Internasjonal POLITIKK Årgang 71 | Nr. 2 | 2013 | 252–262 | ISSN 0020-577X

FOKUS: CYBERSPACE

Cyberkrig og internasjonal rett

KRISTIN BERGTORA SANDVIK
S.J.D., seniorforsker, PRIO
bergtora@prio.no

Problematikken rundt cybersikkerhet stiller nasjonale myndigheter og det internasjonale samfunnet overfor store lovtekniske utfordringer, enten man snakker om handlinger som hactivisme, cyberkriminalitet, cyberterrorisme eller cyberkrigføring.

Med utgangspunkt i det siste problemkomplekset belyser dette bidraget forholdet mellom cybersikkerhet og juss gjennom en bredt anlagt diskusjon av den rettslige reguleringen av cyberkrigføring. Bidraget ser på hvordan cybersikkerhet har gått fra å være et datasikkerhetsproblem til å bli et militært anliggende og et spørsmål om krigføring, og hvilken rolle rettsliggjøring og rettslige instrumenter spiller i denne prosessen. Hvordan kan stater stilles til ansvar for cyberangrep?

Stadig flere land anerkjenner cyberangrep som en grunnleggende trussel mot nasjonal sikkerhet. Ved å utnytte sårbarheter i kritisk informasjonsinfrastruktur spesielt og i IKT-systemer generelt, kan en angriper penetrere, forstyrre, frakoble, stjele eller ødelegge kommunikasjonslinjer, informasjon eller operativsystemene på datamaskiner og nettverk. Den følgende diskusjonen tar utgangspunkt i angrepene som befinner seg i gråsonen mellom kriminelle handlinger og krigshandlinger, og hvor angriperen kan inneha flere roller samtidig: han eller hun kan være en såkalt «black hat» hacker – en patriotisk hacker – og samtidig jobbe på direkte oppdrag fra en statsmakt.

Hvorvidt et cyberangrep defineres som økonomisk eller militært motivert, avhenger av hvor omfattende og sofistikert angrepet er, men også av geopolitiske betraktninger, av de strategiske ressursene til landet som blir angrepet, og av hvem aggressoren antas å være. Internasjonal rett har ingen definisjon av cyberkrigføring, og det er dype uenigheter om hvilke type angrep som kan betegnes som cyberangrep: hvordan det begynner, hvordan slike angrep ender, hva slags engasjementsregler som bør gjelde

eller hvilke krav som bør være oppfylt for at slike angrep skal være lovlige under internasjonal rett.

Denne oversiktsartikkelen ser på noen av de rettslige utfordringene som oppstår i kjølvannet av nasjonale og internasjonale forsøk på å forebygge, regulere og bilegge cyberkrigføring. Samtidig som cyberdomenet gradvis anerkjennes som en femte krigføringsarena,[1] har både beslutningstakere og offentligheten utilstrekkelig kunnskap om de rettslige konsekvensene av denne utviklingen. Det hersker uenighet med hensyn til hvordan man skal forstå konkrete hendelser og når det gjelder utformingen av et begrepsapparat for å beskrive hendelsene. Dette bidraget ser det derfor som hensiktsmessig å diskutere reguleringen av cyberkrig i både et rettssosiologisk og i et rettsdogmatisk perspektiv.

Internasjonal lov om maktbruk og krigens folkerett er hjørnesteinene i arbeidet for å utvikle et rammeverk for å regulere cyberangrep som en trussel mot nasjonal og internasjonal sikkerhet. For å kunne slå fast når cyberkrig er «krig», er det behov for å avklare hva slags maktbruk cyberangrep utgjør og hvilke hendelser som utløser retten til selvforsvar. Mens det er viktig og nødvendig å pensle ut hvilke juridiske normsett som skal anvendes og hvordan, har dette tolkingstekniske arbeidet også viktige strategiske og politiske sider: hvordan og hvorfor er cybersikkerhetsproblematikk blitt til en diskusjon om krigføring, med alle de utenriks- og forsvarspolitiske følgene det medfører? Viktige forsvarspolitiske, militære og økonomiske interesser på spill, og mange aktører står med én fot i statsforvaltningen og én fot i det private næringsliv. Man må her se på samspillet mellom rettslige normer, geopolitiske begivenheter og cyberkrigdiskursen som føres av sikkerhetseksperter og det voksende militær-industrielle «cyberkomplekset». Denne debatten preges av forsøk fra militære, politiske og kommersielle aktører på å flytte cybersikkerhetsproblematikken over i krigføringsdomenet.

