Internasjonal POLITIKK
Årgang 74 | Nr. 4 | 2016 | ISSN 1891-5580

Fagfellevurdert artikkel

Makt og avmakt i cyberspace: hvordan styre det digitale rom?

Lilly Pijnenburg Muller*,
Norsk utenrikspolitisk institutt, Oslo, Norge

Et sikkert cyberspace er nødvendig for en fungerende samfunnsstruktur, økonomisk, politisk og sosialt. Med samfunnets økende avhengighet av cyberspace for å kunne fungere normalt, har sikringen av cyberspace blitt stadig viktigere. For å løse sikkerhetsutfordringene knyttet til utviklingen av cyberspace har stater søkt støtte fra private aktører gjennom såkalte multistakeholder-initiativer. Med slike initiativer mener man en åpen form for samarbeid mellom interessenter, basert på en idé om likeverdige partnere. Stater iverksetter slike initiativer ut fra en tanke om at et samarbeid mellom private og offentlige aktører gir den beste formen for styring og sikring av aktiviteter i cyberspace. Implementeringen foregår imidlertid uten at de nødvendige forutsetningene for at en slik styringsform skal fungere er til stede. Selv om mange i dagens akademiske debatt stiller spørsmål ved om disse initiativene fungerer, er det få som har stilt spørsmål ved hvordan cybersikkerhet kan utøves i praksis. Dette fører til at man overser det sentrale spørsmålet om hvordan maktdynamikken mellom offentlig og privat sektor fungerer med henblikk på sikkerhet i cyberspace. Denne artikkelen diskuterer hvorvidt multistakeholder-initiativene faktisk fungerer som en kontroll- og styringsmekanisme i cyberspace. Ved å se nærmere på offentlig-privat samarbeid om cybersikkerhet i Norge er hensikten å gi en bedre forståelse av årsakene til at multistakeholder-initiativer ofte ikke fungerer i praksis.

Nøkkelord: Cybersikkerhet · multistakeholder · global styring · internasjonale organisasjoner · privat-offentlig styring

Power dynamics in cyberspace: how do we produce cybersecurity?
A secure cyberspace is a necessity for the functioning of the economic, political and social structures of modern-day society. The stability and development of cyberspace is not preordained, but something that has to be facilitated. Cyberspace is constantly changing and to govern the complex set of interests, agendas and implications multistakeholder initiatives that promote cooperation between the public and private sector and civil society are increasingly put forth as the solution. This form for cooperation is widely

*Korrespondanse: Lilly Pijnenburg Muller, Forsker, Norsk utenrikspolitisk institutt, Norge. Email: lilly.muller@nupi.no

Citation: Lilly Pijnenburg Muller (2016). «Makt og avmakt i cyberspace: hvordan styre det digitale rom?». Internasjonal Politikk, 74, 4: 1–23. http://dx.doi.org/10.17585/ip.v74.428

seen in the policy community as a panacea for securing cyberspace. While academics have questioned these initiatives' functionality, few have studied why they do not work in practice. By focusing on the power dynamics between the different actors this article takes a step towards understanding how these dynamics create conflict of interest in governing cyberspace. Through case studies of multistakeholder initiatives on the international level and in Norway, this paper argues that these initiatives are implemented without the necessary preconditions for such a form of governance.

Keywords: Cybersecurity • multistakeholder initiatives • governance theory • international organizations • Public-private partnerships

Innledning

Fremveksten og avhengigheten av den globale informasjonsteknologiske infrastrukturen – cyberspace – har gjort verden sårbar på en ny måte. Systemene som utgjør cyberspace er sårbare for både digitale og fysiske angrep. Slike angrep kan ramme enkeltpersoner, bedrifter og stater. I de siste årene har vi sett mange eksempler på cyberangrep, noe som har forsterket inntrykket blant politiske aktører om at cyberangrep har blitt vanligere, bedre organiserte og sofistikerte, mer kostbare, og alt i alt: farligere (Balzacq & Dunn Cavelty 2016).[1] Dette har igjen ført til at cybersikkerhet har blitt stadig viktigere på den internasjonale sikkerhetsagendaen. Til tross for at spørsmål knyttet til sikkerhet i cyberspace har fått bred mediedekning og betydelig oppmerksomhet fra både sivile og militære beslutningstagere, har den politiske og akademiske tilnærmingen til cybersikkerhet så langt vært nokså fragmentert (Langø & Sandvik 2013).

