig at fortolke gældende international ret i lyset af cyberaktiviteter.

Der kan være gode grunde til, at et rent cyberangreb uden fysiske ødelæggelser kan have samme konsekvenser som et kinetisk. Et vellykket cyberangreb på en børs eller i en nationalbank kan have samme konskvenser, som hvis man f.eks. bombede de samme centrale financielle institutioner. Ligeledes kan en lammelse af internetforbindelsen i et større område eller en længere periode have vidtrækkende konsekvenser økonomisk eller sikkerhedsmæssigt, uden at det nødvendigvis har en direkte destruktiv effekt på personer eller objekter. Det er ifølge Allan problematisk, at disse situationer ifølge Tallinn Manualen ikke sidestilles med angreb, hvori fysisk ødelæggelse finder sted, når vi afgør om der er tale om "use of force" FN-pagtens artikel 2.4 (Allan, 2013, s. 73). Som Tallinn Manualen også selv påpeger, vil man nok i et fremtidigt tilfælde, hvor der ikke er nogen ødelæggelse af fysiske installationer eller skader på befolkningen, men hvor et angreb har vidtrækkende konsekvenser for den angrebne stat, se, at staten *selv* opfatter dette som et væbnet angreb, og hermed kan udvikle statspraksis og opinio juris til en breddere forståelse af, hvad et væbnet angreb i cyberspace kan være, end det som Tallinn Manualen strækker sig til (Schmitt, 2013, rule 30,12). Statspraksis viser på nuværende tidspunkt, at staterne selv er klar til at anerkende cyberspace som et domæne, hvori væbnede angreb kan foregå. Efter NATO topmødet i 2014 blev følgende slået fast om NATO medlemmernes opfattelse af cyberspace:

> *"Our policy also recognizes that international law, including international humanitarian law and the UN Charter, applies in Cyberspace.() We affirm therefore that cyber defence is part of NATO´s core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken on a case-by-case basis." (NATO, 2014, punkt 72)*

Og videre

> *"We will continue to integrate cyber defence into NATO operations and operational and contingency planning. (NATO, 2014, punkt 73)"*

På en pressekonference 14. Juni 2016 gik NATO´s generalsekretær Jens Stoltenberg skridtet videre og slog fast at NATO

> *"will recognize cyberspace as an operational domain, just like air, sea and land…. treating cyber as an operational domain would enable ud to better protect our missions and operations"*

og han slog fast at

> *"a cyber attack can trigger Article 5, meaning that a cyber attack can trigger collective defence, because we regard cyber attacks as something that can cause a lot of damage and be very dangerous".*(Lin, 2016)

Som det ses af ovenstående udtalelser, anerkender man, at et cyberangreb kan være alvorligt nok til at udløse kollektivt selvforsvar – altså svarende til et "armed attack" i FN-pagtens artikel 51. Præmisserne er imidlertid ikke afklarede - *"a lot of damage"* er en politisk formulering helt åben for videre fortolkning. Dog viser citatet fra Stoltenberg, at fokus ligger på en vurdring af *effekten* af angrebet. Hvis vi skal komme det nærmere, må vi se på andre fortolkninger af, hvad der skal til for at man kan tale om et væbnet angreb. Hvis vi alene ser på FN-pagten er der ingen forklaring på, hvad man forstår ved hverken "Use of force" artikel 2,4 eller "armed attack" artikel 51, men i Den Internationale Domstols Nicaragua afgørelse blev det fastslået; at "scale and effect" skal tages i betragtning, når man afgør, hvorvidt bestemte handlinger kan udgøre et væbnet angreb (International Court of Justice, 1986, para 195). Ifølge Schmitt & Vihul betyder det, at "significant injury, death, physical damage or phycial destruction" er alvorligt nok til at udgøre et væbet angreb, også når det er effekter af et cyberangreb. Det er altså ikke *midlet*, men *effekten* i den fysiske verden, der afgører om noget udgør et væbnet angreb (Schmitt & Vihul, 2014, s. 67).

