DIIS REPORT

DIIS REPORT

Anders Henriksen og Jens Ringsmose

Konflikt i cyberspace?
Strategiske og juridiske implikationer

DIIS Report 2014:10

DIIS · DANSK INSTITUT FOR INTERNATIONALE STUDIER

DIIS • Dansk Institut for Internationale Studier
Østbanegade 117, 2100 København Ø
Tlf: 32 69 87 87
E-mail: diis@diis.dk
Web: www.diis.dk

Layout: Allan Lind Jørgensen
Tryk: Vesterkopi A/S

ISBN:
Print: 978-87-7605-683-4
Pdf: 978-87-7605-684-1

Pris: 50.00 kr. inkl. moms
Trykte eksemplarer kan bestilles på publications@diis.dk
DIIS' publikationer kan downloades gratis på www.diis.dk

Anders Henriksen, forsker, Center for International Law and Justice, Københavns Universitet
anders.henriksen@jur.ku,dk

Jens Ringsmose, forsker, Institut for Statskundskab, Syddansk Universitet
jri@sam.sdu,dk

Indhold

Resumé

De seneste års hastige udbredelse af avanceret informations- og kommunikationsteknologi har skabt øget velfærd samt faciliteret udvekslingen af ideer på tværs af nationale skel. Den tiltagende "forbundethed" har imidlertid også ført til en forøget sårbarhed. I takt med at stadig større dele af vores økonomiske, sociale, forvaltningsmæssige og militære aktiviteter er forankret i cyberspace øges også risikoen for, at fjendtligtsindede cyberaktiviteter kan får betydelige negative konsekvenser.

Nærværende rapport sætter fokus på den del af de fjendtligsindede cyberaktiviteter, som er *politisk* motiverede. Konkret zoomer rapporten ind på tre dimensioner: En konceptuel (hvad er et cyberangreb og hvornår – hvis overhovedet – giver det mening at tale om cyberkrig?), en strategisk (hvordan påvirker fremkomsten og udbredelsen af cyber-våben politisk vold og moderne væbnet konflikt i en strategisk henseende?) og en juridisk (hvordan udfordrer politiske aktørers anvendelse af cyberspace de traditionelle retlige begreber, såsom spionage, suverænitetskrænkelse, magt og væbnet angreb?). Rapportens struktur tager afsæt i de tre dimensioner.

Rapportens gennemløbende hovedargument er, at den eksisterende (og endnu temmelig umodne) videnskabelige debat om konflikt i cyberspace i for høj grad har været præget af dommedagsprofetier og "worst case" scenarier. Cybertruslen skal tages alvorligt, men den megen snak om krig og væbnet konflikt i cyberspace har ført til en unødig og til tider uhensigtsmæssig "militarisering" af debatten om cybersikkerhed. I en strategisk henseende er der en del, som tyder på, at cyberspace vil blive et offensiv-dominant domæne. Samtidig peger en række forhold imidlertid også i retning, at denne tendens ikke skal overdrives. I en juridisk henseende ...

Executive summary

The proliferation of advanced information and communication technology has not only enhanced welfare and facilitated the exchange of ideas across national boundaries, but also led to an increasing vulnerability. As more and more of our economy, social, administrative and military activities are conducted through cyberspace, the risk of hostile and potentially harmful cyber activities increases.

This report focuses on *politically* motivated hostile cyber-activities. Specifically, the report looks at three dimensions: A conceptual (what is a cyberattack and when – if ever – does it make sense to talk about cyberwar?), a strategic (how does the emergence and proliferation of "cyberweapons" affect political violence and modern armed conflicts in a strategic sense?), and a legal (how does political actors' use of cyberspace challenge the traditional legal concepts and categories, such as espionage, violation of sovereignty, force and armed attacks?).

The main argument of the report is that the scientific debate about conflicts in cyberspace has so far been dominated by worst-case scenarios. The threats in cyberspace are real and should be taken seriously but all the talk about "cyberwar" has led to an unnecessary and, at times, undesirable "militarization" of the debate on cybersecurity. From a strategic point of view, although cyberspace to a certain extent can be considered an offensive-dominant domain, a number of factors point in the opposite direction. From the point of view of international law, there is still a need for a fundamental – primarily politically driven – clarification of how hostile cyber activities should be classified according to the existing legal categories and, thus, also addressed.

Indledning

De seneste par årtiers eksplosionsagtige udvikling og udbredelse af avanceret informations- og kommunikationsteknologi har haft dramatiske og – helt overvejende – positive følger. Ikke mindst introduktionen og spredningen af internettet samt den deraf følgende "globale forbundethed" har ført til effektiviseringer, vidensdeling, økonomisk vækst, en mere effektfuld brug af væbnet magt samt fremkomsten og styrkelsen af sociale fællesskaber på tværs af nationale grænser (se fx Manyika & Roxburgh 2011; UK MOD 2011). Dertil kommer, at udbredelsen af Internettet har gjort det vanskeligere for autoritære regimer at opretholde et informationsmonopol, hvilket igen har ført til styrkelsen af nationale demokratiseringsprocesser i flere lande (Shirky 2011; Sifry 2011; Betz 2012; Steen-Johnsen, Enjolras & Wollebæk 2013). I en bred forstand har den teknologidrevne udvikling dermed i stort omfang bidraget til det, der med en samlebetegnelse kan beskrives som velfærdsforbedringer.

Udbredelsen og den voksende afhængighed af internettet har imidlertid også resulteret i en øget sårbarhed. I takt med at stadig større dele af vores økonomiske, sociale, forvaltningsmæssige og militære aktiviteter foregår i cyberspace, vokser nemlig også risikoen for, at fjendtligsindede cyberaktiviteter kan få betydelige, negative konsekvenser. Også kriminelle og uvenskabelige politiske aktører har således fået mulighed for at (mis)bruge eller ødelægge den selvsamme informations- og kommunikationsteknologi, som i stigende omfang faciliterer vores generelle velfærd (Lauta m.fl. 2013). I modsætning til de fleste traditionelle trusler mod vor velfærd og sikkerhed, er cybertrusler imidlertid snævert knyttet til angreb i en digital virkelighed. Kun i meget sjældne tilfælde – og kun indirekte – kan cyberangreb føre til ødelæggelser og blodsudgydelser i den fysiske verden.

I sin seneste trusselsvurdering anslår Forsvarets Efterretningstjenestes nyligt oprettede Center for Cybersikkerhed, at "kritisk infrastruktur i Danmark er et potentielt vigtigt strategisk mål for fremmede stater og ikke-statslige aktører", og at antallet "af angrebsmål vil stige i takt med, at flere og flere styrings- og kontrolkomponenter i infrastrukturen opkobles til internettet." Ifølge Forsvarets Efterretningstjeneste har der da også i de seneste år været "cyberangreb mod væsentlige mål i Danmark, hvor informationssikkerheden er blevet kompromitteret", og i 2013 var der cyberangreb, som i en kortere periode forstyrrede eller hindrede "anvendelsen af dansk it- og teleinfrastruktur." Ifølge tjenesten er det "meget sand-

synligt at disse tendenser vil fortsætte" (Forsvarets Efterretningstjeneste 2013:9; se også Kjær 2013; Poulsen 2013). Den vurdering deles tilsyneladende af en stor gruppe danske embedsmænd, forskere, meningsdannere og politikere "med særlig viden, indsigt og erfaring på det udenrigs- og sikkerhedspolitiske område" (Center for Militære Studier 2013:9). I en spørgeskemaundersøgelse gennemført af Center for Militære Studier i 2013 anslog de sikkerhedspolitiske eksperter således, at et potentielt cyberangreb aktuelt udgør den største trussel mod dansk sikkerhed (Center for Militære Studier 2013:21).

Ikke overraskende har den forøgede sårbarhed overfor forskellige typer af offensive cyberoperationer – samt en række faktisk gennemførte angreb mod stater og virksomheder – fået adskillige politikere og eksperter til at råbe vagt i gevær. Eksempelvis advarede den tidligere amerikanske forsvarsminister, Leon Panetta, i oktober 2012 om et kommende "cyber-Pearl Harbor" (Bumiller & Shanker 2012), mens Richard Clarke, der fungerede som "cybersikkerhedspolitisk zar" i Bush-administrationen, i 2010 forudsagde, at et kommende cyber-angreb mod USA meget vel kunne få større konsekvenser end terrorangrebet mod New York og Washington den 11. september 2001 (Clarke & Knake 2010; se også Lynn 2010). I Danmark har flere eksperter og militære analytikere ligeledes advaret mod den tiltagende sårbarhed overfor cyberkriminalitet og politisk motiveret aggression i cyberspace (se fx Kjær 2013; Poulsen 2013). I maj 2012 udtalte daværende forsvarsminister Nick Hækkerup, at "cyberkrig er en ny dimension, som er potentielt lige så farlig som truslerne under den kolde krig" (Brøndum 2012).

På trods af det stærkt forøgede politiske og mediemæssige fokus på cybertrusler er hverken forskningens eller offentlighedens forståelse af cyberdomænet imidlertid endnu særlig dyb. Forskellige videnskabelige discipliner arbejder stadig på at begrebsliggøre og teoretisere det spirende og meget komplekse felt, mens den offentlige debat i høj grad har været domineret af dommedagsprofetier og sensationelle indgangsvinkler til emnet.

Ambitionen med nærværende rapport er frem for alt at informere og kvalificere den offentlige danske debat om brugen af cyber-instrumenter til forfølgelse af *politiske målsætninger*. Det vil også sige, at fokus i rapporten er på det, man kan betegne som "cyberkonflikt" og *politiske aktørers* instrumentelle anvendelse af cyber-relaterede midler til fremme af *politiske målsætninger*. Rapporten beskæftiger sig med andre ord kun i meget begrænset omfang med de cybertrusler, der entydigt kan karakteriseres som enten kriminelle handlinger eller hærværk. I den forstand omhandler de følgen-

de sider kun en lille – men meget væsentlig – del af alle tænkelige fjendtligsindede aktiviteter i cyberspace. Rapporten fokuserer navnlig på de strategiske og juridiske udfordringer og muligheder, fremkomsten af cybervåben skaber.

Konkret retter vi fokus mod tre dimensioner og tre forskellige typer af spørgsmål:

- *Konceptuelt*: Hvordan kan brugen af cyber-instrumenter til fremme af politiske målsætninger begrebsliggøres? Hvad er relevansen af eksisterende kategorier og begreber indenfor studiet af politisk vold, herunder væbnet konflikt? Hvilke typer af cyber-angreb giver det mening at tale om? Hvornår – om overhovedet – kan et cyber-angreb kategoriseres som egentlig krig?
- *Strategisk*: Hvordan påvirker fremkomsten af cyber-våben politisk vold og moderne væbnet konflikt i strategisk henseende? Vil udviklingen af stadig mere avancerede cyber-våben føre til en forøget risiko for krig og væbnet konflikt? Er det sandsynligt, at nye it-baserede våbentyper vil styrke ikke-statslige aktører? Og i hvilket omfang er det muligt at afskrække fjendtlige aktører fra at bruge cybervåben?
- *Legalt*: Hvordan udfordrer politiske aktørers anvendelse af cyberspace de traditionelle retlige begreber, såsom spionage, suverænitetskrænkelse, magt og væbnet angreb, der ligger til grund for den folkeretlige regulering af, hvorledes stater må forfølge deres interesser i det internationale rum? Og hvad betyder det for folkeretten, at det i praksis ofte er noget nær umuligt at identificere den aktør, der står bag et cyber-angreb?

Rapportens gennemløbende hovedargument er, at den eksisterende (og endnu temmelig umodne) videnskabelige debat om konflikt i cyberspace i for høj grad har været præget af dommedagsprofetier og "worst case"-scenarier. Cybertruslen er seriøs og den skal tages alvorligt, men den megen snak om krig og væbnet konflikt i cyberspace har ført til en unødig og til tider uhensigtsmæssig "militarisering" af debatten om cybersikkerhed.

Rapporten er opdelt i tre hoveddele: I første del sætter vi cyberkonflikt i relief. Vi sammenligner således konflikt i cyberspace med konflikt i andre domæner og indkredser det særlige ved konflikt i cyberdomænet. Anden hoveddel rummer først og fremmest en analyse og en diskussion af de væsentligste strategiske debatter vedrørende brugen af cyberinstrumenter i konflikt. Og tredje hoveddel er viet en analyse af to af de mest presserende folkeretlige spørgsmål, der knytter sig til cyberspace som konfliktdomæne. Rapporten rundes af med en kort konklusion og en række

perspektiverende bemærkninger om nogle af de udfordringer, som fremkomsten af de nye trusler fra cyberspace rejser for bl.a. Danmark.

Hvad er cyberkonflikt?