I diskusjoner om hva slags mekanismer og styringsformer som er nødvendige for å etablere sikkerhet i cyberspace har den såkalte «multistakeholder-modellen» blitt det store mantraet. Med det mener man en åpen form for samarbeid mellom interessenter, basert på en idé om likeverdige partnere. Stater iverksetter slike initiativer ut fra en tanke om at et samarbeid mellom private og offentlige aktører gir den beste formen for styring og sikring av aktiviteter i cyberspace. Modellen implementeres både nasjonalt og internasjonalt med begrunnelse om at dette er den beste måten å få på plass enighet og løsninger på problemene som oppstår i sikringen og styringen av cyberspace. Mye tyder imidlertid på at multistakeholder-modellen fungerer suboptimalt, og denne artikkelen forsøker å identifisere mulige årsaker.

Jeg argumenterer for at hovedproblemet ligger i at statsinitierte multistakeholder-initiativer ofte baserer seg på en mangelfull forståelse av statens rolle så vel som av private aktørers interesser i cyberspace. Dette fører til maktkamper og interessekonflikter mellom de forskjellige aktørene. Den statlige implementeringen av multistakeholder-initiativer bidrar dermed til å øke heller enn å svekke

[1] som Stuxnet, Flame, og Duqu.

maktkampene mellom private og offentlige aktører. For å vise hvordan dette fungerer i praksis gjennomgår artikkelen multistakeholder-initiativer både på den internasjonale og nasjonale arena, og ser disse i lys av en neo-liberal styringsmodell. Ved å undersøke hvordan multistakeholder-modellen brukes får vi også et innblikk i hvordan disse ulike sfærene påvirker hverandre. Måten de brukes på nasjonalt og internasjonalt reflekterer igjen hvordan stater ser på og forstår bruken av modellen. Artikkelen fokuserer særlig på Norge, da Norge gjerne nevnes internasjonalt som eksempel på et land med en vellykket nasjonal tilnærming til multistakeholderstyring av cyberspace.

Sikkerhet i cyberspace

Spørsmålet om cybersikkerhet er en kombinasjon av teknologier, prosesser og hverdagslige handlinger. Det er en dynamisk prosess som er et produkt av handlinger og skadelig programvare (såkalt «malware»), og nye tiltak for å motvirke sistnevnte. Disse handlingene blir både muliggjort, og begrenset av den tekniske logikken i cyberspace. Cybersikkerhet kan med andre ord betraktes som reaksjonen på en risiko og trussel mot den moderne, globale informasjonsteknologiske infrastrukturen oftest kjent som 'internett' (Stevens 2016). I et bredt perspektiv omfatter spørsmålet om cybersikkerhet alt som kommuniseres gjennom digitale, elektroniske midler. Cybersikkerhet, slik det defineres av to ledende forskere i feltet, er fraværet av trusler fra eller via informasjons- og kommunikasjonsteknologier og -nettverk. Cybersikkerhet handler altså om sikkerheten vi har både *i* og *gjennom* cyberspace (Dunn Cavelty & Suter 2012: 19, se også Stevens 2016). Cybersikkerhet er slik ikke bare sikring av informasjon eller informasjonsteknologier, men en essensiell del av det å opprettholde samfunnssikkerheten. Samtidig er hvordan vi organiserer samfunnet forøvrig for å kunne sikre cyberspace, også en viktig faktor for å opprettholde denne samfunnssikkerheten.

Siden cyberspace i hovedsak eies og drives av private aktører er spørsmålet om *hvordan* sikringen skal gjennomføres i praksis, vanskelig å gi et entydig svar på. Cyberspace er grenseoverskridende av natur, og utfordringene som følger med kan dermed ikke løses uten internasjonalt politisk samarbeid mellom stater på den ene siden, og aktører i privat sektor på den andre. Dette leder til nye sikkerhetspolitiske utfordringer, og åpner for debatt om hvordan vi mer generelt skal tilnærme oss de store teknologiske utviklingene i informasjonsalderen. Vi må stille spørsmål ved hvilke mekanismer og styringsformer som er nødvendige i et samfunn for å kunne etablere og opprettholde sikkerhet i cyberspace. Til nå har samfunnsdebattene i stor grad fokusert på spørsmålet om overvåkning versus frihet, ikke minst i kjølvannet av Snowden-avsløringene i 2013.[2] Utviklingene i cyberspace har derimot gitt oss en mye større og bredere arena for å diskutere temaer rundt organiseringen av den moderne staten, inkludert spørsmål om hvordan sikre det som et offentlig gode. Her må det stilles spørsmål ved hvordan cyberspace bør styres og kontrolleres, og av hvem.