Artikkelen konkluderer med at militariseringen av cyberspace har skapt et behov for å fremme en «cyberfred»-agenda. Mens det er viktig at normene for å bruke lov om væpnet konflikt er klare, dekker disse normene bare en liten del av cybersikkerhetsutfordringen: mer oppmerksomhet bør gis til manglende beskyttelse av kritisk infrastruktur og koordinering av nasjonale rettslige rammeverk.

Cyberspace som sikkerhetsutfordring

Globaliseringen av IKT medfører sikkerhetsutfordringer på nasjonalt og internasjonalt nivå. For det første har informasjonsinfrastruktur slik som

1. De øvrige er land, luft, sjø og det ytre rom.

Verdensveven og kontrollromsystemet SCADA[2] blitt sentrale for kritisk infrastruktur, og dermed avgjørende for å ivareta økonomi og samfunnssikkerhet og nasjonal sikkerhet. Denne infrastrukturen er svært sårbar og preget av en dynamikk som gjør det utfordrende å regulere cybersikkerhet: privat eierskap gjør at profittmotiv fortrenger investeringer i effektive sikkerhetstiltak, samtidig som offentlige myndigheter ikke i tilstrekkelig grad deler viktig informasjon med private aktører og ofte mangler både kompetanse og en klar ansvarsstruktur for å håndtere cybersikkerhetsproblematikk (Dunn Cavelty 2007).

Et nytt digitalt landskap vokser frem som en konsekvens av at maskinvare og programvare blir mer avansert, mer tilgjengelig og i større grad sosialt og kulturelt integrert i folks dagligliv. Massemobiliseringer organisert gjennom sosiale media og utbredelsen av grasrot-hactivisme har ført til uro både hos demokratisk valgte styresmakter og autoritære regimer. Som et mottrekk til bruken av cyberspace som arena i kampen for frihet, makt eller profitt fester nå nasjonale myndigheter grepet om cyberspace med rettslig regulering som et sentralt virkemiddel: Cyberspace er verken grenseløst eller lovløst. Cybersikkerhet reguleres i dag av en mengde nasjonale og internasjonale instrumenter, innbefattet datalovgivning, menneskerettigheter, strafferett, sikkerhetslovgivning, krigens folkerett og stadig mer cyber-spesifikke standarder og normer som Europarådets konvensjon om cyberkriminalitet fra 2001.

Videre er det et faktum at den økende frekvensen av alvorlige cyberangrep rettet mot internasjonale organisasjoner, multinasjonale selskaper og nasjonalstater gjør stor skade. Angripernes identitet er ofte uklar, deres motiver likeså. Kompliserte jurisdiksjonsspørsmål hindrer effektiv rettshåndheving. Styresmaktene må forholde seg til en cyber-underverden befolket av tenåringer, dataeksperter, profesjonelle hackere, organiserte kriminelle, hactivister, spioner og i økende grad fremmede makters cyberkrigere.

Rettsliggjøringen av cybersikkerhet og cyberkrig

Som en følge av at cyberkrigføring har kommet på den internasjonale agendaen, har spørsmålet om rettslig regulering blitt viktig. Sentralt i den pågående debatten er ideen om at nasjonal sikkerhet er truet på grunn av utilfredsstillende infrastruktur, finansiering, personellkapasitet, nasjonale retningslinjer og nasjonale og internasjonale rettslige rammeverk. Manglende rettslig regulering av mellomstatlige samkvem i cyberspace og

2. SCADA er en forkortelse for Supervisory Control and Data Acquisition, som er et kontrollromsystem for infrastruktur og industri.

av forpliktelser til å satse på cybersikkerhet blir i seg selv en form for sårbarhet som utgjør en trussel både mot nasjonal sikkerhet og mot verdensfreden.