Når nu staterne ikke selv er klar til at opstille, hvilke kriterier de vil inddrage for at afgøre om et angreb i cyberspace kan sidestilles med et væbnet angreb, har eksperterne bag Tallinn Manualen forsøgt at opstille en række forhold til at afdække "scale and effect", som de forventer staterne

vil inddrage i deres bedømmelse af om der er tale om *"Use of force"* her nævnes kriterierne; *Severity, Immediacy, Directness, Invasiveness, Measurability of effects, Military character, State involvement, Presumptive legality* (Schmitt M. N., 2013, s. Rule 11, 9). Man kan forestille sig, at statspraksis i relation til cyberangreb særligt vil søge at udvide fortolkningen af *Immediacy og directness,* således at 2. eller 3. ordens effekter af et angreb f.eks. et imploderet aktiemarked med sammenbrud af centrale økonomoniske institutioner til følge vil være effekter, der bliver medregnet også selv om disse konekvenser først viser sig efter en længere periode og ikke direkte kan knyttes til angrebet. Ligeledes kan man forestille sig, at at angreb hvor *Invasiveness,* altså hvor nogen tilgår statens høj sensitive data knyttet til opretholdelsen af de nationale interesser koblet med at angrebet har en *Military character eller State involvement* fra en fremmed magt, vil give stater stærke inciamenter til at tolke disse handlinger som et væbnet angreb - også uden direkte fysiske effekter.

På nuværende tidspunkt med meget lidt statspraksis eller opinio juris er der ikke etableret en nedre grænse for, hvornår en cyberaktivitet kan karakteriseres som et væbnet angreb med ret til kollektivt selvforsvar. Der tegner sig en accept af, at aktiviteter, der alene foregår i cyberspace, kan udgøre et væbnet angreb, og at det er effekten frem for midlet, der afgør, om det kan opfattes som sådant. Foreløbig synes den nedre grænse for, hvornår et cyberangreb kan sidestilles med et kinetisk væbnet angreb at afhænge af, hvorvidt det har voldlige følger. Det betyder altså, at angreb, der kan sikre ekstern kontrol med statens vitale funktioner uden fysiske ødelæggelse ikke umiddelbart kan sidestilles med *Use of force* og derfor heller ikke kan anskues som et væbet angreb med ret til kollektivt selvforsvar.

En mulig fremtidig udvidelse af definitionen af et væbnet angreb, sådan som ovenstående diskussion lægger op til, vil på den ene side betyde en styrkelse af staternes mulighed for at håndhæve suverænitet og integritet også i cyberspace. Det giver staterne mulighed for at påpege krænkelser og i sidste ende gribe til individuelt eller kollektivt selvforsvar, hvor den moderne stat er allermest sårbar og truet. På den anden side kan man som småstat frygte, at det er de stærkere magter, der har de bedste offensive og defensive cyberkapabiliteter til rådighed, der her langt mere uhindret end i dag, kan bringe retten til selvforsvar i anvendelse. Med retten til selvforsvar kan disse stater således lovligt gribe dybt ind i cyberspace, hvor de data, der er mål for cyberoperationen, ofte er forbundet snævret med udenforstående civile aktørers data og forbindelser, der risikerer destruktion uden mulighed for indsigelser.

HVEM TILHØRER CYBERSPACE?

Hvis vi kan forestille os, at et væbnet angreb kan finde sted gennem aktiviteter i cyberspace, kan vi altså have en væbnet konflikt i cyberspace. Staternes opfattelse af cyberangreb som en selvstændig del af en væbnet konflikt kan ses i formuleringerne om anvendelsen af krigens loves. F.eks. har den amerikanske regering i 2011 formuleret følgende:

> *"Long-standing international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace´s unique aspects may require clarification in certain areas"*(The White House, 2011, s. 7)

Selv om det er muligt at sidestilles væbnede konflikter i cyberspace med væbnede kinetiske konflikter, opstår der alligevel en række udfordringer med at "oversætte" tidligere juridiske formuleringer til cyberspace. Såfremt vi har et mindre alvorligt cyberangreb som del af en væbnet konflikt, der hovedsageligt foregår i andre domæner, skal der etableres et link til operationen for at krigens love finder anvendelse (Droege, 2012, s. 541). En anden problemstilling er at definere territoriet for væbnede konflikter, hvor krigens love finder sin anvendelse. Man kan tale om, at cyberspace samlet set er et såkaldt "global common" på linje med de internationale farvande, det internationale luftrum og det ydre rum. Men cyberspace består også af en fysisk infrastruktur, der befinder sig på staters territorier, og de aktiviteter, der finder sted i cyberspace, udføres ligeledes af personer fra en fysisk location. Stater har som følge af deres suverænitet autoritet over det, som foregår på territoriet, samt i tilgangen eller afgangen herfra. Dette gælder også alle former for kommunikation, herunder cyberspace (Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, 2013, s. 125). Wolff Heintschel von Heinegg opsummere retstilstanden på følgende vis:

> *"The principle of territorial sovereignty and the enduring right of a State to exercise its territorial jurisdiction applies to cyberspace insofar as the cyberinfrastructure is located within its territory or on platforms over which the State exercises exclusive jurisdiction. Territorial sovereignty and territorial jurisdiction also applies to individuals present in the State and to conduct that either takes place within that territory or produces harmful effects therein. The exercise of jurisdiction under any of the recognized bases of international law is limited only if there exist explicit rules to that effect. Thus, the characteristics of cyberspace do not pose an obstacle to the exercise of territorial sovereignty and jurisdiction; they merely increase the difficulty of doing so"* (Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, 2013, s. 134).

En konsekvens af ovenstående er, at stater ikke bare har rettigheder i cyberspace, som knytter sig til deres territoriale suverænitet. De har også pligter. Herunder den centrale pligt til at sikre, at der ikke sker overgreb eller ødelæggelser i andre stater, som er sat i værk fra deres territorium. Den såkaldte handlepligt (Henriksen, 2014, s. 9). Dette forhold er centralt i relation til cyberangreb og muligheden for at reagere i mod dem, som det vil fremgå af afsnittet om modangreb i cyberspace nedenfor.

Såfremt et angreb har nået tærsklen "an armed attack" i FN´s artikel 51 behøver det ikke at betyde, at man skal modsvare et angreb med tilsvarende midler. Der kan altså svares tilbage i de mere kendte domæner: land, sø og luft. Formålet med retten til selvforsvar, der er be-

grænset til det, som er nødvendigt og proportionalt[1], er at bringe et angreb til ophør og sikre, at et angreb ikke genoptages. Kan man dette med andre og mindre indgribende midler end ved anvendelse af voldsmidler, er det selvfølgelig klart efter kriterierne om nødvendighed og proportionalitet (Schmitt M. N., 2013, s. regel 14, s.61-63). Det kan dog ikke udelukkes, at et modsvar i cyberspace bliver aktuelt, og det vil kræve opbygning af offensive cyberkapabiliteter i de enkelte stater. Parallelt med opbygningen af offensive cyberkapabiliteter er det staternes ansvar, at der sker en afklaring af, hvordan og hvornår en sådan kapabilitet kan bringes til anvendelse.

(MOD)ANGREB MOD HVEM?

Cyberangreb har en række fordele, herunder at de statslige aktører kan skjule sig bag tilsyneladende uafhængige hackergrupper, der måske endda er geografisk placeret i andre stater, og hvis relationer til hinanden og den offensive stat er uklare. Mange videnskabelige artikler har allerede beskæftiget sig med vanskelighederne med attribution af ikke-statslig aktørs handlinger til stater med baggrund i reglerne for statsansvar og de internationale domme, der har været på området(Schmitt & Vihul, 2014,)(Allan, 2013)(Henriksen & Ringsmose, 2014,10). En samlet opsummering af disse analyser betyder, at staterne i de allerfleste situationer ikke vil kunne bevise attribution i tilstrækkeligt omfang. Selv om der er sket en opblødning i de forskellige tests, der skal afgøre attribution til stater, fra den meget krævende "fuld kontrol test" i Nicaragua dommen i 1984 til den noget mindre vidtgående "overall kontrol test" i Tadic dommen i 1999 (Allan, 2013, s. s. 66-69) og så til formuleringerne i Den International Lovkommissions Draft Articles on State Responsibility artikel 4 til 11(International Law Commission, 2001), er kravene stadig meget skrappe. De har til formål, at kunne sidestille den ikke-statslige aktørs handlinger med statens, og herved bringe staten til det fulde ansvar for den ikke-statslige aktørs handlinger. Hvis folkeretten i forholdet til spørgsmålet om attribution ikke udvikler i retning mod at tilgodese stater, der angribes af ikke-statslige aktører, vil staterne søge andre legale løsninger end attribution for at tilgodese deres interesser (Schmitt M. N., 2014, s. 272-274). Når det gælder staters tilknytning til konkrete cyberangreb vil det ifølge von Heinegg måske være nok ud fra langt mere liberale kriterier, bare at bevise, hvorfra cyberangrebet kommer, for herefter at kunne rette krav til den eller de stater, der huser angrebet eller hvis borgere står bag det (Heinegg, 2013, s. 139). En del af den territoriale jurisdiktion er retten til at udøve jurisdiktion over aktiviteter, der ikke udspiller sig på territoriet, men har ødelæggende effekter herpå. Dette betyder, at den angrebne stat på trods af manglende attribution til en anden stat, kan udøve jurisdiktion over individer i andre stater og forlange den anden stats medvirken til opklaring og tilbageholdelse af individer i denne stat, samt til at hjælpe med at afslutte eventuelle aktiviteter, der stadig er i gang (Heinegg, 2012, s. 15). Staten, hvorfra angrebet kommer, skal hjælpe med at bringe angrebet til ophør, til at efterforske hvem, der står bag, samt tilbageholde de individer og beslaglægge de fysiske enheder, hvorfra angrebet