[2] Som tidligere CIA-agent offentliggjorde Edward Snowden store mengder informasjon om overvåkingen amerikansk etterretning utførte over internett og telefon, både nasjonalt og internasjonalt. Denne overvåkingen foregikk på daglig basis og dekket flere millioner amerikanere og internasjonale borgere. Blant de sistnevnte var statsledere og allierte av USA.

Til grunn for denne diskusjonen trengs en forståelse av det komplekse forholdet mellom ulike interesser, agendaer, diskurser og praksiser som påvirker utviklingen i cyberspace. Alle datanettverk krever en grad av administrasjon og styring, men cyberspace sin unike natur, kombinert med nettets dype politiske, økonomiske og kulturelle implikasjoner, har allerede ført til betydelige konflikter mellom stater, mellom offentlig og privat sektor, og mellom disse og sivilsamfunnet. Disse faktorene har også konsekvenser for styringen av cyberspace, og har ledet til diskusjon rundt hvilken tilnærming som burde brukes i styringen av cyberspace. Dette har blitt et viktig område som både utfordrer og bringer sammen ulike teorier om sikkerhet og internasjonale relasjoner (Bauer 2005; Dunn Cavelty & Suter 2012; Drezner 2004; Michel & Mueller 2013; Goldsmith & Wu 2006).

Multistakeholder-initiativer og neo-liberalistisk tankegang

Som følge av digitaliseringen av samfunnet, har offentlig og privat sektor i økende grad tatt innover seg utfordringene og sårbarhetene som oppstår i kjølvannet av dette. I forsøket på å håndtere disse problemene har offentlig sektor gått i spissen for å etablere såkalte multistakeholder-initiativ. Bruken av multistakeholder-initiativer for cybersikkerhet er tilsynelatende et logisk skritt for stater på veien mot målet om global cybersikkerhet. Slike initiativ iverksettes, som blant andre Carr (2015) uttrykker, for å bringe sammen «those closest to the bleeding edge of the technology (. . .) to offer insights and perspectives not accessible to policy makers or international bureaucrats» (Carr 2015: 649). I løpet av det siste tiåret har multistakeholder-initiativer blitt fremholdt og forbundet med cyberspace til den grad at de nesten har blitt et synonym for styringen av det. Multistakeholder-modellen fremstår nå i stor grad som «gullstandarden», både i den akademiske og den politiske debatten om styringsrasjonalitet i cyberspace. Både EU og USA har omtalt bruken av multistakeholder-initiativ som vesentlig for Internetts fremtid (ibid.). I akademia blir modellen vurdert som veien fremover fra offentlig-privat samarbeid, med sikte på å oppnå en mer legitim cybersikkerhet med inklusjonen av sivilsamfunnet (Dunn Cavelty & Suter 2012; DeNardis & Raymond 2013). Som et styringsverktøy for å oppnå cybersikkerhet regnes multistakeholder-initiativer ikke bare av mange som den beste måten å organisere seg rundt problemet på; de holdes også opp som en mal for hvordan vi best kan håndtere andre utfordringer som oppstår som følge av en mer sammenkoblet verden (Carr 2015).

Multistakeholder-initiativer er ikke unike for cyberspace. De brukes hyppig av vestlige stater som en mekanisme for å håndtere et bredt spekter av utfordringer. Initiativene stammer fra en neo-liberal tankegang hvor staten desentraliserer styring av effektiviseringshensyn. Denne styringsformen har utviklet seg fra å være direkte til indirekte, og fra å være «politisk» og hierarkisk (i den forstand at stater autoritativt bestemmer hvilke mål og midler den skal bruke), til å være horisontal, frivillig og, følgelig, også mindre «politisk» (Neumann & Sending 2010). Denne formen for styringsrasjonalitet gjør statens egen rolle mindre sentralisert og mer nettverksbasert. Ved å bruke denne formen for styringsmekanisme, skal styring bli mer effektivt og dermed mer økonomisk for staten. Mindre direkte kontroll antas å gjøre selve

styringsformen mindre ressurskrevende for stater. I stedet for at avgjørelser blir tatt ovenfra og ned, tar staten på seg en ny rolle som *tilrettelegger* for samarbeid og samhandling mellom statlige og ikke-statlige aktører. Statens «delegering» av makt til ikke-statlige aktører er her en bevisst handling. Med mål om å styre «mindre», kontrollerer staten isteden gjennom lovgivning og regulering. Selv om multistakeholder-initiativer ofte blir framstilt som en ny administrasjonstilnærming, er tilnærmingen en naturlig utvikling av en neo-liberal tankegang. Et multistakeholder-initiativ involverer alle interessenter i lærings- og utviklingsprosessen. Forskjellige sektorer er involvert i ulik skala, men de jobber alle mot et felles mål. Modellen skiller seg derfor fra direkte offentlig-privat samarbeid ved at den er åpen, transparent, og inkluderer sivilsamfunnet i prosessen. Avtaler i denne prosessen er basert på samarbeid, hvor alle interessenter er bevisste makt- og konfliktelementene blant aktørene.