Som kort beskrevet i indledningen er den eksisterende sikkerhedspolitiske og folkeretlige forskning i konflikt i cyberspace endnu forholdsvis umoden. Mange centrale aspekter er kun kursorisk analyseret i litteraturen, og i modsætning til mere etablerede forskningsfelter, har der kun i mindre udstrækning udkrystalliseret sig en række klare teoretiske positioner.[1] Det hænger selvfølgelig i høj grad sammen med, at genstandsfeltet – konflikt i cyberspace – (formentlig) endnu er i sin vorden. Som pointeret af den sikkerhedspolitiske forsker, David Betz, så er vor tids cyberangreb (som eksempelvis Stuxnet og angrebet på Estland i 2007 – se mere herom senere), mest at sammenligne med 1. Verdenskrigs Zeppelin-bombeangreb på Storbritannien: I sig selv har de haft en meget beskeden effekt, men de udgør en vigtig påmindelse om, hvad fremtiden kan bringe (Betz 2012:694-5). I det følgende sætter vi fokus på, hvordan konflikt i cyberspace hidtil er forsøgt begrebsliggjort, og ser på de vanskeligheder, der er forbundet med at anvende vores traditionelle kategorier på konflikt i cyberspace.

Cyberkonflikt adskiller sig først og fremmest fra andre typer af konflikter ved at finde sted i et helt igennem menneskeskabt domæne: *cyberspace*. I modsætning til andre konfliktdomæner (land, vand, luft og rummet), er cyberspace i stort omfang et virtuelt eller elektronisk domæne, hvori mennesker og maskiner kommunikerer og interagerer med hinanden. I den militære litteratur betegnes cyberspace ofte som "det femte domæne". Cyberspace er således et informationsmiljø, der er karakteriseret ved brugen af elektronik og det elektromagnetiske spektrum med henblik på at "create, store, modify, exchange, and exploit information via inter-connected information and communication technology-based systems and their associated infra-structure" (Kuehl 2009:28). *Cyberkonflikt* adskiller sig dermed også fra andre former for konflikt ved udelukkende at blive ført med ikke-kinetiske midler. Ganske vist kan cyberoperationer have fysiske/kinetiske effekter, men for at kvalificere som et cyberangreb, må en given aggression benytte sig af det virtuelle domæne (se fx Liff 2012:404).

Blandt såvel praktikere som forskere er der langtfra enighed om, hvordan cyberspace skal defineres, men flere abonnerer på Martin Libicki's beskrivelse af cyberspace som et rum bestående af tre lag: et fysisk lag, et syntaktisk lag og et semantisk lag. Det *fysiske*

[1] For forsøg på at kategorisere den eksisterende forskning, se Eriksson & Giacomello (2006); Gartzke (2013); Kello (2013); Langø, (2013a; 2013b).

lag omfatter computere, routere, fiberledninger, skærme, kabler etc. Det *syntaktiske* lag rummer software samt de instruktioner, som programdesignere og brugere giver en given computer. Det er også i det syntaktiske lag, at de protokoller, der muliggør, at en given computer kan interagere med andre computere, findes. Ofte er det i dette lag, at hackere forsøger at opnå kontrol med de instruktioner, som programdesignere og brugere har tildelt computeren. Endelig rummer det øverste *semantiske* lag den information (kodet i naturlige sprog), der er relevant for brugeren. Det semantiske lag udgør herved en form for bro mellem menneske og maskine (Libicki 2007:1-72; se også Libicki 2009:11-3; Tabansky 2011; Schreier 2012:10-14; Betz 2012:691-2). I forskningen er der i øvrigt almindelig enighed om, at cyberspace er mere end blot internettet. Det omfatter ligeledes de netværk – private som offentlige – der ikke er koblet på internettet. Som koncist beskrevet af Fred Schreier:"Thus, cyberspace includes the Internet *plus* lots of other networks of computers, including those that are not supposed to be accessible from the Internet" (2012:10).[2]

Der er endnu ikke helt ensartethed i terminologien over fjendtligsindede offensive aktiviteter i cyberspace, men de forskellige handlinger inddeles ikke desto mindre ofte i tre overordnede kategorier: "cyberkriminalitet", "cyberspionage" og egentlige "cyberangreb" (se fx Arquilla & Ronfeldt 1993; Kello 2013; Schreier 2012; Liff 2012).[3] I virkelighedens verden kan det dog fra tid til anden være vanskeligt at bestemme præcis, hvilken af kategorierne en bestemt fjendtligsindet aktivitet passer ind i. Det skyldes dels, at en given cyberoperation kan befinde sig i spændingsfeltet mellem eksempelvis cyberspionage og cyberkriminalitet, og dels, at det kan være vanskeligt at bestemme intentionerne bag operationen. Et forhold vi kommer tilbage til senere i rapporten. Det ændrer imidlertid ikke ved, at typologien tjener som et udmærket begrebsligt afsæt for en dybere forståelse af feltet.

Cyberkriminalitet adskiller sig grundlæggende fra de to øvrige kategorier ved at være handlinger, der ikke umiddelbart er motiveret af politiske målsætninger. Det kan fx dreje sig om berigelseskriminalitet (kreditkortsvindel på Internettet, manipulation med bankkontodata etc.), identitetstyveri, traditionel industrispionage eller udveksling af børnepornografisk billedmateriale. Til denne kategori hører også hacking begået af personer, som alene er motiveret af spænding eller ønsket om at opnå prestige.

[2] For andre definitioner, se Clarke & Knake (2010:69); German Federal Ministry of the Interior (2011:14); UK MOD 2011:11).

[3] På engelsk: "cybercrime", "cyberexploitation"/"computer network exploitation" og "cyberattack/computer network attack".

Cyberspionage refererer til politisk motiveret indtrængning i andre staters eller ikke-statslige aktørers computernetværk med henblik på at få adgang til informationer. I modsætning til regulære cyberangreb (se nedenfor) kræver succesfuld cyberspionage ikke manipulering med informationer eller data. Ofte vil succes tværtimod afhænge af en så usynlig digital tilstedeværelse som mulig. Som beskrevet af Kello: "Essentially an intelligence-gathering activity, cyberexploitation relies on stealth and undetectability; thus disruption of the host system, which can lead to discovery and closure of access, defeats the purpose of exploitation" (2013:20). Den amerikanske efterretningstjeneste, National Security Agency's, aflytning af forbundskansler Angela Merkels mobiltelefon samt kinesisk statssponsoreret spionage rettet mod Lockheed Martins Joint Strike Fighter-projekt hører til denne kategori af offensive cyberoperationer.

Regulære *cyberangreb* er de fjendtligsindede aktiviteter i cyberspace, der er politisk og/eller strategisk motiverede, og som tager sigte mod at ødelægge, manipulere eller nægte adgangen til information lagret på en anden aktørs computere eller computernetværk.[4] 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. I sådanne tilfælde bliver civil infrastruktur (i en bred forstand) anvendt som våben. Det vil herved ikke være cybervåbenet (softwarekoden) som sådan, der dræber eller har en kinetisk effekt, men derimod den fysiske struktur, der kontrolleres af den angrebne computer eller det angrebne computernetværk (Lewis 2010). En særlig kategori af cyberangreb udgøres af forsøg på at overtage styringen med et eller flere af modstanderens netværksforbundne militære våbensystemer (Alford 2010).

Et bemærkelsesværdigt kendetegn ved de "våben" og "cyberinstrumenter", der anvendes i forbindelse med forskellige former for fjendtligsindede aktiviteter i cyberspace, er, at de meget ofte kun kan anvendes én gang. Der er så at sige tit tale om "engangsvåben". Det hænger sammen med, at den angrebne part i reglen vil få kendskab til den sikkerhedsbrist, som muliggjorde angrebet i første omgang, samt til det anvendte "cybervåbens" særlige digitale signatur. Dermed bliver det ofte også forholdsvis let at forsvare sig mod en gentagen brug af samme våben (Trias & Bell 2010). Det betyder

[4] Kello definerer cyberattack på følgende vis: "Cyberattack refers to the use of code to interfere with functionality of a computer system for political or strategic purpose (2013:19).

endvidere, at en potentiel angriber har god grund til nøje at overveje, om tidspunktet for brugen af et givent cybervåben er det helt rigtige. Anvender man våbnet, kan det nemlig meget vel være ensbetydende med, at man også mister det (se fx Lewis 2010:4).[5]

Reelt set er det en ekstremt lille del af de faktisk gennemførte og fjendtligsindede cyberaktiviteter, der på nogen rimelig måde lader sig kategorisere som "cyberkrig". For det første er det alene politisk motiverede cyberangreb (men langt fra alle politisk motiverede cyberangreb), der i sig selv kan have karakter af at udgøre en egentlig krigshandling (se fx Lindsay 2013). Eksempelvis er én stats cyberspionage mod en anden stat ikke (isoleret betragtet) at anse for en krigshandling. For det andet er de mange forsøg på indtrængning og industrispionage, som blandt andet danske myndigheder og virksomheder dagligt udsættes for, med al sandsynlighed og i helt overvejende omfang foretaget af private hackere, som enten håber på en økonomisk gevinst ved at få adgang til "industrielle hemmeligheder" eller blot ønsker at bevise deres tekniske kunnen (McGraw 2013).[6] Selvom disse angreb udgør en sikkerhedsmæssig udfordring, kvalificerer størstedelen af aktiviteterne ikke som meget andet end "cyber-irritationsmomenter".[7] Det hører dog med til historien, at det i praksis kan være vanskeligt at trække en klar grænse mellem henholdsvis politisk motiveret cyberspionage og den form for cyberkriminalitet, der består i økonomisk betinget industrispionage.

En anderledes måde at kategorisere de forskellige typer af fjendtligsindede cyberaktiviteter på tager sit afsæt i to centrale dimensioner: Intentionen bag handlingen samt handlingens effekt (se figur 1 nedenfor). I forhold til *intention* kan en aggressiv cyberaktivitet groft sagt enten være politisk motiveret eller kriminel.[8] *Effekten* af en fjendtligsindet aktivitet i cyberspace kan 1) begrænse sig til at ramme informationer og software i en eller flere computere eller computernetværk; 2) forvolde skader på og ødelægge "døde ting" som fx fysisk infrastruktur og militære installationer (via manipulation af information og software); 3) være voldelige og resultere i person-

[5] For en analyse og diskussion af hvilken rolle timing spiller i forbindelse brugen af cybervåben, se Robert Axelrod & Rumen Iliev (2014). En paradoksal konsekvens af, at cybervåben ofte kun kan anvendes én gang, er, at fjendtligtsindede aktører har et incitament til hurtigt at gøre brug af et givent cybervåben mod en aktør, der er god til at finde og lukke sikkerhedshuller. Modsat: Investerer en stat meget lidt i cybersikkerhed, vil sårbarheder bestå, og den fjendtligtsindede aktør vil med ro i sjælen kunne vente på det helt rigtige tidspunkt for anvendelsen af sit våben (Schreier 2012:99f; Nuzzo 2014).

[6] Forsvarets Efterretningstjeneste vurderede i 2013, at det ikke er sandsynligt, at Danmark i et tiårigt perspektiv vil blive ramt af et omfattende, statssponsoreret cyberangreb (2013:9).

[7] Interview med James Lewis, Center for Strategic and International Studies, September 2013.

[8] I virkelighedens verden vil der selvsagt være typer af aktiviteter, der er både kriminelle og politisk motiverede, ligesom der vil være typer af fjendtligtsindede aktiviteter, der befinder sig i en gråzone mellem de to kategorier. Endelig er det også værd at bemærke, at den aktør, som den fjendtlige aktivitet er rettet imod, sjældent har mulighed for rent faktisk at afgøre, hvilken kategori aktiviteten hører til.

Figur 1. Typologi over forskellige cyberangreb

	Kriminalitet	*Politisk motiveret angreb*
Ingen umiddelbare fysiske effekter	• Industrispionage • Identitetstyveri • Internetsvindel • Phishing	• Spionage • DDoS-angreb[9] (Estland 2007) • Manipulation af bankdata • Ødelæggelse af dataregistre
Fysiske (midlertidige og/eller permanente) skader på bygninger, infrastruktur, militære installationer etc.	• Manipulation med virksomheders kontrol- og styringssystemer (SCADA)[10] • Hærværk	• Lammelse af radaranlæg og våbensystemer (Operation Orchard) • Ødelæggelse af nukleare reaktorer (fx Stuxnet/ Operation Olympic Games) • Strømafbrydelse
Personskade (døde og/eller sårede)	• Cybermord og lign.	• Afsporing af tog • Hacking og anvendelse af våbensystemer mod egne styrker eller civilbefolkning • Dæmningsbrud

skade og/eller tab af menneskeliv. I litteraturen fremhæves det ofte, at 1) udelukkende dækker over *direkte effekter*, mens 2) og 3) har *indirekte effekter*, der rækker udover cyberspace (Kello 2013:19).

Betragtet gennem ovenstående typologi bliver det tydeligt, at jo mere man nærmer sig figurens sydøstlige hjørne, i jo højere grad giver det mening at tale om egentlige krigshandlinger. Jo mere voldeligt og politisk motiveret et cyberangreb er, jo mere relevant bliver det at bruge prædikatet krig. Enkelte forskere og kommentatorer

[9] Distributed Denial of Service-angreb

[10] SCADA – "Supervisory Control and Data Acquisition". Angreb på kontrol- og styringssystemer kan også være politisk motiverede.