1) Kriterierne om proportionalitet og nødvendighed anses som international sædvaneret og er desuden præciseret ved flere domsafsigelser herunder af Nürnberg Tribunatet og i Nicaragua dommen.

styres. Såfremt staten, hvorfra angrebet pågår, ikke i tilstrækkeligt omfang samarbejder og bringer angrebet til ophør opstår en ny situation:

> *"A state´*s passiveness and indifference towar*ds cyberattacks make it a sanctuary state from where attackers can safely operate. When viewed in this light, a state can be held indirectly responsible for cyberattacks"*(Sklerov, 2009, s. 14).

Yderligere kan vi forestille os situationer, hvor staten, hvorfra angrebet kommer, ikke bare er passiv og ikke samarbejdende, men tilmed anerkender handlingen fra den ikke-statslige aktør. Under visse forudsætninger er det her muligt, at staten kommer til at være direkte ansvarlig for den ikke-statslige aktørs handlinger. Barren for dette er høj, men Den Internationale Domstol har i Tehran Hostage sagen fastslået, at Iran havde ansvaret for at holde amerikanske gidsler. De fik ansvaret på grund af

> *"the approval given by Ayatollah Khomeni and other organs of the Iranian State and the decision to perpetuate them, translated continuing occupation of the Embassy and the detention of the hostages into acts of that State"*(International Court of Justice, 1980, s. para. 74).

For at holde en stat direkte ansvarlig for handlinger udført af ikke-statslige aktører og uden at møde kriterierne i Den International Lovkommissions Draft Articles on State Responsibility artikel 4 til 11, kræver det altså at staten tillader og tilslutter sig den ikke-statlige aktørs handlinger.

Både i tilfælde hvor staten ved eller har vidst, at der foregår handlinger, hvis "scale and effect" svarer til et væbnet angreb eller i tilfælde, hvor staten ikke kan eller vil stoppe et sådant angreb og endelig i tilfælde, hvor staten direkte har anerkendt og tilskyndet til disse handlinger giver det, ifølge de fleste eksperter, mulighed for selvforsvar. Siden 11. september 2001 har statpraksis og *opinio juris* ændret sædvaneretten og fortolkningen af FN-pagtens artikel 51 mod en mere fleksibel fortolkning og retten til selvforsvar mod ikke-statslige aktører, samt de stater, der huser de ikke-statslige aktører (Ruys, 2008, s. 11) (Schmitt & Vihul, 2014, s. 68,69)(Schmitt M. N., 2013, s. rule 13(23))[2]

Hvis man skal finde ud af, hvem de ikke-statslige aktører er, søge at skabe samarbejde med den stat angrebet kom fra, bevise at denne stat er uvillig eller ikke er i stand til at stoppe angrebet, og herefter iværksætte et modangreb, kan meget allerede være gået tabt. Der er imidlertid