På 1990-tallet så vi en klar intensivering av multistakeholder-initiativer i vestlige samfunn, noe som også reflekteres i en voksende faglitteratur som studerer denne typen initiativer. Sentrale bidrag har for eksempel sett på bakgrunnen for slike initiativer (Linder 1999; Wettenhall 2003), mulighetene for at slike initiativer kan oppstå (Stiglitz & Wallsten 1999; Dunn 1999, Auerswald et al. 2007), hvordan man kan måle om de har vært vellykkede (Hodge & Greve 2007; Garvin & Bosso 2008) og hvordan ansvar og autoritet delegeres innenfor slike modeller (Pongsiri, 2002; Schaferhoff Campe & Kaan 2009). Et knippe studier har også sett spesifikt på multistakeholdertilnærmingen i cybersikkerhet. Disse fokuserer på sivilsamfunnets deltakelse og på hvordan statlige og ikke-statlige aktører deler makten igjennom multistakeholderstrukturer og -prosesser (Froomkin 2003; Klein 2004; Kleinwächter 2004; Koppell 2005; Palfrey 2004; Pavane & Diani 2008; Huijstee 2012). En viktig del av denne debatten omhandler hvorvidt en multistakeholdertilnærming er best egnet (Sahel 2016), eller hvorvidt et direkte samarbeid mellom staten og privat sektor vil fungere bedre (Cavelty & Suter 2009; DeNardis & Raymond 2013; Drezner 2004). Fra et mer kritisk ståsted har DeNardis og Raymond (2013) og Carr (2015) argumentert for at multistakeholder-initiativer ikke er egnet til å regulere alle områdene cyberspace dekker. Kombinert gir denne litteraturen oss et godt utgangspunkt for denne artikkelens analyse og for å besvare spørsmål om hvorfor multistakeholder-initiativene *ikke* egner seg til å sikre og styre cyberspace.

Nasjonalt og internasjonalt samspill

Multistakeholder-initiativer er basert på en ide om å bringe alle relevante deltagere sammen i arbeidet mot et sammenfallende mål. Dette er derimot ikke tilfelle i cyberspace. Når interessentene har forskjellig oppfatning av hva det vil si å sikre og styre cyberspace fungerer ikke multistakeholder-modellen i seg selv som en mekanisme til å motvirke den eksisterende maktdynamikken som utspiller seg i kontrollen og styringen av cyberspace. Den akademiske litteraturen har til dags dato fokusert på den internasjonale arenaen (Dunn Cavelty & Suter 2009; DeNardis & Raymond 2013; Carr 2015; Chakravarty 2006; Kleinwächter 2004), men da cyberspace er grenseoverskridende kan man argumentere for at det er nødvendig

å analysere hvordan modellen blir brukt både internasjonalt og nasjonalt. Disse to sfærene påvirker hverandre gjensidig i utviklingen og implementeringen av multistakeholder-modellen. Stater tar med seg sin (ofte unike) forståelse av cyberspace og av multistakeholder-modellen til den internasjonale arenaen, og erfaringene fra det som skjer internasjonalt overføres i neste omgang til det som skjer nasjonalt.

I det følgende skal jeg begynne med å se nærmere på den internasjonale arenaen, ettersom det er her tanker og ideer om multistakeholder-modellen som et styringsverktøy i cybersikkerhet oppsto, og som igjen påvirker implementeringen på nasjonalt plan. På den internasjonale arenaen er både maktkamper og en eksklusjon av visse aktører tydelig. Dette tyder på at forutsetningene for en neo-liberal styringsmodell ikke er på plass. Implementeringen av modellen synes å forsterke heller enn å redusere maktkamper mellom de forskjellige sektorene. Etter å ha diskutert det internasjonale nivået, beveger jeg meg over til å studere enkeltlands tilnærming til cybersikkerhet. Avgjørelser rundt cybersikkerhet blir til syvende og sist tatt nasjonalt, og man kan argumentere for at det er her de forskjellige kulturene for hvordan styre internett utvikler seg. Jeg forsøker å vise dette gjennom en casestudie av Norge, som ofte omtales internasjonalt som eksempel på et land med en vellykket nasjonal tilnærming til en multistakeholdermodell for styring av internett. Gjennom det norske caset får vi innblikk i de interne maktkampene om cyberspace, nasjonalt og internasjonalt, og mellom privat sektor og stater. Dermed kan vi også ta steg mot å forstå hvorfor multistakeholder-modellen ofte ikke fungerer i praksis.[3] Jeg belyser modellens forankring i lovverket, maktdynamikken mellom de forskjellige partene og utøvelsen av kontroll. Fordi Norge blir ansett som et av landene som har lykkes best i å opprette et samarbeid mellom offentlig, privat sektor og sivilsamfunnet om sikkerhet i cyberspace, tilbyr dette studiet oss et unikt innblikk i multistakeholder-modellens funksjon og legitimitet.