(især de såkaldte "skeptikere/traditionalister") har imidlertid argumenteret for, at cyberangreb med al sandsynlighed aldrig for alvor vil få en karakter, der berettiger til en indplacering i figurens sydøstligste hjørne. Under alle omstændigheder er vurderingerne af truslen fra cyberspace temmelig overdrevne, lyder det fra denne gruppe.[11] Thomas Rid – der er forfatter til bogen *Cyber War will Not Take Place* – har eksempelvis argumenteret for, at krig nødvendigvis må være politisk, instrumentel og voldelig, og da cyberangreb aldrig har ført til sårede eller dræbte (og ifølge Rid sandsynligvis heller ikke kommer til det), kan aggressioner i cyberspace per definition ikke have karakter af egentlig "krig" (Rid 2012; 2013).

Selvom Rid og hans ligesindede kan have en pointe i, at debatten om cyberkonflikt fra tid til anden kan virke en smule skinger – og at der er betydelige risici forbundet med at overdrive truslen fra cyberspace – fremstår deres kontante afvisning af at tale om krig og krigshandlinger i cyberspace en anelse radikal. For det første kan det virke uhensigtsmæssigt, at begrænse kategorien "krigshandlinger" til aktiviteter, som fører til sårede og/eller dræbte[12], og man kan spørge, om ikke et massivt luftbombardement rettet mod en stats infrastruktur eller andre fysiske installationer, såsom radarstationer og lignende, der har til formål at beskytte staten, vil kvalificere som "krigshandlinger" – også selv om ingen personer såres eller slås ihjel. Det samme kunne gøre sig gældende, når angrebet gennemføres med cybervåben. Skulle det eksempelvis lykkes stat A at gøre stat B's nukleare arsenal ubrugeligt via anvendelsen af malware eller andre cyberinstrumenter, kan det som minimum diskuteres, om der ikke er tale om en egentlig krigshandling. Selvom om midlerne er forskellige, kan konsekvenserne være de samme (Stone 2013). Det er også værd at bemærke, at et cyberangreb kan nå at strække sig over ganske lang tid, inden det opdages og bringes til ophør, og at virkningerne af angrebet – selvom de måske er mindre spektakulære end ved et konventionelt angreb – derfor kan nå et ganske voldsomt omfang.

For det andet overser en række af skeptikerne, at et cyberangrebs *intensitet* kan have et omfang, der muligvis kan retfærdiggøre brugen af begrebet "krig" – på trods af,

[11] Til skeptikerne/traditionalisterne hører blandt andre Jean-Loup Samaan (2010), Jerry Brito & Tate Watkins (2011), Tim Maurer (2011), Thomas Rid (2012; 2013), Stephen M. Walt (2010), Jon R. Lindsay (2013) og Erik Gartzke (2013).

[12] Rid baserer sin definition af krig på en meget snæver læsning af Clausewitz (Rid 2013:1). At krig ifølge Clausewitz er "an act of force to compel the enemy to do our will" fortolker Rid således, som om "[a]ll war, pretty simply, is violent" (2013:1). Spørgsmålet er imidlertid, om ikke "an act of force" også kan være anvendelsen af fysisk magt – eller af ikke-fysiske instrumenter – uden at det nødvendigvis resulterer i vold mod mennesker (se også Gray 2005:293-4; Langø 2013a:23-26; Stone 2013). Eller som formuleret af Gregory J. Rattray:"... the achievement of political objectives may not require the actual use of violent means. The use of non-violent digital attacks to achieve political objectives must be understood as part of a new form of warfare" (2001:20).

at der måske ikke engang er sket skade på fysiske strukturer. I den optik er det muligt, at selv et angreb, der ingen indirekte (fysiske) effekter har, udgør en krigshandling – blot de politiske, sociale og/eller økonomiske konsekvenser er store nok. Det vil fx være tilfældet, hvis stat A har held til at slette samtlige bankdata i stat B. De økonomiske, sociale og muligvis også politiske konsekvenser af et sådant angreb er potentielt set enorme. På trods af at aggressionen set igennem ovenstående typologi ikke rækker udover et type 1)-angreb, er det bestemt ikke muligt klart og entydigt at afvise, at der skulle være tale om en krigshandling. Under alle omstændigheder er det sandsynligt, at den angrebne stat vil opfatte det som en krigshandling.

Et særligt karakteristikum ved politisk motiverede angreb i cyberspace er, at de meget ofte vil finde sted i en form for ingenmandsland mellem vores traditionelle opfattelser og konceptualiseringer af krig og fred. I international politik har der altid eksisteret et rum mellem på den ene side almindelige fredelige, diplomatiske og økonomiske relationer imellem systemets aktører og på den anden side kategorien "væbnet konflikt". Det er eksempelvis i dette spændingsfelt, at stater og andre politiske aktører i århundreder har udspioneret, bestjålet, saboteret og propaganderet imod hinanden. Det er også i dette rum, at stater har benyttet sig af handelssanktioner og embargoer. Fordi cyberangreb kun i meget sjældne tilfælde vil resultere i døde og sårede, rimer offensive aktiviteter i cyberspace kun dårligt med vores traditionelle forståelse af krig. På den anden side er der entydigt heller ikke tale om almindelige, fredelige relationer.

I sidste ende vil forskellige former for konflikt i cyberdomænet derfor ofte skulle henføres til et sted i rummet mellem krig og fred, hvilket udfordrer de politiske beslutningstageres muligheder for at svare igen på sådanne angreb. Som formuleret af Lucas Kello: "...because cyberweapons are not overtly violent, their use is unlikely to fit the traditional criterion for interstate war; rather, the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace – with important consequences for national and international security" (2013:7).

Som det fremgår af ovenstående kan det være endog meget vanskeligt at afgøre, hvorvidt en fjendtlig aktivitet i cyberspace udgør en krigshandling eller ej. Dels passer brugen af cybervåben kun i et meget begrænset omfang til vores traditionelle kategorier, og dels kan det være særdeles besværligt at bestemme de reelle effekter af – samt intentioner bag – et givent cyberangreb.[13] Det betyder, at de eksisterende kategorier

[13] Med til at gøre det vanskeligt at bestemme de reelle effekter af et cyberangreb er, at de ofte vil have ikke-linære kaskadeeffekter. Det betyder også, at den der udfører angrebet, kan have vanskeligt ved på forhånd at bestemme effekten af angrebet.

og distinktioner, som vi normalt anvender i forsøget på at forstå og begrebsliggøre krig og væbnet konflikt, bliver udfordrede. Vi vender senere i rapporten tilbage til de folkeretlige problemer, som det fører med sig.

Cyberkonfliktens strategiske dimension

Helt som man kunne forvente, har fremkomsten og den pågående spredning af cybervåben givet anledning til mange overvejelser og debatter om, hvordan de strategiske relationer mellem såvel stater som ikke-statslige aktører bliver påvirket af muligheden for at føre konflikt i cyberspace. Det følgende afsnit er et forsøg på at give et overblik over de væsentligste positioner og stridspunkter i diskussionerne. Givet feltets kompleksitet og generelt flydende karakter samt den allerede omfattende litteratur om cyberkonfliktens strategiske dimension kan der i sagens natur kun blive tale om et relativt overfladisk signalement.

Udgangspunktet for præsentationen og analysen af den aktuelle debat er tre hyppigt fremførte påstande om de strategiske effekter af udviklingen og spredningen af cybervåben.[14] Det drejer sig henholdsvis om påstanden om

- At angriberen har en grundlæggende fordel i cyberspace, fordi cyberforsvar er dyrt og vanskeligt, mens cyberangreb er billigt og let;
- At det er vanskeligt – hvis ikke umuligt – at afskrække i cyberspace, fordi det er svært – hvis ikke umuligt – at identificere en angriber (det såkaldte "attributionsproblem");
- At udviklingen og spredningen af cybervåben i relativ forstand styrker en række konventionelt betragtet svage aktører, fordi cybervåben er billige og lover anonymitet.

I det følgende diskuterer vi de tre teser, og afsnittets gennemløbende argument er, at de alle har noget for sig, men at der også er en række forhold, der taler imod deres holdbarhed.

Cyberspace er et "offensivt domæne"

Den vel nok hyppigst gentagne og mest konsoliderede strategiske forestilling om konflikt i cyberspace er, at det er let at angribe og svært at forsvare sig i det såkaldte "femte domæne" (se fx Arquilla & Ronfeldt 1996; Clarke & Knake 2010; Lynn 2010; Department of Defence 2011; Liff 2012; Lieberthal & Singer 2012; Junio 2013I;

[14] De tre påstande (eller hypoteser) om cyberdomænets strategiske beskaffenhed kom blandt andet klart til udtryk da den amerikanske vice-forsvarsminister, William J. Lynn III, i 2010 præsenterede grundelementerne i den amerikanske cybersikkerhedsstrategi i tidskriftet *Foreign Affairs* (Lynn 2010).

Kello 2013; Lindsay 2013; McGraw 2013; Singer & Friedman 2014). Det er i høj grad også denne forestilling, der har givet anledning til mest pessimisme blandt en stor del af de forskere med tilknytning til den videnskabelige disciplin "strategiske studier", som har beskæftiget sig med cyberkonflikt. Det hænger frem for alt sammen med en grundlæggende forventning om, at det øger sandsynligheden for væbnet konflikt, når offensive våben dominerer. Alt andet lige vil risikoen ved et væbnet angreb således være større, når offensive våben er de defensive våben overlegne. Eller anderledes formuleret: Risikoen for væbnet konflikt vokser, når aggression betaler sig.[15]

Forskere og praktikere har især peget på to grupper af faktorer, som bidrager til at tilte balancen i cyberspace i retning af de offensive instrumenter. Det fremhæves for det første ofte, at cyberforsvar af strukturelle årsager er teknisk vanskeligt, mens mulighederne for at udnytte forskellige netværks svagheder er enorme og relativt billige. Cyberspace er derfor i høj grad det, der i den militær-strategiske litteratur betegnes som et "target rich environment". Forsvareren har mange aktiver at forsvare, mens angriberen i ro og mag kan udvælge sig ét bestemt mål. Som William J. Lynn beskriver:

> In cyberspace, the offense has the upper hand. The Internet was designed to be collaborative and rapidly expandable and to have low barriers to technological innovation; security and identity management were lower priorities. For these structural reasons, the U.S. government's ability to defend its networks always lags behind its adversaries' ability to exploit U.S. networks weaknesses. Adept programmers will find vulnerabilities and overcome security measures put in place to prevent intrusions (Lynn 2010:99).

For det andet har flere forskere peget på, at den ekstreme hastighed, hvormed et velforberedt cyberangreb kan gennemføres, bidrager til at gøre cyberspace til et offensiv-dominant domæne. Årsagen er den simple, at høj hastighed alt andet lige gør det lettere at gennemføre succesfulde overraskelsesangreb. Det samme gør de gunstige muligheder for at hemmeligholde et angreb, indtil umiddelbart før aggressionen påbegyndes. I modsætning til konventionel krigsførelse er det således ikke nødvendigt at samle og opmarchere tropper, fly eller skibe (se fx Liff 2012:415f). Et velforberedt

[15] Dette er hovedantagelsen i den såkaldte "offense-defense"-litteratur (se fx Van Evera 1984, Fearon 1995 samt Glaser & Kaufmann 1998). Kogt ind til benet baserer denne litteratur sig på en forestilling om, at et sikkerhedsmiljø domineret af offensive våben øger risikoen for væbnet konflikt af (i hvert fald) tre årsager: 1) staterne vil tendere i retning af at føre en mere aggressiv udenrigspolitik, 2) et offensiv-dominant miljø øger incitamentet til at handle præventivt, og 3) staterne vil i større udstrækning benytte sig af hemmeligt diplomati, hvilket øger risikoen for fejltagelser.

cyberangreb kræver "blot" kendskab til modstanderens svagheder samt softwarekode designet til at udnytte den identificerede sårbarhed.