Cybersikkerhet blir nå institusjonalisert relativt hurtig på et internasjonalt nivå, i FN så vel som i NATO og EU. FN-prosessen følger i hovedsak to spor: et økonomisk spor hvor cyberkriminalitet står sentralt, og en politisk-militær tilnærming som fokuserer på cyberkrigføring (Maurer 2011). Denne normproduksjonen er i stor grad preget av kulturkonflikt: Siden slutten av 1990-tallet har Russland og de andre medlemslandene i Shanghai Cooperation Organization (SCO) ønsket en internasjonal avtale for å regulere cybersikkerhet. I 2011 lanserte SCO forslag om retningslinjer for internett på FNs generalforsamling. Dette ble avvist. Støttet av Russland og andre forsøkte den internasjonale telekommunikasjonsunionen (ITU) i 2012 å utvide det internasjonale rammeverket for telekommunikasjon til å omfatte internett. Forsøket mislyktes fordi vestlige land og privat sektor anklaget ITU og land som Russland og Kina for å forsøke å ta kontroll over styringen av internett (Kruger 2013). Som svar på cyberangrepet på Estland 2007,[3] vedtok NATO å sette opp sitt «Cooperative Cyber Defense Center of Excellence» i Tallin (CCDCOE). Både deklarasjonen fra Lisboatoppmøtet i 2010 og NATOS strategiske konsept fra 2010 vektlegger cyberforsvar som en grunnleggende del av NATOs oppgaver (selv om cyberangrep antas ikke å utløse artikkel 5-forpliktelser). NATOs første offisielle cyberretningslinjer kom i 2011.

En ytterligere faktor som spiller inn er fremveksten av et cybersikkerhetsindustrielt kompleks. Den store veksten hos transnasjonale IT-selskaper som Symantec og MacAfee er delvis basert på den faktiske økningen i cyberangrep, men har også sitt utspring i cybertrussel-vurderingene produsert av de samme selskapene. Tradisjonelle leverandører av forsvarsmateriell som Northrop Grumman investerer nå tungt i informasjonssikkerhet. Statlige myndigheter og internasjonale organisasjoner må forholde seg til industriens aktive forsøk på å påvirke den rettslige reguleringen og definisjonen av cybersikkerhet og cyberkrigføring.

Sist, men ikke minst kan behovet for rettsliggjøring forklares ved å peke på selve institusjonaliseringen av cyberkrigføring. Stadig flere land sier at de har eller har planer om å anskaffe militære cyberkrigføringsenheter – den mest kjente så langt er den amerikanske U.S. Cyber Command som ble stiftet i mai 2010. Ansvarsområdene til disse institusjonene må være klart avgrenset, og det er behov for operasjonelle regler som er avpasset til resten av rettssystemet.

3. Angrepet kom etter at estiske myndighetene hadde vedtatt å fjerne krigsmonumentet «Bronsesoldaten i Tallin». Det er antatt at russiske hackere stod bak, med støtte fra russiske myndigheter.

Hvilken rolle spiller jussen i cyberkrigdiskursen?

Begrepet «cyberkrig» anvendes ofte i metaforisk øyemed, og manglende presisjon i begrepsapparatet for å beskrive cyberkonflikt leder ofte til overdrivelser. For å sitere sikkerhetsekspert Bruce Schneier: «words have meaning, and metaphors matter ... if we accept the military's expansive cyberspace definition of 'war', we feed our fears» (Schneier 2010). Det er derfor nødvendig å rette et kritisk blikk mot hvordan retten bidrar til å opprettholde en diskurs hvor cyberangrep sees som trusler mot nasjonal og internasjonal sikkerhet, og hvor lov om maktbruk og krigens folkerett vektlegges som passende rettslige rammeverk.

Rettsliggjøring skaper tiltrengt legitimitet for en militariseringsprosess: I en kontekst hvor tap av menneskeliv har vært fraværende i de to kjente tilfellene av «cyberkrig», Estland og Georgia[4] (hvor vanlig militær styrke medførte sivile tap), og hvor territorial-dimensjonen som er så sentral for tradisjonelle rettslige definisjoner av krig og slagmark mangler, har kommentatorer uttrykt skepsis til hvorvidt «krigføring» er en passende betegnelse for å beskrive følgene av cyberangrep. Den nye *Manualen for internasjonal rett og cyberkrig* (2012), den såkalte Tallin-manualen, er det godt eksempel: Manualen er utviklet av en gruppe nordamerikanske og europeiske juridiske eksperter. Manualen er ikke rettslig bindende, men vil over tid kunne oppnå status som internasjonal sedvanerett. I denne sammenhengen kan det argumenteres med at en slik fremstilling av cyberkrig som et passende emne for krigens folkerett og nasjonal sikkerhetslovgivning blir prognostisk: Det politiske fokuset blir da rettet mot å regulere militære løsninger og å trekke opp de rettslige grensene for de spesifikke strategiene, taktikkene og formålene hvorpå militære løsninger oppnås.