Multistakeholder-initiativer kan i et bredere perspektiv forstås som en neo-liberal styringsform. Min analyse viser imidlertid at det sentrale neo-liberalistiske grunnlaget for multistakeholder-initiativer ikke er på plass, noe som igjen gjør at initiativene slik de blir implementert i dag, ikke fungerer. Resultatet er at multistakeholder-initiativer for å styre og sikre cyberspace i dets nåværende form har begrenset effektivitet.

[3] Denne artikkelen tar utgangspunkt i Steven Lukes' (1974) tre dimensjoner av makt. Her bygger den første dimensjonen på Dahls (1957) definisjon av makt hvor aktør A har makt over aktør B når A påvirker B til å handle mot Bs interesse. Den andre dimensjonen er evnen til å påvirke avgjørelser ved å sette en agenda, å kontrollere narrativer, og definere referanser for å minimere (eller delegitimere) uenighet. Den tredje er å få aktør B til å handle mot hva som virker som deres egentlige interesse, ved at systemet rundt dem får de til å handle på en annen måte enn hva som er intuitivt for aktør B (Lukes 2001). Alle disse dimensjonene er i spill, og tredelingen er viktig da den belyser det å 'skape konsensus' istedenfor tvang. Videre blir dynamikken mellom de som lager reglene og de som blir regulert i den globale styringen av cyberspace synliggjort, og hvordan de er bundet sammen gjennom en felles forståelse av et sett med politiske ideologier og et sett med normer om hva cybersikkerhet 'er' og 'burde' være. Ved å promotere en styringsmodell som promoterer normer som 'frihet', 'regulering mot overvåkning', 'demokrati' og 'likestilling', blir det å være imot *multistakeholderism* synonymt med å være mot disse normene, med lite rom for alternativer.

Multistakeholder-initiativer i den internasjonale arenaen

Siden midten av 1990-tallet har det pågått arbeid for å etablere internasjonale regimer for global styring av cyberspace. Både statlige og private aktører har initiert slike initiativer basert på en forståelse av at internasjonalt samarbeid på tvers av næringssektorer er en nødvendig forutsetning for sikkerhet i cyberspace. Disse institusjonene, aktørene og prosessene varierer i type, størrelse og innflytelse, men har til felles at de er basert på en kollektiv, «policymotivert» utforming av et sosioteknisk system (Bauer 2005; Eeten & Mueller 2013). Det alle disse initiativene har til felles, er at de blir definert og omtalt som multistakeholder-initiativer. En forståelse av hva som må ligge til grunn for at et initiativ er nettopp dette er derimot ikke på plass. Dette leder til konflikter mellom de forskjellige makthaverne i cyberspace.

ICANN og WSIS

Begrepet «multi-stakeholder» ble først brukt i internasjonal cyber-sammenheng i oppfølgingen og beskrivelsen av de problemene som utviklet seg etter at den da private «non-profit»- organisasjonen Internet Corporation for Assigned Names and Numbers (ICANN)[4] ble etablert i 1998. Denne organisasjonen ble opprettet for å koordinere, vedlikeholde og utvikle metodikken for flere databaser, med unike identifikatorer knyttet til de domenenavnene som brukes på Internett, og skulle være ansvarlig for sikkerhet og stabilitet på nettet.[5] ICANN ble registrert i California og var knyttet til US Department of Commerce gjennom en kontrakt på én dollar. For å styrke sin egen legitimitet, startet ICANN i 2016 flyttingen av ansvaret for såkalte Internett Assigned Numbers Authority (IANA)[6] fra å være privat amerikansk styrt til det internasjonale samfunnet (Farrell 2016; ICANN 2016a, ICANN 2016b). Dette ble gjort gjennom en koordineringsgruppe bestående av aktører fra alle sektorene (ICANN 2016c; Sahel 2016). Denne gruppen ble dermed ansvarlig for hvordan denne overføringen skulle skje. IANA prosessen har som mål å gjøre ICANN til en non-profit organisasjon, som sammen med flere private, non-profit og frivillige aktører skal drifte internett. Dette oppsettet innebærer at ICANN *ikke* er å betrakte som et multistakeholderorgan, selv om det ofte fremstilles som det i andre internasjonale fora (Sahel 2016). IANA-prosessen er en åpen prosess, hvor både offentlig og privat sektor og sivilsamfunnet har mulighet til å bidra i utformingen av prosessen, primært via debatter og fora på internett. Gjennom hele prosessen har det vært mulig for alle aktør-grupper å søke om å få være med, men dette gjør ikke nødvendigvis ICANN eller IANA til multistakeholdere. På papiret har de forskjellige aktørene muligheten til å delta i utbyggingen av institusjonen (Sahel 2016), men det er