Der kan næppe herske tvivl om, at forestillingen om cyberspace som et offensivt domæne har en hel del for sig. Alene det forhold, at de fleste praktikere og forskere antager, at cyberspace er offensiv-dominant, er formentlig med til at forøge investeringerne i offensive cyberkapabiliteter og dermed styrke de offensive instrumenter relativt betragtet. I den forstand er forestillingen i nogen grad selvopfyldende. Der er imidlertid også flere gode grunde til ikke at overdrive de offensive cybervåbens fordele. For det første hæfter flere eksperter sig ved, at der for tiden udvikles stadig mere effektive cyberforsvarsmekanismer, og det gælder ikke mindst i forhold til forsvaret af kritisk infrastruktur (Lindsay 2013:394ff; Rid 2013: 168ff). Så selv om de offensive våben måske stadig har et forspring, reduceres afstanden med tiden.[16]

Der er for det andet grund til at udfordre antagelsen om, at cyberangreb *generelt betragtet* er billige og teknisk set lette at udføre. På den ene side er det åbenlyst, at mange former for cyberkriminalitet og mindre angreb på hjemmesider ikke kræver mange års erfaring og uddannelse. Det er aktiviteter, som den nok så berømte "teenager i kælderværelset" kan udføre på sin bærbare computer. På den anden side er det lige så oplagt, at større angreb på kritisk infrastruktur og kontrolsystemer som regel er overordentligt komplicerede og enormt ressourcekrævende. Det illustrerer det såkaldte "Stuxnet-angreb" på Iran, der i form af en computervirus i sommeren 2010 inficerede et stort antal centrifuger på det iranske atomanlæg ved Natanz. Ifølge eksperter fik virussen centrifugerne til at destruere sig selv med det resultat, at der skete alvorlig skade på det påståede iranske atomvåbenprogram (Stark, 2011, og Borad m.fl., 2011). USA og Israel er under mistanke for at stå bag angrebet, men det er aldrig blevet officielt bekræftet (Sanger & Mazetti, 2007).

Den ekstremt avancerede software i Stuxnet krævede ikke blot i tusindvis af timers kodearbejde, men formentligt også et stort stykke traditionelt efterretningsarbejde og agenter på jorden i Iran (Farwell & Rohozinski 2011; Lindsay 2013). Efterfølgende oplysninger har endvidere vist, at Stuxnet-angrebet udgjorde et led i en større og mere ambitiøs offensiv amerikansk hemmelig kampagne – "Operation Olympic Games" – mod det iranske atomprogram (Sanger 2012). Det kan således godt være, at den nedre ende af cyberaggression-spektret er offensiv-dominant –

[16] Interview med James Lewis CSIS, Washington DC, September 2013.

men det gælder næppe i samme omfang (hvis overhovedet) i den øvre ende. Med Thomas Rids ord:

> Maximizing the destructive potential of a cyber weapon is likely to come with a double effect: it will significantly *increase* the resources, intelligence, and time required to build and deploy it – and increasing a cyber weapon's potential is likely to *decrease* significantly the number of targets (Rid 2013:36; se også Knake 2010).

Når de strategiske konsekvenser af fremkomsten af cybervåben skal vurderes, er det – for det tredje – nødvendigt at holde sig for øje, at cyberkonflikt aldrig vil komme til at finde sted i et vakuum. At der føjes et nyt offensivt-dominant domæne til de eksisterende konfliktdomæner (land, vand, luft og rummet), er således ikke nødvendigvis ensbetydende med, at der rokkes grundlæggende ved den overordnede balance mellem offensive og defensive kapaciteter i systemet. Det er derfor også langtfra givet, at risikoen for væbnet konflikt vil vokse nævneværdigt. I den sammenhæng er det helt afgørende, at den aktuelle overordnede balance mellem offensive og defensive våben hælder kraftigt i retning af forsvaret på grund af spredningen af atomvåben. Så selvom udviklingen af stadig mere avancerede cybervåben måske nok skaber incitamenter, der øger risikoen for væbnet konflikt, vil det ultimative defensive våben – atombomben – fortsat lægge en meget markant dæmper på i hvert fald stormagternes lyst til at indlede en væbnet konflikt – med eller uden cybervåben.

For det fjerde vil en række stater formentlig være tilbageholdende med at bruge offensive cybervåben, fordi disse med relativ stor sandsynlighed vil føre til omfattende skader på civile netværk, computere og infrastruktur ("collateral damage"). Som det til dels er tilfældet med kemiske og bakteriologiske våben, er også offensive cybervåben nemlig i praksis meget vanskelige at kontrollere og målrette. Det kan være endog meget svært at fokusere effekterne, og ifølge flere eksperter vil ikke-lineære kaskadeeffekter mere være reglen end undtagelsen (Liff 2012:421). Det er et forhold, der i sig selv kan gøre det vanskeligt at anvende i hvert fald nogle typer af cybervåben på en måde, der er forenelig med folkeretten.

Endelig er det vigtigt at understrege, at det på det generelle plan langt fra er givet at fremkomsten af cybervåben nødvendigvis øger risikoen for væbnet konflikt. Det kan endda vise sig, at det forholder sig lige modsat i den forstand, at en mulighed for at ramme en modstander i cyberspace overflødiggør konventio-

nel militær magtanvendelse / væbnet konflikt. Stuxnet-angrebet var formentlig en næsten lige så effektiv måde at forsinke det påståede iranske atomprogram på, som et vanskeligt gennemførligt konventionelt militært angreb havde været. Forskellen var bare, at angrebene ikke efterlod nogen døde og sårede. Som beskrevet af Thomas Rid:

> The first and main conclusion, and this book's core argument, is that the rise of cyber offenses represents an attack on violence itself. Almost all cyber attacks on record are non-violent. Those cyber attacks that actually do have the potential to inflict physical violence on machines or humans can do so only indirectly...: so far, violence administered through cyberspace is less physical, less emotional, less symbolic, and less instrumental than more conventional uses of political violence... cyber attacks of all strands, even in their predominantly non-violent ways, may achieve a goal that previously required some form of political violence... (Rid 2013: 166f)

I den udlægning er cyberspace ikke et offensiv-dominant domæne, men derimod et medium der faciliterer en potentielt set mindre voldelig form for politisk konflikt.

Afskrækkelse og attribution

En anden ofte fremført hypotese om konflikt i cyberspace er, at det i reglen er meget vanskeligt – hvis ikke umuligt – at identificere aktøren/aktørerne bag en fjendtligtsindet cyberhandling – det såkaldte *attributionsproblem*. Med informationsudvekslinger på Internettet (digitale pakker) følger ganske vist både en modtager- og afsenderadresse i form af IP-adresser, men fordi fjendtligsindede aktører nemt kan skjule sig og sågar undertiden vil kunne "overtage" andre aktørers computere til at gennemføre angreb, kriminalitet eller spionage – såkaldte "*zombie-aktiviteter*" – er det ofte forbundet med store udfordringer at fastlægge identiteten på angriberen. Som en rapport fra Chatham House har bemærket, er en af "the main attractions of cyberspace ... 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" (Cornish m.fl. 2010:11). Dertil kommer, at cyberspace i stor udstrækning gør det muligt for fjendtlige aktører at iværksætte deres skadevoldende angreb uden varsel for herefter at "forsvinde" igen (Tsagourias 2012:5), og at det i øvrigt langt fra er givet, at den stat, hvortil en IP-adresse eventuelt kan spores, er behjælpelig med at opklare, hvem der stod bag et angreb. At en cyber-

forsvarer således fra tid til anden er i stand til at spore angriberens reelle IP-adresse, er derfor langt fra ensbetydende med, at det bliver muligt at straffe den eller de pågældende personer/stater bag angrebet (Libicki 2009; Knake 2010; Clark & Landau 2011; Schreier 2012:77ff).

Set i et strategisk perspektiv er identifikationsproblemerne foruroligende. Anonymitet vanskeliggør nemlig en helt central sikkerhedspolitisk strategi: Afskrækkelse.[17] Kernen i afskrækkelse som strategisk instrument er at overbevise en potentiel angriber om det uhensigtsmæssige i at gennemføre en fjendtlig handling, fordi det er muligt at forsvare sig imod aggressionen på en effektiv måde ("deterrence by denial"), og/eller fordi et angreb vil blive gengældt på en facon, der i et passende omfang truer angriberens interesser ("deterrence by punishment"). Sidstnævnte type af afskrækkelsesstrategi – der i reglen betragtes som den mest betydningsfulde (Libicki 2009) – fungerer selvsagt ikke, når angriberen ikke kan identificeres. En strategi baseret på gengældelse er ganske enkelt ikke troværdig i et domæne præget af anonymitet. Eller som formuleret af Adam Liff: "The challenges inherent in attributing CNA [Computer Network Attacks, AH & JR], developing active cyberdefenses (and thus the ability to credible threaten retaliation), … will make it difficult to deter potential aggressors and thus increase the frequency of war" (Liff 2012: 417).

Heller ikke denne ortodoksi om de strategiske udfordringer i cyberspace er imidlertid problemfri. I hvert fald to forhold taler nemlig for, at attributionsproblemet er mindre alvorligt end almindeligvis antaget. For det første peger flere eksperter på, at identifikationsproblemet ikke er helt så monumentalt som antaget af mange. Selvom det kan være et omkostningstungt, tidskrævende og møjsommeligt arbejde, har stater med en vis portion teknisk ekspertise rent faktisk relativt gode chancer for at fastlægge identiteten på en cyberangriber (Knake 2010; Gartzke 2013: 46ff). Men fordi attribution i reglen vil lægge beslag på omfattende ressourcer, vil et opsporingsarbejde dog kun blive sat i gang i relation til de mest alvorlige cyberangreb. Selvom fjendtligsindede aktiviteter i den nedre ende af skalaen kan udgøre et alvorligt irritationsmoment, vil det ofte ikke kunne betale sig at sætte et stort detektivarbejde i gang for at undgå mindre alvorlige forsøg på eksempelvis hacking, phishing eller DDoS-angreb. Med Knake's ord: "For nuisance attacks, attribution is rarely a problem. The problem is that few if any investigative resources are assigned to cyber criminal activity that does not have a high monetary val-

[17] For autoritative analyser af forskellige former for afskrækkelsesstrategier, se Bernard Brodie (1959); Glenn Snyder (1961); John Mearsheimer (1983) og Freedman (2004).

ue associated with it" (Knake 2010: 6). De alvorligste cyberangreb vil imidlertid med al sandsynlighed udløse indsættelse af omfattende efterretningsressourcer.

Dertil kommer, at kun et meget begrænset antal (primært) statslige aktører har den fornødne ekspertise og de nødvendige ressourcer til at kunne udvikle cybervåben, som hører hjemme i den øvre ende af trusselsskalaen (se fx Forsvarets Efterretningstjeneste 2013). Dermed er antallet af "mistænkte" stærkt reduceret. Igen med Knakes ord:

> For the highest level threat, that of cyber warfare, the attribution problem is largely overstated. As with other Internet based attacks, technical attribution may be difficult and the forensic work will take time, but at present there are limited number of actors that are capable of carrying out such attacks. Moreover, the resources, planning, and timeline for such attacks would provide many opportunities to identify and disrupt such attacks (Knake 2010:4).

Af ressourcemæssige årsager er attributionsproblemet således samlet set fortrinsvis knyttet til de mange – mindre alvorlige – fjendtligsindede cyberaktiviteter, som stater, virksomheder og privatpersoner dagligt plages af.

Det andet forhold, som bidrager til at gøre attributionsproblemet mindre end vanligvis antaget, knytter sig til en helt grundlægende clausewitziansk forestilling om krigens natur: At krig og brugen af væbnet magt basalt set sigter mod at "tvinge en modstander til at gøre vores politiske vilje". Krig er et politisk instrument, der skal sikre en fred på egne betingelser. Det betyder imidlertid også, at den politiske vilje skal kommunikeres. Brugen af væbnet magt uden medfølgende besked om voldsanvendelsens politiske mål vil blot efterlade den angrebne part såret og forvirret. For at gennemtvinge sin politiske vilje må aggressoren altså kommunikere og således "vise sit ansigt". I den optik bliver anonymitet lige så stor en udfordring for angriberen som for den angrebne part (Betz 2012: 694ff). Det gælder i reglen også for terrororganisationer. For at vinde opbakning til sin sag må organisationen tage ansvaret for handlingen. Som pointeret af Gartzke:"Terrorists spend as much time marketing their exploits as they do fighting, bombing, assassinating, and so on. Where anonymity protects an aggressor from retribution, it also dilutes credit for the deed (Gartzke 2013: 46f).

Denne snævre clausewitzianske argumentation er dog heller ikke uden faldgruber. For nok vil væbnet magt – herunder cybervåben – i reglen bliver anvendt med henblik på at få en modstander til at gøre "vores politiske vilje", men voldsanvendelsen kan

også tage sigte mod at erodere modstanderens fysiske evne til at kæmpe eller opstille et militært forsvar. Og i sådanne tilfælde er det ikke nødvendigt at kommunikere den politiske vilje og give sig til kende over for modstanderen. Det var med al sandsynlighed intentionen bag det førnævnte Stuxnet-angreb under "Operation Olympic Games" mod det iranske atomprogram. Angrebet var således mindst lige så meget et forsøg på at underminere iranernes bestræbelser på at berige uran, som det var et politisk signal til Teheran om det hensigtsmæssige i at indstille atomprogrammet. Og derfor var det ikke nødvendigt, at iranerne vidste, hvem der stod bag. På samme måde er det muligt at forestille sig en lang række andre angreb, der har til hensigt at svække en anden stats militære og økonomiske styrke fremfor at få modstanderen til at træffe nogle helt bestemte politiske valg. For så vidt angår den type af cyberangreb, er anonymitet ikke et problem for aggressoren. Tværtimod. Og herved genopstår attributionsproblemet for den stat, der gøres til genstand for cyber-operationen.