2) Både Sikkerhedsrådsresolution 1368 og 1373 efter 11. september 2001 anerkender USAs ret til selvforsvar. Dette blev ligeledes støttet af NATO og OAS. Herudover støttede en majoritet af FNs medlemmer Opreration Enduring Freedom i Afghanistan fra oktober 2001. En helt stribe af eksempler fra statspraksis i andre stater mod andre ikke-statslige aktører har siden vist samme opfattelse af retten til selvforsvar. På den anden side har Den Internationale Domstol i flere domme fastholdt, at retten til selvforsvar handler om væbnede angreb fra en anden stat. Disse domme har dog været præget stor uenighed blandt dommerne. Der er med andre ord ikke enighed om dette spørgsmål (Ruys, 2008, s. 9-10)

flere muligheder for den angrebne stat, mens angrebet pågår. Såfremt den angrebne stat med rimelighed kan forvente, at et pågående angreb vil fortsætte og kan forårsage yderligere ødelæggelser, hvis der ikke iværksættes modforanstaltninger, kan staten igangsætte "a plea of necessity" inden for en række begrænsninger uden at dette fører til brud på internatonal lov. Modforanstaltningerne skal være nødvendige og proportionale og være den eneste mulige vej. Disse modforanstaltninger, der kunne bestå i offensive cyberoperationer, kan dog kun fortsætte indtil angrebet er ovre og ikke længere gør skade. Mulighederne for modforanstaltninger findes beskrevet i Den International Lovkommissions Draft Articles on State Responsibility artikel 25 (International Law Commission, 2001) og i Tallinn Manualen (Schmitt M. N., 2013, s. rule 9 (10-13)).

KONKLUSIONER

En af de mest diskuterede problemstillinger omkring cyberaktiviteter er vanskelighederne med at knytte ansvaret for ikke-statslige aktørers aktiviteter i cyberspace til stater, og herved muliggøre, at disse stater stilles til ansvar. Selvom kravene til attribution af ansvar for ikke-statslige aktørers handlinger til staterne under de gældende regler og deres fortolkning er meget vanskelig, viser dette brief, at angrebne stater faktisk har mange muligheder for at stille stater til ansvar. Det skyldes først og fremmest, at stater ikke bare har rettigheder som følge af deres territoriale suverænitet, men at de også har en række pligter til at gribe ind, hvis aktiviteter på deres territorium eller begået af deres borgere skader andre stater, og de får kendskab hertil. Ligeledes gælder det, at hvis staten ikke kan eller vil hjælpe til at afværge et cyberangreb, kan staten efter udviklingen i statspraksis og *opinio juris* opleve sin territoriale suverænitet kompromitteret af den angrebne stats ret til selvforsvar. Herudover kan den angrebne stat i en række situationer foretage umiddelbare modforanstaltninger mod et cyberangreb, uden at det er ulovligt under international ret.

Tallinn Manualen peger på, at effekterne af et væbnet angreb i cyberspace skal svare til et kinetisk angreb med fysiske ødelæggelser, døde og sårede. Staterne selv er meget vage i deres angivelse af kriterier og peger på, at disse skal vurderes fra case til case eller at effekten af et angreb er "masssere af ødelæggelse". Grundet den øgede betydning af cyberspace for statens generelle funktioner og også dens sikkerhed, må vi forvente at staterne fremover vil vægte ødelæggelser eller længerevarende afbrydelser i cyberspace uden fysiske ødelæggelser til følge, som langt mere alvorlige end man hidtil har gjort.

Briefet peger på en udvikling i statspraksis, der vil øge staters muligheder i forhold til væbnede angreb i cyberspace. Det betyder, at staterne i fremtiden forventeligt vil sænke tærsklen for, hvornår en aktivitet opfattes som at have effekter, der udgør et væbnet angreb. Udvidelsen af forståelsen af "Use of force" kan give stater bedre handlerum til at modsvare destruktion af digitale værdier, infrastruktur og data, men er også en seriøs udfordring for staters beskyttelse mod magtanvendelse, som er hele omdrejningspunktet for artikel 2,4 i FN pagten.