[4] Som Eeten & Mueller (2013) påpeker, har det oppstått en misforståelse om at internett på en eller annen måte er «styrt» av ICANN, og denne henger igjen i mange akademiske og politiske debatter. Det kan for eksempel sees i The Economist for september 2009, som referer til forhandlingene over den nye kontrakten mellom ICANN og den amerikanske regjeringen som om de omhandlet «kontrollen over cyberspace».

[5] Se «ICANN Bylaw» 30 juli 2014 for mer informasjon.

[6] Dette er avdelingen av ICANN som har ansvar for å fordele og tildele både IP-adresser globalt, autonome nummer-systemer, har rotsoneledelsen i Domain Name System (DNS), og andre Internett Protocol-relaterte symboler og tall.

ikke en prosess initiert for å fordele makten i organisasjonen. Videre er prosessen vanskelig å ta del i. Eksklusjon av visse aktører er tydelig i flere områder, for eksempel holdes alle de transparente live-diskusjonene på internett i amerikansk tidssone. Videre blir informasjon om *når* debattene skal holdes annonsert kort tid i forveien, og informasjon om hvordan man kan delta er ikke lett tilgjengelig. Dette betyr at kun de som har tid og mulighet kan delta.[7] Videre er det viktig å ha en kontaktperson i prosessen for å nyss om når ting skjer og holde seg oppdatert på de korte påmeldingsfristene.[8] Ved at deltagelse og informasjon kun blir muliggjort i begrenset grad kan det argumenteres at aktørene som sitter på kontrollen ikke nødvendigvis ønsker at andre aktørene skal ha samme premisser for å delta. En maktdynamikk hvor de nærmest kontrollen holder styringen og kun et fåtall sivilsamfunn representanter blir inkludert er tydelig.

En tilsvarende drakamp er også tydelig i World Summit on the Information Society Forum (WSIS), det første stedet ordet «multistakeholder» ble brukt om et offentlig arrangert initiativ siden ICANN. Dette skjedde først under en konferanse holdt av Working Group on Internet Governance (WGIG) under etableringen av WSIS.[9] I denne rekken av statsfokuserte diplomatiske konferanser arrangert mellom 2002 og 2005, skulle WSIS utgjøre en plattform der utviklingsland og EU kunne utfordre USAs dominans i cyberdomenet.[10] Denne plattformen har siden vokst og WSIS har blitt et sted hvor stater kommer sammen for å bestemme hvilke skritt de ville ta mot en sikker styring av Internett. I 2015 ble WSIS' mandat fornyet i ti nye år igjennom WSIS + 10 prosessen. Denne prosessen var på papiret en åpen prosess hvor både privat sektor og sivilsamfunnet ble invitert til å delta. Slik som i årene før var det et sted hvor G77 landene kunne utfordre USA og EUs dominans. Dokumenter fra prosessen i utformingen av mandatet ble delt på internett, hvor

[7] Intervju med Salanieta Tamanikaiwaimaro, Secretariat of the ICANN Oceania Working Group, Suva Fiji, 8. november 2015. Gjennom intervjuer med IANA-representant for det sivile samfunn ble det tydeliggjort at det var vanskelig for ikke-vestlige medlemmer å ha mulighet og kapasitet til å delta i disse forumene, da de ble avholdt i amerikansk tidsone, og dermed midt på natten, lokal tid, for mange land i globale sør. Videre deltar alle frivillig i arbeidet. Der vestlige representanter ofte kunne få betaling via å være ansatt i en NGO som fokuserte på prosessen, var dette arbeid mange ikke-vestlige påtok seg ved siden av sine egne dagjobber. Dette begrenset deres mulighet for deltagelse. See også Sahel (2016: 12–13) for diskusjon om hvordan forbedre dette.

[8] Påmeldingsfristen for sivilsamfunndeltagere blir ofte publisert på hjemmesiden til iCANN kun få dager i forveien av store eventer og diskusjoner, med kort påmeldingsfrist. Basert på egen observasjon og uformelle samtaler med sivilsamfunnaktører.