Styrkelsen af de svage

Den tredje ofte fremførte påstand om de strategiske implikationer forbundet med fremkomsten af "det femte konfliktdomæne" er, at cybervåben vil styrke det internationale systems svageste aktører. I den udlægning vil cybervåben uafværgeligt blive terroristernes og de fattigste staters foretrukne magtmiddel. Som præsident Obama skriver i en artikel fra 2012: "In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home" (Obama 2012). Centralt i denne argumentation står forestillingen om, at en svag aktør kan opnå en betydelig strategisk effekt gennem indsatsen af forholdsvis små økonomiske ressourcer. I modsætning til stærke vestlige aktører, behøver den svage ikke længere at investere i kampfly, hangarskibe og kampvogne for at kunne udfordre den konventionelt betragtet stærke aktør, hedder det. Ifølge fortalerne for denne tese er resultatet derfor en markant udjævning af konventionelle magtasymmetrier (se fx Hughes 2010; Lynn 2010; Lambeth 2011, Schreier 2012:27f).

Af de tre påstande, der præsenteres og diskuteres her, er denne sidste tese formentlig den mest problematiske. En del tyder ganske vist på, at en række forholdsvis svage statslige og ikke-statslige aktører (heriblandt al-Qaeda, Hamas, Hizbollah og zapatister) har vist interesse for og/eller investeret i cyberkapabiliteter (Hughes 2010; Forsvarets Efterretningstjeneste 2013). Og det er indlysende, at størstedelen af disse "svage aktører" kun i meget begrænset omfang selv er sårbare overfor cyberangreb. Ydermere vil en række af disse aktører formentlig have den nødvendige ekspertise til at kunne udvikle cybervåben i den lettere og mellemtunge ende af skalaen.

Det er imidlertid lige så indlysende, at selvom prisen på et avanceret cybervåben måske nok er diminutiv set i forhold til priserne på moderne kampfly eller hangarskibe, så kræver det en formidabel teknisk ekspertise at udvikle målrettede våben som eksempelvis Stuxnet-virussen, der blev anvendt under "Operation Olympic Games". Virkelig effektfulde cybervåben lader sig næppe producere i en landsby i Nordwaziristan eller i Gaza-striben. Effektive cyberinstrumenter må nødvendigvis tage afsæt i et detaljeret kendskab til de systemer – og ikke mindst de styrings- og kontrolkomponenter – som et angreb ofte vil være rettet imod. For at kunne udvikle en operationel software vil det således ofte være nødvendigt at have adgang til nøjagtige kopier af de systemer, man ønsker at angribe. Som i tilfældet med Stuxnet-virussen kan der være behov for at gennemteste softwaren (cybervåbnet) på lignende styrings- og kontrolkomponenter. Og da disse systemer måske ikke er tilgængelige på det åbne marked, kan det også være nødvendigt med en velfungerende efterretningstjeneste.

Med til at dæmpe svage staters appetit på at gennemføre cyberangreb mod stærkere statslige modstandere er formentlig også, at sidstnævnte har gode muligheder for at svare igen med konventionelle våben. Under den kortvarige væbnede konflikt i august 2008 mellem Georgien og Rusland blev Georgien ramt af omfattende cyberangreb, der ifølge flere kilder udgik fra Rusland (Tikk m.fl. 2010:66-90). Mens Rusland således ikke ville løbe en stor risiko ved at gennemføre et cyberangreb på en del af Georgiens kritiske infrastruktur (fordi Georgien næppe ville turde svare igen med militær magt), forholder det sig helt omvendt i det modsatte tilfælde. På samme måde kan der argumenteres for, at det netop var USA's og Israels overlegenhed på det konventionelle militære område, der var selve forudsætningen for "Operation Olympic Games" og Stuxnet-angrebet. Et ødelæggende *iransk* cyberangreb mod USA's nukleare våbenprogram ville antageligvis have medført en anderledes kontant reaktion fra amerikanerne.

Der er med andre ord gode grunde til at forholde sig skeptisk til forestillingen om cybervåben som den store "magtudjævner". Rent faktisk er det mindst lige så megen grund til at hævde, at udbredelsen af cybervåben vil styrke de stærkeste og mest ressourcestærke aktører, og dermed konsolidere eksisterende magtasymmetrier (Rid 2013:166ff).[18] Eller som formuleret af Lindsay:

[18] I november 2013 skrev Forsvarets Efterretningstjeneste: "Ikke-statslige grupperinger viser interesse for at angribe kritisk infrastruktur [i Danmark, AH & JR], men har ikke de fornødne tekniske kapaciteter til at udføre avancerede angreb". Videre hed det: "Det er derfor primært de særligt teknisk dygtige aktører, herunder stater, der på kort til mellemlangt sigt vil kunne udgøre en trussel mod kritisk infrastruktur i Danmark" (Forsvarets Efterretningstjeneste 2013).

> Cyber warfare is not a weapon of the weak. Weaker actors face steep barriers to weaponization for causing meaningful damage, and they are vulnerable to punishing retaliation if they somehow do succeed in injuring the strong. Strong states, by contrast, have the resources and risk tolerance to wage cyber warfare against relatively weaker targets like Iran. The barriers will tend to price weaker actors out of strategic cyber warfare. The technically and organizational sophistication level of play required for cyber warfare is generally beyond the capacity of a lone hacker, a small group of amateurs, or even organized criminals, some of the favorite bogeymen of cyberwar discourse (Lindsay 2013:389).

De mange afsløringer af NSA's programmer for avanceret spionage og aflytning af alt fra fremmede statsoverhoveder og udenlandske virksomheder til statsborgere viser da også med al tydelighed, at cyberrelaterede midler og våben på ingen måde kun er de svages redskab. Og i sammenhæng med bl.a. "Operation Olympic Games" mod Iran illustrerer afsløringerne også, at den megen snak om, at Kina og Rusland skulle være de mest aggressive aktører i cyberspace er en sandhed med modifikationer. Amerikanerne er mindst lige så aktive – hvis ikke mere. Dermed bliver det også mere og mere tydeligt, at der på trods af meget forskelligartet retorik – og tilsyneladende divergerende syn på legitimiteten af at bruge cyberspace i et strategisk og konfliktøjemed – i virkeligheden ikke er de store regionale forskelle i opfattelsen af, hvorvidt cyberinstrumenter er legitime i konkurrencen med andre stater. Det er imidlertid ikke ensbetydende med, at forskellige stater ikke kan have forskellige syn på, hvornår cyberinstrumenter kan anvendes i bestræbelserne på at kontrollere *egne* borgere.

Endelig udfordrer de faktiske historiske erfaringer med krig og magtanvendelse i cyberspace den udbredte forestilling om cybervåben som den store strategiske magtudjævner og de ikke-statslige aktørers foretrukne magtmiddel. Selvom en række vestlige stater i efterhånden en årrække har baseret store dele af deres økonomiske, militære og forvaltningsmæssige infrastruktur på internetbaserede løsninger, så har det store cyberterror-angreb indtil videre glimret ved sit fravær (Healey 2012. Hvis cyberterrorisme var så enkelt og billigt at udføre, som anført af flere, havde vi nok allerede set eksempler på det.

Cyberkonflikts folkeretlige implikationer

Vi har indtil nu set, at konflikt i cyberspace udfordrer vores traditionelle måder at begrebsliggøre politisk vold og væbnet konflikt på, og at fremkomsten af cybervåben også stiller en række nye spørgsmål ved de strategiske relationer mellem stater og mellem stater og ikke-statslige aktører. I denne del af rapporten stiller vi nu skarpt på to af de folkeretlige implikationer, der er forbundet med fremkomsten af cybervåben og andre former for cyberrelaterede midler. For det er nemlig langt fra kun de strategiske studier og studierne i sikkerhedspolitik, der udfordres af cyberkonflikt. Det samme gør retsvidenskaben.

Det er der sådan set intet overraskende i. Nye teknologier og nye magtmidler udfordrer som regel det eksisterende retsgrundlag (Henriksen 2012: 8-9). Sådan var det i det forbindelse med de første eksempler på luftkrig i 1910-20'erne, sådan var det i 1940'erne, da atomvåbnene blev "opfundet" og anvendt og senest har der i løbet af det seneste årti været en vis tvivl om, hvorledes anvendelsen af nye førerløse teknologier, såsom bevæbnede førerløse luftfartøjer, på kampladsen har skullet forenes med det eksisterende retsgrundlag (Kessing 2013; Henriksen & Ringsmose 2013).

Det er indledningsvis vigtigt at slå fast, at cyberspace og cyber-operationer *ikke* er undtaget folkeretlig regulering. Ingen betvivler for alvor, at cyberspace i hvert fald i udgangspunktet reguleres af de samme folkeretlige normer og principper, der regulerer de mere fysiske domæner (Goldsmith 2006). Men dermed ikke sagt, at det så er ligetil at vurdere, hvorledes folkeretten mere præcist finder anvendelse i cyberspace og på cyber-operationer. Tværtimod. I det følgende kigger vi på de to udfordringer, der efter vores opfattelse er af størst principiel betydning. Det drejer sig for det første om den aktuelle uklarhed om, hvorledes cyber-operationer passer ind i den folkeretlige regulering af, hvordan og med hvilke midler stater må forfølge deres interesser i deres internationale relationer. Og for det andet om, at det ikke kun er de strategiske studier, men også folkeretten, der udfordres af det forhold, at det ofte er endog særdeles vanskeligt at identificere den aktør, der står bag konkrete cyberoperationer. Formålet med gennemgangen i det følgende er med andre ord ikke at forsøge at opregne, *hvorledes* folkeretten regulerer cyberkonflikt (her må læseren søge tilflugt i den folkeretlige faglitteratur[19]), men i stedet at redegøre for to af de forhold, der på nuværende tidspunkt *gør det vanskeligt* at lave en sådan opregning.

[19] Se eventuelt Schmitt 2011, og Henriksen 2012 & 2014, og de heri opregnede henvisninger.

Vi beskrev tidligere i rapporten, at det i studierne af politisk vold og væbnet konflikt kan være begrebsmæssigt vanskeligt at afgøre, hvorvidt en fjendtlig aktivitet i cyberspace udgør en krigshandling eller ej. Anvendelsen af cybervåben passer nemlig kun i begrænset omfang til de traditionelle kategorier, og det kan være særdeles besværligt at bestemme de reelle effekter af – samt intentioner bag – et givet cyberangreb. Disse begrebsmæssige implikationer genfindes i folkeretten, hvor der består en markant udfordring i at vurdere, hvorledes cyberoperationer skal og bør klassificeres på den skala over tilladte og folkeretsstridige handlinger, der ligger til grund for reguleringen af, hvorledes stater må agere internationalt for at fremme deres interesser. Det er med andre ord heller ikke i folkeretten helt oplagt, hvordan teorien skal forholde sig til den særlige form for gene og/eller skade, som forårsages af elektroniske magtmidler.

Den eksisterende regulering tager sit udspring i det helt fundamentale princip, at alle stater er suveræne og beskyttede af et princip om *territoriel ukrænkelighed*, og at en stats udøvelse af myndighed på en anden stats territorium derfor som det helt klare udgangspunkt udgør en folkeretsstridig suverænitetskrænkelse. Spionage strider dog ikke mod folkeretten, medmindre det rettes mod infrastruktur, individer eller kommunikation, der er særlig beskyttet (Chesterman 2006: 1081-1090). Stater må med andre ord godt udspionere og genere hinanden en lille smule, og det er derfor heller ikke sikkert, at NSA's spionprogrammer nødvendigvis strider med folkeretten.

Folkeretten er baseret på et princip om, at suveræne stater skal have lov til at udforme deres egen politik i fred, og derfor vil suverænitetskrænkelser, der søger at presse/påvirke en stat på et spørgsmål, hvor denne ikke skal tåle fremmed indblanding (Jamnejad & Wood 2009: 349), stride mod et folkeretligt "*ikke-interventionsprincip*", der genfindes i folkeretlige sædvane (Imternational Court of Justice *Nicaragua*: pr. 202-205; . Langt alvorligere bliver det imidlertid – og her er vi endnu et niveau oppe på skalaen over folkeretsstridige handlinger – hvis en konkret handling har karakter af egentligt *magtanvendelse*. FN-pagtens artikel 2, stk. 4, forbyder medlemsstaterne at true eller gøre brug af magt i deres internationale relationer, og pagten opstiller herved en ydre grænse for, hvor langt stater må gå for at forfølge deres politiske interesser, inden de kan komme i konflikt med deres forpligtelser i henhold til pagten. Det øverste og dermed mest alvorlige niveau for folkeretsstridige handlinger udgøres af de væbnede handlinger, der har karakter af *væbnede angreb* i henhold til artikel 51 i FN-pagten, og som anses for at være et så alvorligt anslag mod en stat, at det – trods det generelle magtforbud – udløser

en ret til selvforsvar for den stat, der gøres til genstand for angrebet. Et væbnet angreb udløser med andre ord en ret til at gå i krig.