Et dominerende trekk ved cyberdiskursen er utbredelsen av cyber-dommedags scenarier, eller «cybergeddons». Ser vi på amerikanske debatter, er det merkelapper som «et digitalt Pearl Harbour», «cyber 9/11», «eWMD» (elektroniske masseødeleggelsesvåpen) eller «cyber-Katharina» (se Lawson 2011). Dommedagsprofetiene fremføres i stor grad av en gruppe «cyberhauker», eksperter i den private sektor som forsøker å skaffe seg kontrakter med amerikanske myndigheter og andre. I deres billedspråk er vestlige land og NATO utilstrekkelig forberedt på en cyberkrig mot Russland, Kina, Nord-Korea og andre fiendtlige makter. Krav om å anvende loven om væpnet konflikt og/eller et nytt cyber-spesifikt instrument er ofte en del av et mer generelt krav om at myndighetene må innta en tøffere holdning til antatte motstandere, integrere satsing på cyberkrig i

4. Forut for den militære konflikten mellom Georgia og Russland over Sør-Ossetia i august 2008, ble Georgia utsatt for et massivt cyberangrep.

den nasjonale sikkerhetsinfrastrukturen og vedta videre budsjettrammer for defensiv og offensiv cyberkapasitet (se Clarke & Knake 2010).

En annen tilnærming avviser disse kravene som en militarisering av cyberspace: cyberkrig er ikke virkelig «krig» – cyberangrep er ikke voldsutøvelse, og ingen blir drept. Fordi cyberkrig i realiteten er et datasikkerhetsproblem, bør ikke krigens folkerett komme til anvendelse (se Rid 2012). En tredje, pragmatisk tilnærming aksepterer at enkelte cyberhendelser utgjør nasjonale sikkerhetstrusler. Uansett merkelapper er cybertrusler virkelige, og ulike cyberverktøy og -teknikker blir i økende grad viktige i internasjonale konflikter. Denne tilnærmingen fokuserer på viktigheten av å beskytte kritisk informasjonsinfrastruktur ved å fokusere på robusthet. Robusthet oppnås ved å bruke både menneskelige og teknologiske ressurser for å forebygge, motstå, absorbere og mitigere angrep. Det som behøves er en bredt anlagt rettslig strategi som inkluderer, men ikke er begrenset til krigens folkerett (Tikk 2011).

Det rettsdogmatiske perspektivet

I den følgende drøftingen tas både eksistensen av cyberkrig og behovet for å regulere den for gitt. Cyberkrigføringsdiskursens begynnelse kan spores tilbake til begynnelsen av 1990 tallet, hvor cyberkrig ble kategorisert som en av flere typer informasjonskrigføring. Mens samfunnsdiskursen generelt var preget av en forestilling om at man befant seg «i informasjonsalderen», var militær strategi dominert av tenkningen rundt revolusjonen i militære affærer – RMA.

Mens ideen om cyberkrig i en kort tidsperiode etter 11. september 2011 ble utkonkurrert av en forestilling om «cyberterror», tyder utbredelsen av cyberkrigføringsretorikken siden 2007–08 på en militarisering av cyberspace og cybersikkerhetstemaer. Forsøkene på å komme til enighet om funksjonelle normer har vært hindret av at det mangler en definisjon av cyberkrig. For vide eller for snevre definisjoner skaper utfordringer med henblikk på arbeidsfordelingen mellom sivile og militære domener, mellom myndighetene og den private sektor, og mellom nasjonale myndigheter og internasjonale organisasjoner. Samtidig må en definisjon av cyberkrig være knyttet til en praktisk forståelse av hva slags rolle cyberangrep kan spille i en væpnet konflikt, enten cyberangrepet er en forløper for konvensjonelle angrep eller cyberangrepet i seg selv utgjør et væpnet angrep.