Selvom det umiddelbart kan være fristende, at arbejde for en udvidelse af retten til selvforsvar via en mindre restriktiv fortolkning af begrebet væbnet angreb end det som Tallinn Manualen lægger op til, er det imidlertid væsentligt for en hyperdigitaliseret småstat som Danmark, at vi selv har mest mulig kontrol over vores egen del af cyberspace som en del af vores digitale territorium. Lettes retten til selvforsvar bliver det yderst vanskeligt at modsætte sig territoriale krænkelser digitalt i de tætforbundne netværk. Danmark bør satse på, at øge vores eget cyberforsvar mest muligt samtidig med, at vi fortsat søger at beskytte magtanvendelseforbuddet. Vores suverænitet og integritet er bedst beskyttet ved en snæver tolkning af det væbnede angreb i cyberspace og herved en fortsat vanskelig vej til adgangen til retten til selvforsvar også i Cyberspace.

LITTERATURLISTE

Allan, C. S. (Spring 2013). Attribution Issues in Cyberspace. *Chicargo-Kent-Journal of International and Comrarative Law Vol. 13, Issue 2*.

Boothby, W. (2012). *The Law of Targeting.* Oxford.

Convention on Cybercrime, Budapest (23. November 2001).

Droege, C. (2012). Get off my cloud: cyber warefare, international humanitarian law, and the protection of civilians.vol. 94, number 886. *International review of the Red Cross*.

Heinegg, W. H. (2012). *Legal Implications of Territorial Sovereignty in Cyberspace.* Tallinn: NATO CCD COE Publications.

Heinegg, W. H. (2013). Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies U.S. Naval War College vol. 89*, s. 123-156.

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

Henriksen, A., & Ringsmose, J. (2014,10). *Konflikt i cyberspace? Strategiske og juridiske implikationer.* Dansk Institut for Internationale Studier.

International Court of Justice. (1980). *Tehran Hostage case (US vs. Iran).*

International Court of Justice. (1986). *Military and Paramilitary Activities in and against Nicaragua,Merits, Judgment,.*

International Law Commission. (2001). *Draft Articles on State Responsibility.*

Lewis, J. A. (2015). The Role of Cyber Operations in NATO's Collective Defence. *Tallinn Paper no. 8*.

Lin, H. (15. 6 2016). *NATO's Designation of Cyber as an Operational Domain of Conflict*. Hentet fra Lawfare: https://lawfareblog.com/natos-designation-cyber-operational-domain-conflict

NATO. (5. 9 2014). Hentet fra Wales Summit Declaration: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

Prosecutor vs. Dusko Tadic. (u.d.). *ICTY Appeals Chamber Decision og the Defence Motion for Interlicutory Appeal on Jurisdiction of 2 October 1995.* IT-94-1-A.

Protocol I. (1977). *Protocol Additional to the Geneva Conventions af 12 august 1949, and relation to the Pretection of Victims og International Armed Conflicts.* Geneva.

Redegørelse for den tværministerielle arbejdsgruppe om Folketingets inddragelse ved anvendelse af den militære Computer Network Attack (CNA) - kapacitet, UPN ALM. DEL Bilag 291, FOU Alm. del Bilag 170 (Det Udenrigspolitiske Nævn, Forsvarsudvalget 2015-16).

Regeringen. (2014). *National Strategi for Cyber- og informationssikkerhed - Øget professionaliseing og mere viden.*

Ruys, T. (2008). Quo Vadit Jus Ad Bellum? A Legal Analysis of Tyrkey´s Military Operations Against The PPK in Northern Iraq. *Melboune Journal of International Law 9(2)*.

Sanger, D. (2016). U.S: Wrestles with How to Fight Back Against Cyberattacks, July, 30. *New York Times*.

Schmitt, M. N. (2013). *Tallinn Manual On The International Law Applicable To Cyber Warfare.* New York: Cambridge University Press.

Schmitt, M. N. (2014). The Law of Cyber Warfare: Quo Vadis? *Stanford Law & Policy Review Vol. 25*.

Schmitt, M. N., & Vihul, L. (Spring 2014,). Proxy Wars in Cyberspace: The Evolving International Law of Attribution. *Fletcher Security Review Vol 1, Issue 2*.

Sklerov, M. J. (2009). *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use og Active Defenses against States Who Neglect Their Duty to Prevent.* 57th Judge Advocate Officer Graduate Course, United States Navy.

The White House. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Opennes in a Networked World* .

Valeriano, B., & Maness, R. (2015). *Cyber War versus Cyber Realities - Cyber Conflict in the International System.* Oxford University Press.