I forhold til cyber-operationer består opgaven altså i at afklare, hvordan sådanne magtmidler passer ind i det ovennævnte hierarki. Hvor går den nedre grænse for, hvornår statslig adfærd i cyberspace krænker andre staters suverænitet? Hvornår bliver cyberspionage til en folkeretsstridig suverænitetskrænkelse? Hvornår strider cyberoperationer med ikke-interventionsprincippet? Kan cyberoperationer sidestilles med magtanvendelse i FN-pagtens forstand? Og så videre (se figur 2).

Det er imidlertid lettere sagt end gjort, og det skyldes bl.a., at der endnu ikke er vedtaget nogen folkeretlige instrumenter, der er målrettet den konkrete regulering af spørgsmålet.[20] Der er derfor ikke noget alternativ til at forsøge at drage analogier og paralleller fra de mere traditionelle former for magtanvendelse og prøve at vurdere, hvad cyberoperationer og deres effekter minder mest om (Ryan m.fl. 2010; Henriksen 2012: 9). Skal cyberoperationer sidestilles med politisk og økonomisk pression, såsom sanktioner, embargoer? Eller med magtanvendelse?

Som berørt tidligere er cyberoperationer imidlertid særdeles svære at forene med de velkendte magt- og pressionsformer. Med Daniel T. Kuehls ord forudsætter vores "existing paradigm of war ... kinetic actions, destroying things, or crossing of phys-

Figur 2. Niveauer for cyberoperationer

[20] Europarådet vedtog i 2001 en konvention til bekæmpelse af cyberkriminalitet, se *Convention on Cybercrime, CETS No. 185*, men den forholder sig ikke direkte til den form cyberangreb, der er i fokus her.

ical boundaries with physical objects such as airplanes and tanks" (Kuehl 1999:54). FN-pagten tager da også først og fremmest sigte på at regulere de *midler,* som staterne gør brug af for at fremme deres interesser, og ikke de *konsekvenser*, staternes konkrete ageren måtte have(Schmitt 2011: 573).

Når det er vanskeligt at drage analogier, så hænger det også sammen med, at det endnu er meget sparsomt, hvad der ligger af retsafgørelser og statspraksis, der kan bruges som fortolkningsbidrag. Der findes en masse bidrag fra folkeretlige eksperter i litteraturen, og i foråret 2013 offentliggjorde en international ekspertgruppe en manual om reguleringen af de mest væbnede former for cyberangreb – den såkaldte "Tallinn Manual" (Schmitt 2013). Men der findes endnu meget få bidrag fra domstole og staterne selv. Det er også et problem, at offentligheden kun i begrænset omfang har indblik i, hvad stater og andre aktører konkret foretager sig i cyberspace. Det er særdeles sparsomt, hvad der findes af offentligt tilgængelige oplysninger om de nærmere omstændigheder omkring påståede cyberangreb, og om den måde, som stater har reageret herpå. Den manglende "gennemsigtighed" gør det vanskeligt at identificere klare cases, der kan bidrage til at kaste lys over, hvorledes de relevante analogier bør drages.

Den eksisterende uklarhed leder til tre centrale pointer. Den *første* er, at det nu engang indtil videre kun er muligt at give tentative bud på, hvorledes de relevante analogier skal drages og cyberoperationer reguleres. Den hidtidige forskning indikerer, at der formentlig skal anlægges en såkaldt "effektbaseret tilgang", og at cyberoperationer derfor sidestilles med mere traditionelle former for magtanvendelse i det omfang, de direkte effekter af operationerne har tilstrækkelig lighed med kinetisk magt (Schmitt 2013: regel 11, pkt. 8-10; Henriksen 2012: 13-17). Det er indtil videre imidlertid kun et bud.

En række praktiske eksempler illustrerer, hvor kompliceret det i praksis kan være at vurdere, hvorledes cyberaktiviteter skal klassificeres folkeretligt. Det første eksempel er fra april og maj 2007, hvor Estland som berørt tidligere blev udsat for et tre uger langt cyberangreb i form af såkaldte "Distributed Denial of Service" (DDOS)-angreb, der lammede et stort antal offentlige og private mål (Tikk m.fl. 2010:15-22. Angrebene fulgte i kølvandet på 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 det russiske mindretal i Estland og af den russiske regering i Moskva. Estland har efterfølgende insinueret, at angrebet blev udført af "patriotiske hackergrupper" fra den kriminelle un-

derverden i Rusland, der blev støttet af de russiske myndigheder, men den russiske regering har kategorisk afvist enhver form for indblanding (Tikk m.fl. 2010:23). Det er vanskeligt at vurdere det tre uger lange angreb på den folkeretlige skala over acceptable og uacceptable handlinger. Hvis Rusland stod bag, kvalificerer angrebene som krænkelser af estisk suverænitet, og hvis angrebene skulle presse de estiske myndigheder til at omgøre beslutningen om at flytte krigsmonumentet, udgjorde de nok også en folkeretsstridig russisk "intervention" i Estlands indre anliggender (Henriksen 2012:26). Det er imidlertid straks sværere at vurdere, om angrebene også kan sidestilles med egentlig magtanvendelse i henhold til FN-pagten. Det forhold, at angrebene hverken forårsagede personskade eller fysisk skade taler umiddelbart imod (se også Henriksen 2012: 26), men ikke alle er enige (se bl.a. Schmitt 2011:577). Angrebene udgjorde imidlertid med stor sandsynlighed ikke et væbnet angreb, der udløste en estisk ret til selvforsvar (Henriksen 2012:27; Schmitt 2013, regel 13, pkt. 13). Estland påberåbte sig da heller ikke NATO's 'musketer-ed' i Washington-traktatens artikel 5, hvorefter et væbnet angreb på et medlem af alliancen anses som et angreb på alliancen som helhed. (Tikk m.fl. 2010:25-26).

Det andet eksempel er fra marts 2013, hvor Sydkorea blev ramt af et massivt cyberangreb, der forårsagede omfattende lammelse af bl.a. banker og nyhedsmedier. Angrebene blev indledningsvis anset for at være en isoleret episode – der fik tilnavnet "Dark Seoul" – men efterfølgende undersøgelser viste, at der i virkeligheden var tale om en årelang serie af cyberrelaterede angreb på landet – "Operation Troy" – der også inkluderede omfattende cyberspionage rettet mod sydkoreanske militære netværk (Sherstobitoff m.fl. 2013). Eksperter spekulerer i, at angrebene udgik fra Sydkoreas nabo i nord (Junio 2013II), men det er ikke blevet bekræftet. På samme måde som angrebet mod Estland kan have krænket estisk suverænitet og udgjorde en folkeretsstridig intervention (hvis det var Rusland, der var ansvarlig for angrebene), vil de dele af Operation Troy, der forårsagede reel skade i Sydkorea, formentlig også udgøre en krænkelse af sydkoreansk suverænitet, hvis det var en anden stat, såsom Nordkorea, der stod bag. Men herefter bliver det mindre oplagt. Som berørt tidligere strider spionage i udgangspunktet ikke mod folkeretten, og det betyder formentlig, at de dele af Operation Troy, der alene bestod i cyberspionage næppe heller gjorde det. Det er heller ikke sikkert, at angrebene udgjorde en ulovlig intervention i Sydkorea, for som nævnt forudsætter en folkeretsstridig intervention, at den "intervenerende" stat på en eller anden måde forsøger at presse territorialstaten til at ændre sin politik på et givet område. Og det er ikke lige til at se, hvilken sydkoreansk politik, Operation Troy havde til formål at ændre. Det må også af den grund stå hen i det uvisse, om cyberangrebene krænke-

de forbuddet mod brug af magt i FN-pagten. Et væbnet angreb var det dog under alle omstændigheder næppe.

Det tredje og sidste eksempel er det "Stuxnet-angreb" på det iranske atomprogram, som vi allerede har berørt flere gange, og som blev udført som led i "Operation Olympic Games". Heller ikke dette angreb er nemlig helt let at klassificere på den folkeretlige skala for potentielt retsstridige handlinger. Der er næppe tvivl om, at angrebet krænkede Irans suverænitet og også udgjorde et brud på interventionsforbuddet. Men var det også at anse som egentlig magtanvendelse, der stred med FN-pagten? Muligvis. Den direkte effekt af angrebet – den fysiske destruktion af et stort antal centrifuger – kan i hvert fald umiddelbart sammenlignes med den fysiske skade, der forårsages ved brugen af kinetiske våben (Schmitt 2013: regel 13, pkt. 13; Henriksen 2012:27). Enkelte medlemmer af den ekspertgruppe, der udarbejdede Tallinn-manualen går faktisk så langt som til at påstå, at Stuxnet bør klassificeres som et væbnet angreb, der i teorien kunne have udløst en iransk ret til selvforsvar (Schmitt 2013: regel 13, pkt. 13).

Den *anden* centrale pointe er, at den aktuelle uklarhed ikke blot bør interessere jurister, men i høj grad også eksperter i sikkerhedspolitik, militære eksperter og naturligvis politikere. Uvisheden handler nemlig ikke alene om jura, men i høj grad også om strategi og politik. Folkeret og international politik hænger uløseligt sammen, og den eksisterende uklarhed om, hvordan der skal trækkes analogier fra traditionelle retlige figurer og gøren og laden i cyberspace, betyder i praksis, at der bliver et stort spillerum for udfoldelse af politik. Det er nemlig som berørt i høj grad staterne og deres praksis, der leverer svarene på de åbne folkeretlige spørgsmål, og derfor bliver spørgsmålet om, hvordan folkeretten regulerer cyber-operationer i høj grad også til et spørgsmål om, hvordan sådanne operationer *bør* reguleres. Det giver med andre ord ikke mening at adskille de tidligere berørte begrebsmæssige uklarheder om cyberkonflikt fra de folkeretlige ditto. I praksis kan den retlige uklarhed herved også være en kærkommen anledning til, at stater som Danmark gør sig nogle strategiske overvejelser om, hvorledes cyberspace bør reguleres på sigt. Hvad *bør* være acceptabel og uacceptabel adfærd i cyberspace? Hvor går grænsen for, hvor meget gene Danmark vil finde sig i på nettet? Hvor synes vi, at grænsen skal drages mellem spionage og kriminalitet i cyberspace? Bør det være muligt for NSA at udspionere ikke bare danske politikere men også danske borgere uden en retskendelse? Og så videre.

Da folkeretten som bekendt opstiller de internationale spilleregler for, hvordan og hvorledes stater må forsøge at fremme deres interesser, kan det ikke undre, at stater til alle

tider har anvendt folkeretten og folkeretlige fortolkninger som et redskab til at fremme deres interesser. Betegnelsen "lawfare" bruges i stigende grad som en samlebetegnelse om strategisk anvendelse af jura og retlige argumenter (Dunlap 2011; Henriksen 2013), og den strategiske anvendelse af retlige argumenter er særlig tydelig på området for reguleringen af magtmidler, hvor staters fortolkninger af folkeretten ofte afspejler deres magtforhold. Svage stater har eksempelvis historisk arbejdet for, at magtforbuddet i FN-pagten har skullet fortolkes meget bredt, mens stærkere stater har arbejdet for det modsatte. Debatten om reguleringen af cyberspace er blot det seneste eksempel på denne tilbagevendende dynamik (Waxman 2011; Henriksen 2012).

Hvilket leder os frem til den *tredje* centrale pointe, der flyder af den eksisterende folkeretlige uklarhed om reguleringen af cyberoperationer. *Netop* fordi den aktuelle uklarhed ikke kun handler om jura, men nok så meget om politik, må staterne forvente, at det bliver endog særdeles vanskeligt at opnå international enighed. Nationale forskelle i niveauer af sårbarhed overfor cyberangreb, forskelle i offensive cyberkapaciteter, forskelle i graden af respekt for folkeretlige normer og lignende vil ganske enkelt gøre det svært for stater at enes om den mest hensigtsmæssige regulering af cyberrelaterede midler (Waxman 2011:456). I det omfang, opbygningen af en avanceret cyberkapacitet eksempelvis kan bidrage til at opveje en eksisterende konventionel militær underlegenhed, er det urealistisk, at en militær underlegen stat vil have den samme interesse som en militær overlegen stat i en regulering, der begrænser cyberoperationer. Og det gælder i særdeleshed i det omfang, den militært underlegne stat er mindre sårbar over for andre staters cyber-operationer end den militært overlegne stat. Hvorfor skulle en stat som Nordkorea, der efter sigende har udviklet stærke offensive cyberkapaciteter og samtidig selv er meget lidt sårbar over for cyberangreb på dets infrastruktur, arbejde for at gøre et bredt spektrum af skadevoldende cyberaktiviteter retsstridige?