[9] WGIG-rapporten bruker ordet 11 ganger og påpeker blant annet nødvendigheten av et «globalt stakeholderforum som kan ta opp internett-relaterte policyproblemer». Det var under WGIG at ordet kom inn i Tunis-agendaen, som refererer til «multistakeholder» 18 ganger, fire av dem relatert til internett Governance Forum (IGF).

[10] Måten WGIG skal være multistakeholder på den måten at de inviterer ikke-statlige aktører, privat sektor og det sivile samfunn til å bli direkte involvert i den politiske prosessen, men virkeligheten er imidlertid en annen. Den vage invitasjonen til ikke-statlige aktører har ført til uenighet mellom regjeringer og mellom stater og ikke-statlige aktører. Invitasjonen oppfordrer ikke-statlige aktører til å gå imot statlige argumenter, men kun som «observatører». De får dermed ikke status som representanter, og kan ikke snakke med en koordinert stemme ved å organisere seg selv for å vise legitimitet, ekspertise og et konstruktivt engasjement.

aktørene fra alle sektorene kunne kommentere og sende inn anbefalinger til styret av WSIS. Videre kunne sivil og privat sektor søke om å få delta i prosessen, både gjennom å sende inn kommentarer til styret av WSIS og ved å søke om å få være med på toppmøtene i FN i Genève og New York. Som i ICANN-prosessen var imidlertid informasjonen om *hvordan* dette skulle gjøres vanskelig å finne, og videre samsvarte den ikke nødvendigvis med informasjon som ble delt i kort tid før toppmøtene. Dokumentene publisert på internett var ofte utdatert eller kun kort versjoner av hva som ble delt og sagt på eventene. Dette gjorde det vanskelig for både privat sektor og sivil samfunnet å komme med relevante innspill. Selv med en slik åpen prosess var det dermed tydelig i selve møtene at det var statene som hadde det siste ordet, og som i praksis var maktholdere i dette forumet.

Allikevel har få, om ingen, av de internasjonale politiske konfliktene som førte til etableringen av WSIS, blitt løst her. Selv om innflytelsesrike og mektige statlige aktører er tilstede, har de ikke klart å bli enige om hvordan de skal endre eller institusjonalisere styresettet i praksis, eller hvilke regler som skal gjelde for og i cyberspace. ICANN er en non-profit privat organisasjon (Muller 2016)[11] mens WSIS er en del av FN-apparatet. Selv om begge påstår at de er multistakeholder-institusjoner fordi de åpner opp for innspill fra privat sektor og sivil samfunnet, er de primært organisasjoner hvor staten har styringsmakten. Prosessen som ledet frem til utformingen av foraene har elementer av multistakeholder-modellen i seg, men det er en tydelig ubalanse mellom makthaverne som ikke forsvinner bare fordi prosessen kalles multistakeholder. De som leder initiativene har størst innflytelse, og det siste ordet i prosessen.

IGF

I kjølvannet av ICANN og WSIS som multistakeholder-initiativer har FNs Internet Governance Forum (IGF) blitt opprettet for å tilby en ikke-truende, ikke-bindende arena for multistakeholderdialog mellom alle partene (Eeten & Mueller 2013). Initiativet løser imidlertid ikke problemene det har blitt skapt for å løse. Som et av de største initiativene, som oftest blir referert til som et eksempel på multistakeholder-initiativ, skal IGF være en arena hvor statsledere skal kunne komme sammen med sivilsamfunnet og privat sektor for å diskutere hvordan styringen av internett skal foregå (Eeten & Mueller 2013). I teorien skal dette årlige arrangementet bringe statlige og private aktører og sivilsamfunnet sammen for å diskutere utfordringene rundt styringen av internett. Men aktørene som har operasjonell kontroll over internettsikkerhet og cyberspace er i økende grad ikke involvert i IGF. Deltagelse er frivillig og åpent for alle, men det tekniske samfunnet har i økende grad latt være å delta. Samtidig ser vi en nedgang i statlig representasjon. Det tekniske og det private samfunnet på sin side utrykker at de ikke føler seg hørt, og at de dermed har minimal påvirkning på hva som kommer ut av IGF. Dette har ført til at de i mindre grad ønsket å delta i slike fora. Samtidig ser vi en nedgang i statlig representasjon fra sentrale nasjoner som ser IGF som et «snakkeforum» uten

[11] Dette er kun fra 2016, inntil da var dette også statlig eid av USA som en non-profit organisasjon.