Siden begynnelsen har det eksistert en spenning mellom en holdning om at cyberkrig simpelthen er for vanskelig å regulere, en forståelse av cyberkrigføring som en ny type konflikt hvor nye rettslige instrument er påkrevd, og en oppfatning av at cyberkrigføring dekkes godt nok av eksisterende regelsett. Den siste tilnærmingen har bredest støtte blant jurister

og akademikere. Neste avsnitt tar for seg de viktigste diskusjonstemaene under lov om maktbruk og krigens folkerett.

Lov om maktbruk

Lov om maktbruk, den såkalte *jus ad bellum*, gjelder bruk av makt under FN-charteret. Generelt er tolkingen av jus ad bellum preget av mellomstatlig uenighet, ujevne maktforhold og strategiske prioriteringer. Hvorvidt politiske aktører støtter strenge eller mer liberale tolkningsalternativer, avhenger også av om maktbruken gjelder militære eller sivile sfærer. En anvendelse av dette normsettet på cyberkonflikt må balansere hensyn til jurisdiksjon, statssuverenitet og maktbruk.

Mens kommentatorene stort sett er enige om at cyberangrep kan representere forbudt maktbruk under artikkel 2(4), er nivåene for *når* et cyberangrep utgjør maktbruk, fremdeles omdiskutert. Tre alternativer har vært diskutert: den første tilnærmingen går ut på at man ser på hva slags instrument som er brukt ved angrepet og at man foretar en konkret vurdering av om ødeleggelsene tilsvarer ødeleggelser som følger av konvensjonell, kinetisk maktbruk. Den andre tilnærmingen definerer alle cyberangrep mot kritisk infrastruktur som væpnede angrep. En tredje tilnærming ser på de samlede konsekvensene for staten som er blitt angrepet. Vurderingen blir relativt enkel i de tilfellene hvor cyberangrepet har resultert i fysisk ødeleggelse, personskade eller død, men komplisert i de tilfellene hvor skadevirkningene er indirekte og årsakssammenhengene vanskelige å etablere.

Et annet uavklart tema er spørsmålet om når en stat kan iverksette selvforsvar under artikkel 51 som reaksjon på cyberangrep som tilsvarer et væpnet angrep. Tradisjonelt sett har det å anse handlinger som væpnede angrep som utløser rett til selvforsvar under artikkel 51, hatt avskrekkende virkning. Men når dataangrep øker sterkt i omfang, vil en vid adgang til maktbruk som undergraver begrensninger på militære reaksjoner på ikkemilitære ødeleggelser, skape større usikkerhet i det internasjonale systemet. Derfor, jo høyere terskelen er for å tillate selvforsvar, dess mindre er sjansene for å eskalere maktbruk. Selvforsvaret må være «nødvendig» og «proporsjonalt». Videre diskuteres det hva som bør være de spesifikke vilkårene for å tilskrive en aktør ansvar for angrep på stat, og når en stat blir ansvarlig for angrep foretatt av tredjepart fra statens territorium. Under internasjonal rett har statene forpliktet seg til å hindre at deres territorium brukes som base for angrep. Statene er forpliktet til å vedta og implementere cyber-relevant straffelovgivning, og å samarbeide med den angrepne stats etterforskning av angrepet.

Fra et rettsdogmatisk perspektiv gjenstår en rekke uavklarte spørsmål: er det eksisterende rammeverket i stand til å skille mellom ulike aktiviteter som cyberspionasje og nettverksangrep som krysser terskelen for å utgjøre «væpnede angrep»? Hva er sannsynligheten for å oppnå internasjonal enighet om tolknings- og implementeringsspørsmål når stater oppfatter cybertrusler ulikt og foretar ulike skiller mellom hva som teller som offensive og defensive tiltak? Vil noen stater foretrekke å gjemme seg bak rettslig uklarhet?

Krigens folkerett

Krigens folkerett, eller *jus in bello*, regulerer slags handlinger som er tillatt under kamphandlinger. Reglene som anvendes på cyberkrigføring fins hovedsakelig i tilleggsprotokoll I for beskyttelse av ofre for internasjonale væpnede konflikter fra 1977 (del V som gjelder sivilbefolkningen), og lov om nøytralitet slik den er kodifisert i 1907 Haag-konvensjonen. Mens fortolkningsspørsmål gjenstår, er det generell enighet blant kommentatorer om at dette normsettet kan anvendes på cyberkrigføring.