Det hører også med til historien, at stater har meget forskellige opfattelser af, i hvilket omfang kommunikation og aktiviteter i cyberspace i øvrigt bør beskyttes. For mens vestlige demokratier i høj grad anser cyberspace som et grundlæggende positivt medium, der kan bidrage til at fremme frihed og demokratiske værdier, forholder det sig anderledes i andre dele af verden, såsom i Kina og i mange stater i Mellemøsten. Her opfattes cyberspace og dets muligheder for grænseoverskrivende udvekslinger af ideer og ytringer i stedet som en trussel mod eksisterende autoritære styreformer (Healey 2012:7). Sådanne forskelle vil uundgåeligt komme til udtryk i staternes holdninger til, hvorledes aktiviteter og handlinger i cyberspace bør reguleres folkeretligt (Waxman 2011:456-457).

Behovet for attribution i folkeretten

Den anden væsentlige folkeretlige udfordring ved anvendelsen af cyberrelaterede magtmidler er en konsekvens af de identifikationsproblemer i cyberspace, vi berørte tidligere i rapporten. Cyberspace gør det i stor udstrækning muligt for fjendtlige aktører at skjule deres identitet, og det er ikke kun stater, der kan blive fristede af anonymiteten i cyberspace og den deraf følgende lave risiko for at blive afsløret. Det kan private aktører også, og fristelsen for disse bliver selvsagt ikke mindre af, at de mindst avancerede cybervåben som berørt er relativt frit tilgængelige og ikke forbundet med de store økonomiske udgifter at anskaffe.

Et af problemerne ved identifikationsproblemerne i cyberspace er, at det i høj grad muliggør såkaldt "plausible deniability" (Cornish m.fl. 2010:13), hvor stater i strid med de faktiske forhold kan fremstå, som om de ikke er involveret i de konkrete cyberangreb, som diverse private aktører udfører mod andre stater. En af de stater, der er under mistanke for at lukrere på identifikationsproblemerne, er Rusland, der i forbindelse med cyberangrebet mod Estland i 2007 som berørt ovenfor bl.a. blev mistænkt for at have samarbejdet med de patriotiske hackergrupper, der stod bag angrebet (Traynor 2007). En tilsvarende mistanke retter sig i øvrigt mod Rusland i forhold til omfattende cyberangreb, som russiske hackere som tidligere beskrevet rettede mod mål i Georgien i optakten til – og under – den væbnede konflikt mellem Rusland og Georgien i august 2008 (Allan 2013). Også Kina er flere gange blevet beskyldt for at udnytte de omfattende identifikationsproblemer i cyberspace og muligheden for at opretholde "plausible deniability" ved enten selv eller ved hjælp af mere eller mindre statskontrollerede hackere at gennemføre omfattende cyberaktiviteter mod mål i andre stater (BBC 2013).

Vi beskrev tidligere, at en mangel på attribution gør det vanskeligt at anvende strategier, der er baseret på afskrækkelse. Med folkeretlige briller består det problematiske ved manglen på identifikation bl.a. i, at en stat kun sjældent vil være internationalt ansvarlig for private hackeres skadevoldende cyberaktiviteter, der udgår fra dets territorium. For at statuere et internationalt ansvar kræves som udgangspunkt, at det kan godtgøres, at en privat aktør handler efter *ordre* fra staten, eller at sidstnævnte kan udøve *effektiv kontrol* over aktøren i det tidsrum, hvor denne begik de pågældende handlinger (International Law Commission: art. 8; International Court of Justice *Nicaragua*: pr. 115; International Court of Justice *Genocide*: pr. 400). Og det vil kun yderst sjældent kunne godtgøres.

De høje krav til at statuere statsansvar er en kilde til stor frustration for de stater, der mistænker andre stater, såsom Rusland og Kina, for at udnytte identifikationspro-

blemerne til at gennemføre cyberoperationer mod andre stater, og flere kommentatorer er af den opfattelse, at retstilstanden er så uholdbar, at den bør genovervejes. Ifølge Collin S. Allan er der ganske enkelt behov for "a new test ... for state attribution" (Allan 2013:78), og også Jason Healey og Matthew Hoisington lægger op til en ny tilgang til problemstillingen (Healey 2012; Hoisington, 2009:453). Collin S. Allan foreslår bl.a. at vende bevisbyrden om i de tilfælde, hvor der er et tidsmæssigt sammenfald mellem private hackerangreb og en igangværende kontrovers mellem to stater. I sådanne situationer ville det derfor ikke – som tilfældet er i dag – være stat A, der skal godtgøre, at stat B står bag konkrete hackerangreb, men derimod op til stat B at vise, at det *ikke* er tilfældet. Som Allan bemærker, så ville "the attacking state ... have the burden of showing that it did not work in tandem with the non-state cyber attacker" (Allan 2013:81). En omvendt bevisbyrde ville betyde, at Rusland blev holdt internationalt ansvarligt for de patriotiske hackergruppers omfattende cyberangreb mod henholdsvis Estland og Georgien i 2007 og 2008, medmindre russerne kunne godtgøre, at de *ikke* samarbejdede med hackerne.

Indtil videre er der imidlertid ikke nogen tegn på, at de folkeretlige principper for statsansvar er under forandring, og et internationalt ansvar forudsætter derfor også fortsat, at det kan godtgøres, at en stat som minimum udøvede effektiv kontrol med private hackere (Dinstein 1999:111; Barkham 2001-02:82). Som vi vender tilbage til i den konkluderende del af rapporten, er det da heller ikke sikkert, at en ændring af reglerne for statsansvar i sidste ende er at foretrække.

Afslutningsvis skal det med, at den manglende attribution også betyder, at det kan være umuligt at kende det eller de motiver, der ligger til grund for fjendtlige aktørers cyberoperationer. Som vi beskrev tidligere i rapporten, forudsætter vores traditionelle opfattelser af, hvad der er at anse som henholdsvis "krig", "spionage", "kriminalitet" "terrorisme" og lignende som regel viden om identiteten af den aktør, der står bag den givne aktivitet. Krig og spionage udøves af stater, mens kriminalitet og terrorisme udøves af private aktører osv. (Brenner 2007:379-475; Hunker m.fl. 2008:7-10). I fraværet af kendskab til identiteten på den fjendtlige aktør er det derfor vanskeligt at vide, hvad formålet med aktiviteten er. Det skaber bl.a. problemer, fordi det statslige beredskab over for skadevoldende aktiviteter og det retsgrundlag, der omgiver det, i høj grad er baseret på netop viden om, hvad de pågældende aktiviteter tilsigter at opnå. Krig er et anliggende for militæret og dermed for den humanitære folkeret, mens kriminalitet håndteres af det politimæssige beredskab og det dertil indrettede retsgrundlag. Og så videre. Som Duncan B. Hollis noterer sig, "If you do not know who authored an attack, how can you know whether to treat it as a crime or an act of

war? Attribution problems create serious risks of mistakes and miscalculations over *which* set of rules applies to a cyberattack or exploit." (Hollis 2011:405).

Konklusion og perspektiver

Vi har i rapporten peget på nogle udfordringer, der efter vores opfattelse rejser en række mere principielle spørgsmål om den måde, de nye trusler i cyberspace håndteres på. En af de mest centrale pointer er, at vi fortsat er i de meget tidlige stadier af forskningen i cybersikkerhed, og at der derfor også stadig er adskilligt, vi endnu ikke ved tilstrækkeligt om. Der er derfor al mulig grund til at være varsom med at drage for kategoriske konklusioner. Men tager vi udgangspunkt i, hvad vi ved, og hvad vi hidtil har set af cyberangreb, er det ikke desto mindre vores opfattelse, at debatten om cybersikkerhed indtil nu i alt for høj grad har været domineret af dommedagsprofetier og "worst case scenarier" om nedsmeltede atomreaktorer, fly, der falder ned fra himlen, og tog, der afspores. Frem for at centrere forskningen og debatten omkring de scenarier, der er sandsynlige, har megen fokus i stedet været rettet mod alle de forfærdelige ting, som man naturligvis aldrig kan udelukke vil ske, men som næppe vil. Der har med andre ord været for megen snak om en væbnet konflikt i cyberspace, som endnu aldrig har fundet sted.

Cybertruslen er naturligvis reel, og politikerne har en pligt til at sørge for, at de ansvarlige myndigheder har de beføjelser og redskaber, der er nødvendige for at kunne beskytte staten og borgerne mod de fjendtlige aktører, der hver dag lukrerer på den udstrakte grad af anonymitet, som cyberspace giver. Det er bl.a. vigtigt, at de relevante samfundsstrukturer og myndigheder opbygger den fornødne grad af modstandsdygtighed ("resilience") over for bl.a. skadelige cyberangreb. Det er også givet, at den statslige forpligtelse til at beskytte samfundet mod fjendtlige cyberaktiviteter øges i takt med, at staterne gør borgernes velfærd afhængig af netop et velfungerede cyberspace. Jo mere politikerne vil have borgerne til at benytte sig af cyberspace, jo bedre må de blive til at beskytte det. Den megen snak om cyberkrig har imidlertid efter vores opfattelse ført til en unødig og til tider uhensigtsmæssig "militarisering" af debatten om cybersikkerhed og cyberkonflikt.

Situationen for Danmark er ikke væsensforskellig fra situationen i andre højteknologiske og digitaliserede stater i den forstand, at den primære opgave for Danmark og de relevante danske myndigheder består i at identificere de mål og de sektorer, der er af særlig stor betydning, og hvis svækkelse/lammelse derfor vil være specielt problematisk. I sin seneste trusselsvurdering vurderer Center for Cybersikkerhed, at det ikke er sandsynligt, at fremmede stater vil udføre et målrettet angreb på kritisk infrastruktur i Danmark på kort til mellemlangt sigt, og det vurderes også, at

ikke-statslige aktører ikke p.t. har de fornødne kapaciteter til at udføre avancerede angreb (Forsvarets Efterretningstjeneste 2013).

Men det betyder ikke, at Danmark og danske mål ikke er truet af fjendtlige aktører i cyberspace. Især truslen fra industrispionage er betragtelig, og ifølge chefen for Center for Cybersikkerhed er store danske virksomheder som Novo Nordisk dagligt udsat for fjendtligsindede handlinger i cyberspace. Der består derfor en klar udfordring i at hindre omfattende tyveri af industrielle hemmeligheder i de højteknologiske erhvervssektorer, der må anses for at være af særlig stor betydning for Danmark, såsom sektorerne for udvikling af medicin og vindkraft.[21] Herudover er det også oplagt, at danske myndigheder skal være opmærksomme på, at der kan være særlige politikområder, hvor den danske holdning kan være af væsentlig interesse for andre stater og derfor også være et oplagt mål for andre staters spionage. Et eksempel vil være den danske Arktis-politik. Endvidere kan danske overvejelser på det militærindustrielle område tænkes at have en særlig interesse for andre stater og/eller store udenlandske virksomheder.

Som andre stater skal også Danmark og de relevante danske myndigheder og politikere være opmærksomme på, at flere af de udfordringer, som vi har beskrevet, er iboende i cyberspace, og derfor ikke komme med noget "quick fix". Et cybervåben er eksempelvis ikke som mere traditionelle våben i den fysiske verden i den forstand, at de bare kan forbydes, og handlen med dem kan standses. Det er også værd at understrege, at det langt fra er sikkert, at det er prisen værd at forsøge at løse alle de problemer, som cyberspace rejser. De mange udfordringer udspringer nemlig i høj grad af de selvsamme forhold, der er med til at gøre cyberspace til et så positivt bidrag til verden, som det er. Et konkret eksempel er de attributionsproblemer, som vi har beskrevet i rapporten, og som skaber en masse problemer af både strategisk og juridisk karakter. Hvis problemet med manglende identifikation skal forsøges afhjulpet, vil det umiddelbart kræve etablering af et system, der giver staten eksakt viden om, hvem der benytter cyberspace, og hvad disse personer foretager sig. Og det er nok de færreste, der ønsker det. Vi må heller ikke glemme, at identifikationsproblemerne i cyberspace ikke kun gavner kriminelle og fjendtlige aktører, men også dissidenter og andre, der nyder godt af anonymiteten i cyberspace til at stå op imod undertrykkende regimer. Det viser bl.a. udviklingen i de senere års revolutioner i Mellemøsten. Som Duncan B. Hollis bemærker, er "non-attribution" langt hen ad vejen "a value to be *celebrated*; it facilitates freedom of expression and protects individual privacy" (Hollis 2011: 403).

[21] Personlig samtale, april 2014.

Et andet eksempel vedrører det forhold, at det er en kilde til stor frustration, at det i praksis ofte er vanskeligt for stater at gribe ind over for de fjendtlige cyberaktiviteter, som private aktører (såsom hackere) udøver fra staternes egne territorier. Og som vi har beskrevet, er der for tiden eksperter, der advokerer for, at stater bør kunne holdes ansvarlige for alle sådanne aktiviteter. Det er naturligvis nødvendigt, at stater gør en aktiv indsats for at skride ind over for de kriminelle handlinger, der udøves fra deres territorier, men det er ikke givet, at den rigtige løsning vil være at gøre staterne ansvarlige for alle de skadevoldende cyberaktiviteter, der udøves fra deres territorier. Det vil nemlig i så fald øge staternes incitament til at overvåge borgerne og deres adfærd i cyberspace. Jo skrappere krav til staterne om effektiv "patruljering" af cyberspace, jo større vil risikoen være for statslig overvågning og registrering.

Hvilket leder os til den sidste pointe, der naturligvis også relaterer sig til den måde, som en stat som Danmark vælger at imødegå truslerne i cyberspace på. Vi har nemlig i rapporten peget på, at der fortsat er ganske stor begrebsmæssig og folkeretlig uklarhed om, hvorledes vi skal forholde os til cyber-relaterede magtmidler og de gråzoner, der eksisterer imellem de forskellige mere velkendte begreber og figurer. Og vi har også redegjort for, hvordan nogle af uklarhederne går igen på tværs af disciplinerne. Den aktuelle tvivl og mangel på klarhed nødvendiggør en mere principiel diskussion om, hvorledes vi fra dansk side bør forholde os til de nye trusler og konfliktformer i cyberspace. De mange afsløringer om omfattende kinesisk industrispionage, patriotiske hackergrupper i Rusland og NSA's spionprogrammer fordrer altså ikke blot detailprægede diskussioner om, hvorledes vi bedst imødegår de andres cyberangreb eller gør det vanskeligt at snage i vores privatliv, men i højere grad en mere principiel strategisk dansk debat om cybersikkerhed og herved også en drøftelse af, hvor grænserne bør gå mellem tilladelig og utilladelig opførsel i det nye domæne. For en ting er, hvad stater som USA og Rusland gerne vil bruge cyberspace til. Noget andet er, hvad vi vil. Hvad for et cyberspace vil vi gerne i Danmark have i fremtiden? Hvad er vores interesser, styrker og svagheder? Og hvor meget sikkerhed og velfærd er vi villige til at give køb på for at værne om et åbent og frit cyberspace?

Litteratur

Alexander, Keith (2010), *Unclassified Senate Testimony by Lt Gen Keith Alexander, Nominee for Commander of US Cyber Command*, 15 April.

Alford, Lionel D. (2010), "Cyber Warfare: The Threat to Weapon Systems", WSTIAC, Weapon Systems Technology Information Analysis Center, New York, *WASTIAC* Quarterly, Vol. 9, No. 4.

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

Arquilla, John & David Ronfeldt (1993), "Cyberwar is Coming!", *Comparative Strategy*, Vol. 12.

Arquilla, John & David Ronfeldt (1996), *The Advent of Netwar*, Santa Monica: RAND.

Axelrod, Robert & Rumen Iliev (2014), "Timing of cyber conflict ", *Proceedings of the National Academy of Sciences*, 13 January.

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

BBC News (2013), "Cyber Attacks Blamed on China", January 31st, 2013, http://www.bbc.co.uk/news/world-asia-china-21272613

Betz, David (2012), "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed", *Journal of Strategic Studies*, Vol. 35, No. 5, pp. 689-711.

Borad, William J., m.fl. (2011), "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *New York Times*, January 15

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

Brito, Jerry & Tate Watkins (2011), "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy", *Harvard National Security Journal* 3, no. 1, 39

Brodie, Bernard (1959), *Strategy in the Missile Age*, Princeton: Princeton University Press.

Bumiller, Elisabeth & Thom Shanker (2012), "Panetta Warns of Dire Threat of Cyberattack", *New York Times*, October 11.

Brøndum, Christian, "Forsvarsminister advarer mod cyberkrig", *Berlingske Tidende*, 4. maj 2012, http://www.b.dk/politiko/forsvarsminister-advarer-om-cyberkrig

Center for Militære Studier (2013), *Sikkerhedspolitisk barometer: CMS Survey 2014*, København: Center for Militære Studier.

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

Clark, David D. & Susan Landau (2011), "Untangling Attribution", *Harvard National Security Journal*, Vol. 2

Clarke, Richard & Robert K. Knake (2010), *Cyber War: The Next Threat to National Security and What To Do About It*, New York: HarperCollins Publishers.

Convention on Cybercrime, ETS no. 185 (2001)

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

Department of Defense (2011), *Cyberspace Policy Report*, Washington DC: Department of Defense.

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

Dunlap, Charles J. (2011), "Lawfare Today ... and Tomorrow", in Pedrozo, Raul A. "Pete" & Daria P. Wollschlaeger (Eds.), *International Law and the Changing Character of War*, International Law Studies (the Blue Book), Vol. 87, Naval War College, Newport, 315.

Eriksson, Johan & Giampiero Giacomello (2006), "The Information Revolution, Security, and International Relations: (IR)relevant Theory?", *International Political Science Review*, Vol. 27, No. 3, 221.

Farwell, James P. & Rafal Rohozinski (2011), "Stuxnet and the Future of Cyber War", *Survival*, Vol. 53, No. 1, 23.

Fearon, James (1995), "Rationalists Explanations for War", *International Organization*, Vol. 49, No. 3.

Forsvarets Efterretningstjeneste, Efterretningsmæssig Risikovurdering 2013, http://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2013.pdf

Freedman, Lawrence (2004), *Deterrence*, Cambridge: Polity Press.

Gartzke, Erik (2013), "The Myth of Cyberwar": Bringing War in Cyberspace Down to Earth", *International Security,* Vol. 38, No. 2, 41

German Federal Ministry of the Interior (2011), *Cyber Security Strategy for Germany*, Berlin: German Federal Ministry of the Interior.

Glaser, Charles L. & Chaim Kaufmann (1998), "What is the Offense-Defense Balance? And Can We Measure it?", *International Security*, Vol. 22, No. 4, 44

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

Gray, Colin S. (2005), *Another Bloody Century: Future Warfare*, London: Weidenfeld & Nicolson.

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

Henriksen, Anders (2014), *Folkeretten og modreaktioner i cyberspace*, Center for Militære Studier

Henriksen, Anders (2013), "Jura som Strategi og Danmark i krig", i Kristian Søby Kristensen, *Danmark i Krig*, Jurist- og Økonomforbundets Forlag, s. 133

Henriksen, Anders & Jens Ringsmose (2013), "Dronerne er her! Strategiske, retlige og etiske konsekvenser", Dansk Institut for Internationale Studier

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

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

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

Hughes, Rex (2010), "A treaty for cyberspace", *International Affairs*, Vol. 86, no. 2, 523.

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

International Court of Justice (ICJ), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA)*, Judgment, ICJ Rep. (1986) 14

International Court of Justice (ICJ), *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, ICJ Rep. (2007) 43

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

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

Junio, Timothy J. (2013I), "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate", *Journal of Strategic Studies*, Vol. 36, No. 1, 125.

Junio, Tim (2013II), "More Shots Fired on the Cyber Front: Key Takeaways from Operation Troy", *Huffington Post* (7. November) available at http://www.huffingtonpost.com/tim-junio/operation-troy-cybersecurity_b_3582308.html (besøgt 12. december 2013)

Kello, Lucas (2013), "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, Vol. 38, No. 2, 7.

Kessing, Peter Vedel (2013), "Våbendroner – likvidering eller legitim magtudøvelse? (Armed drones – assassination or legitimate use of force?"*), EU-ret & Menneskeret,* Nr. 2, maj, 59

Kjær, Jakob Sorgenfri (2013), "Danmark bagud på it-sikkerhed i Europa", *politiken.dk*, 22. december, http://politiken.dk/indland/ECE2166430/danmark-bagud-paa-it-sikkerhed-i-europa/.

Knake, Robert K. (2010), "Untangling Attribution: Moving to Accountability in Cyberspace", Prepared Statement before the Subcommittee on Technology and Innovation, Committee on Science and Technology, Hearing: Planning for the Future of Cyber Attack.

Kuehl, Daniel T. (2009), "From Cyberspace to Cyberpower: Defining the problem", in Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz (eds), *Cyberpower and National Security*, Washington D.C.: National Defense University Press.

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

Lambeth, Benjamin (2011), "Airpower, Spacepower and Cyberpower", *Joint Force Quarterly*, issue 60, 1st quarter.

Langø, Hans-Inge (2013a), "Slaying the Cyber Dragons: Competing Academic Approaches to Cyber Security", *NUPI Working Paper 820*, Oslo: NUPI:

Langø, Hans-Inge (2013b), "Cyberspace og sikkerthet", *Internasjonal Politikk*, Årg. 71, Nr. 2, 221.

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

Lewis, James A. (2010), *Thresholds for Cyberwar*, Center for Strategic and International Studies, http://csis.org/publication/thresholds-cyberwar.

Libicki, Martin C. (2007), *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge UK: Cambridge University Press.

Libicki, Martin C. (2009), *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Cooperation.

Liebertahl, Kenneth & Peter W. Singer (2012), *Cybersecurity and U.S.-China Relations*, Washington DC: Brookings Institution.

Liff, Adam P. (2012), "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies*, Vol. 35, No. 3.

Lindsay, Jon R (2013), "Stuxnet and the Limits of Cyber Warfare", *Security Studies*, Vol. 22, 365.

Lynn, William J. (2010), "Defending a New Domain: The Pentagon's Cyberstrategy", *Foreign Affairs*, Vol. 89, No. 5, 97.

Maurer, Tim (2011), "The Case for Cyberwarfare", *Foreign Policy*, October 19, http://wwwforeignpolicy.com/articles/2011/10/19/the_case_for_cyberwar.

McGraw, Gary (2013), "Cyber War is Inevitable (Unless we Build Security In)", *Journal of Strategic Studies*, Vol. 36, No.1, 109.

Mearsheimer, John J. (1983), *Conventional Deterrence*, Ithaca: Cornell University Press.

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

Nuzzo, Regina (2014), "The best time to wage cyberwar", *nature.com*, January 13.

Manyika, James & Charles Roxburgh (2011), "The great transformer: The impact of the Internet on economic growth and prosperity", *McKinsey Global Institute*. http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_transformer.

Obama, Barack (2012), "Taking the Cyberthreat Seriously", *Wall Street Journal*, 19. juli.

Poulsen, Lasse Hedegaard (2013), "Center for Cybersikkerhed: Danmark er potentielt strategisk mål", *version2.dk*, 5. november, http://www.version2.dk/artikel/center-cybersikkerhed-danmark-er-et-potentielt-strategisk-maal-54798.

Rattray, Gregory J. (2001), *Strategic Warfare in Cyberspace*, Cambridge, MIT Press.

Rid, Thomas (2012), "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1, pp. 5-32.

Rid, Thomas (2013), *Cyber War Will Not Take Place*, Oxford: Oxford University Press.

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

Samaan, Jean Loup (2010), "Cyber Command: The Rift in US Military Cyber-Strategy", *The RUSI Journal* 155, no. 6, pp. 16-21.

Sanger, David E. & Mark Mazetti (2007), 'Israel Struck Syrian Nuclear Project, Analysts Say', *New York Times*, October 14.

Sanger, David E. (2012), Obama Order Sped Up Wave of Cyberattacks Against Iran', *New York Times*, June 1.

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

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

Schmitt, Michael N. (2011), 'Cyber Operations and the Jus ad Bellum Revisited', *Vilanova Law Review*, Vol. 56, 569.

Schreier, Fred (2012), *On Cyberwarfare*, Geneva: The Geneva Centre for the Democratic Control of Armed Forces, Horizon 2015, Working Paper no. 7.

Sherstobitoff, Ryan, m.fl. (2013), *Dissecting Operation Troy: Cyberespionage in South Korea*, McAfee Labs, White Paper

Shirky, Clay (2011), "The Political Power of Social Media", *Foreign Affairs* 90/1.

Sifry, Micah (2011), *Wikileaks and the Age of Transparency*, New York: OR Books.

Snyder, Glenn (1961), *Deterrence and Defense: Toward a Theory of National Security*, Princeton: Princeton University Press.

Stark, Holger (2011), 'Mossad's Miracle Weapon, Stuxnet Virus Opens New Era of Cyber War', *Der Spiegel*, 8. august

Steen-Johnsen, Kari, Bernard Enjolras & Dag Wollebæk (2013), "Sosiale medier, samfunnspolitisk deltagelse og kontroll", *Internasjonal Politikk*, Årg. 71, Nr. 2, 263-73.

Stone, John (2013), "Cyber War *Will* Take Place!", *Journal of Strategic Studies*, Vol. 36, No. 1, pp. 101-108.

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

Traynor, Ian (2007), "Russia Accused of Unleashing Cyberwar to Disable Estonia", *The Guardian*, 17, maj, http://www.theguardian.com/world/2007/may/17/topstories3.russia

Trias, Eric D. & Bryan M. Bell (2010), "Cyber This, Cyber That... So What?", *Air & Space Journal*, Vol. XXIV, No. 1.

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

UK MOD (2011), *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, London: UK MOD.

Van Evera, Stephen (1984), "The Cult of the Offensive and the Origins of the First World War", *International Security*, Vol. 9, No. 1.

Walt, Stephen M. (2010), "Is the Cyber Threat Overblown?", *Foreign Policy*, March 30. http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.

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