Mye energi har vært brukt på å trekke opp et skille mellom militære og sivile sfærer: Hvem er beskyttet mot cyberangrep og hvem kan angripes, og hvordan skjer overgangen mellom de to kategoriene? Hvem kan lovlig delta i kamphandlinger? Hva slags beskyttelse har sivilister, f.eks. datateknikere, som deltar i kamphandlinger – når blir de legitime mål? En annen gruppe spørsmål gjelder hvilke objekt som kan angripes: mens det er forbudt å angripe infrastruktur, gjenstander o.l. som er nødvendige for sivilbefolkningens overlevelse (strømnett, drikkevannskilder), er det uklart hva som skjer med objekt som er i både sivil og militær anvendelse.

Det er dessuten begrensning på hvilke midler og metoder cyberangrep kan benytte for å være lovlige. Angrep må være proporsjonale, nødvendige og avgrensede. Foranstaltninger må være tatt for å sikre at angrepet ikke forårsaker unødig sivil lidelse. Militær vinning må være større enn skaden for sivilsamfunnet. Viktig er også forbudet mot svik og bedrag: det er forbud mot å seile under falskt flagg ved f.eks. å late som om man er sivilist eller tilhører Røde Kors. Endelig har nøytrale stater en rett på immunitet fra angrep, men er forpliktet til ikke å la eget territorium misbrukes i angrepsøyemed av tredjepart.

Manualen for internasjonal rett og cyberkrig, den såkalte Tallin-manualen fra 2012, er et forsøk på å klarlegge disse normene. Imidlertid viderefører manualen flere uklarheter med hensyn til hva som utgjør et væpnet angrep, og hva slags status som skal gis til personell involvert i cyberangrep.

Konklusjon

Formålet med dette bidraget har vært todelt: først, å undersøke hvilken rolle rettsliggjøring og rettslige instrumenter har spilt i dannelsen av begrepet «cyberkrigføring», og dernest å presentere de hovedspørsmålene som oppstår under internasjonal lov om maktbruk og krigens folkerett. Tre observasjoner har særskilt relevans for politiske beslutningstagere på nasjonalt nivå: for det første, mens diskusjoner rundt rettslige tvilsspørsmål er viktige og nyttige, er de også strategiske og politiske. Mange av de utfordringene som oppstår i forbindelse med cyberkrigføring er ikke først og fremst av rettslig natur: sterke militære, politiske og kommersielle interesser ønsker å fremme en forståelse av cybersikkerhetsutfordringer som «cyberkrig». Mens enkelte kommentatorer argumenterer for at en dreining mot krigføring i cyberspace medfører at sivile oftere blir mål, har andre begynt å argumentere for at cyberkrigføring vil lede til en mer human form for krigføring og at internasjonal rett bør tilpasse seg og fremme cyberkrigføring som et alternativ til tradisjonell krigføring.

Denne utviklingen kan også bidra til å skape større statlig og militær kontroll over sivile nettverk, noe som kan være problematisk ut fra hensynet til privatlivets fred og andre sentrale politiske og sosiale menneskerettigheter. Et generelt problem er at juriststanden mangler tilstrekkelig med vitenskapelige og tekniske ferdigheter til å analysere de rettslige konsekvensene av den teknologiske utviklingen. I tillegg er forskning på cyberkrigføring ofte hemmeligstemplet og utilgjengelig.

For det andre kan fokuset på cyberkrig som en trussel mot nasjonal sikkerhet og internasjonal fred lede til at løsningen på cybersikkerhetsproblemer ikke blir klarlagt tilstrekkelig. Internasjonal rett kan tilby et rettslig rammeverk for en sentral, men like fullt begrenset del av utfordringene knyttet til cybersikkerhet: utilstrekkelig beskyttelse av kritisk informasjonsinfrastruktur og utilfredsstillende koordinering av nasjonale regimer diskuteres fremdeles i for liten grad av beslutningstagere i de aller fleste jurisdiksjoner. Den tilnærmingen som betegnes som en «helhetlig rettslig tilnærming», med sitt fokus på å koordinere ulike samfunnsområder som informasjonssamfunnet og telekommunikasjon, cyberkriminalitet, nasjonal sikkerhet og væpnet konflikt, er lovende. Denne tilnærmingen innebærer å anvende flere ulike rettslige instrumenter samtidig, inkludert lov om væpnet konflikt, for å kombinere trusselvurderinger, avskrekking og tilsvar fra ulike myndigheter. Ved å argumentere for en slik tilnærming kan også militære ledere kreve mer proaktive holdninger fra statlige myndigheter og privat sektor. Det er viktig å merke seg at denne tilnærmingen indirekte utfordrer fokuset på krig som et hovedtema for cybersikkerhetsdiskurs.

For det tredje nødvendiggjør militariseringen av cyberspace et større fokus på hvordan man kan fremme en «cyberfred»-agenda på utenrikspolitisk nivå. Det foreslås avslutningsvis at cyberfred kan fremmes ved å frakoble cybersikkerhet fra væpnet makt, og ved å innføre en høy rettslig terskel for å behandle disse som likeverdige. Samtidig bør ikke en slik «cyberfred» bare behandles ved negative definisjoner: diplomatiet og det utenrikspolitiske juristkorpset må gi mer oppmerksomhet til rollen internasjonal rett kan spille i utviklingen av en substansiell «cyberfred»-agenda (Wegener 2011).

Om bidraget

Bidraget er basert på rapporten *Towards a Militarization of Cyberspace? Cyberwar as an Issue of International Law*, fra det pågående prosjektet «Regulating Cyberwar: Understanding Challenges to Norwegian Security and International Law» (finansiert av Forsvarsdepartementet, 2011–2014).

Litteratur

Clarke, Richard & Robert Knake (2010) *Cyber War: The Next Threat to National Security and What to Do About it*. New York: Ecco.

Council of Europe (2001) Convention on Cybercrime of the Council of Europe. Tilgjengelig på: http://conventions.coe.int/Treaty/Commun/QueVoulez-Vous.asp?NT=185&CM=8&DF=&CL=ENG. Lesedato 18.01.2013.

Dunn Cavelty, Myriam (2007) Critical information infrastructure: Vulnerabilities, threats and responses. *Disarmament Forum ICTs and International Security*, (3): 15–22.

Kruger, Lennard G. (2013) Internet Governance and the Domain Name System: Issues for Congress, Congressional Research Service 7-5700 www.crs.gov R42351. Tilgjengelig på: www.fas.org/sgp/crs/misc/R42351.pdf. Lesedato 18.01.2013.

Lawson, Sean (2011) Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History. *Mercatus Center Working Paper*, 10 (77). Tilgjengelig på: http://mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidencehistory_1.pdf. Lesedato 18.01.2013.

Maurer, Tim (2011) Cyber norm emergence at the United Nations – An Analysis of the Activities at the UN Regarding Cyber-Security. *Explorations in Cyber International Relations Discussion Paper Series*. Tilgjengelig på: http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf. Lesedato 18.01.2013.

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). (Opprettet 2008) Tilgjengelig på: https://www.ccdcoe.org/ Lesedato 18.01.2013.

NATO Policy on Cyber Defence (2011). Tilgjengelig på: www.nato.int/nato_static/assets/pdf/pdf_2011_09/20111004_110914-policy-cyberdefence.pdf. Lesedato 18.01.2013.

NATO, Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation (2010). Tilgjengelig på: www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf. Lesedato 18.01.2013.

NATO Lisbon Summit Declaration (2010). Tilgjengelig på: www.nato.int/cps/en/natolive/official_texts_68828.htm. Lesedato 18.01.2013.

Rid, Thomas (2012) Cyber War Will Not Take Place. *Journal of Strategic Studies, 35* (1):5–32.

Schneier, Bruce (2010) *Threat of «Cyberwar» Has Been Hugely Hyped.* 07.07. Tilgjengelig på: www.schneier.com/essay-320.html. Lesedato 18.01.2013.

The Tallinn Manual on the International Law Applicable to Cyber Warfare (2012) Tilgjengelig på: www.ccdcoe.org/249.html. Lesedato 18.01.2013.

Tikk, Eneken (2011) *Comprehensive Legal Approach to Cyber Security.* PhD Dissertation, Tartu University Press. Tilgjengelig på: http://dspace.utlib.ee/dspace/bitstream/handle/10062/17914/tikk_eneken.pdf?sequence=1, Lesedato 18.01.2013.

Wegener, Henning (2011) Cyber Peace, in *The Quest for Cyber Peace,* International Telecommunication Union and World Federation of Scientists. Tilgjengelig på: www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf. Lesedato 18.01.2013.