handlingskraft (Mueller 2010). Dialogen blir dermed preget av sivilsamfunnets agenda, uten at statsoverhoder og direktører av sentrale private selskaper er tilstede og er med på diskusjonen (Mueller 2013). Med et begrenset antall aktører med direkte innflytelse fra både offentlig og privat sektor har de stats-initierte multistakeholder-initiativene evne til å produsere en kollektiv resolusjon eller bindende avtaler med en reell effekt på cybersikkerhet vært begrenset. Markus Kummer, administrerende koordinator for IGF-sekretariatet, har slik sett rett i at IGF er blitt et redskap og et instrument «for politisk dialog der alle deltar på lik linje» gjennom en åpen, inkluderende og transparent prosess (Kummer 2013). I praksis blir likevel denne deltagelsen begrenset, ved at de som har makt til å påvirke prosesser ikke deltar i forumene. IGF mangler dermed evnen til å lede til internasjonale avtaler som forbedrer cybersikkerhet, ved at den internasjonale politiske konteksten blir oversett. Ansvaret for sikringen av cyberspace synes å bli flyttet rundt, og det blir utydelig hvor avgjørelser blir tatt og hvem som tar dem. Avtalene og resultatene fra IGF har liten innvirkning på de aktørene som faktisk opererer i cyberspace, mange av de berørte aktørene er ikke involvert i beslutningsprosessen.

Åpenheten i disse organisasjonene er dermed i teorien velegnet til å skape en plattform for dialog, men i praksis er de ikke organer som kan ta beslutninger over styringen av cyberspace. IGF kan da heller ikke defineres som et forum hvor styring av internett kan sies å finne sted. Erkjennelsen blant stater av at styringen av cyberspace utføres av andre enn dem selv, er begrenset. Dette fører til bemerkelsesverdig lite operasjonalisering av «multistakeholder-modellen» i de initiativene som er initiert av de formelle institusjonene med sikte på sikker styring av cyberspace på et internasjonalt nivå. Det er tydelig at USA og EU versus G-77 landene har klare divergerende interesser for styringen av cyberspace. Gjennom WSIS + 10 prosessen var det tydelig at USA og Europa arbeidet for multistakeholder-modellen og IGF, i motsetning til Kina og Russland som ønsker mer statlig kontroll (Muller 2016). Dette viser hvordan multistakeholder-modellen og institusjonene rundt det også kan sees som en politisk kampplass, rundt hva internett og cyberspace skal og bør være, mer enn bare et forsøk på å bringe de rette tekniske ekspertene til bordet.

FIRST

I mangelen på en felles kommunikasjonsplattform for å sikre cyberspace, har den private-sektoren lansert sine egne initiativer for å fostre samarbeid mellom de som sitter på spakene av det daglig som utformer og utgjør cyberspace. Et slikt initiativ er Forum for Incident Response and Security Teams (FIRST), som har som mål å koordinere statlige tiltak og private Computer Emergency Response Teams (CERT) på en internasjonal skala.[12] Med mål om å opprette standarder på et teknisk nivå, arbeider medlemsorganisasjonene for å utvikle og dele teknisk informasjon, redskaper, metoder, prosesser og «best practices». Ved å bruke sin kombinerte kunnskap og

[12] Selv om FIRST har et mer teknisk fokus og ikke er en multistakeholder-organisasjon per definisjon, blir de definert som det av blant annet NetMundial, som fører opp FIRST som den første på deres liste over fungerende multistakeholder-initiativer http://content.netmundial.br/contribution/the-importance-of-a-multistakeholder-approach-to-cybersecurity-effectiveness/180

erfaring, arbeides det for å fremme et sterkere og sikrere miljø for å bedre cybersikkerhet. FIRST jobber både med privat sektor, statlige og ikke statlige aktører for å dele kunnskap og erfaring om «best-practice» i sikringen av cyberspace. Lignende initiativer, slik som National Computer Security Incident Response Teams (NatCSIRT), organiserer et årlig møte for responsteam med nasjonalt ansvar. Her kan organisasjonene som er ansvarlige for å sikre økonomiers og staters kritiske infrastruktur, diskutere de utfordringene de møter i cyberspace. Disse initiativene regner imidlertid selv med å ha relativt begrenset innflytelse på stater og statenes syn på cybersikkerhet, men har påvirkning på hvordan cyberspace sikres i det daglige. Statlige myndigheter og deres representanter viser generelt liten interesse for å delta på disse tiltakene og FIRST-eventene.[13] Resultatet er at både de internasjonale og private initiativene blir sektorbaserte, med lite tverrgående informasjonsdeling. Initiativene ledet av privat sektor er gode til å utvikle tekniske standarder for det tekniske samfunnet, men lite av det som blir avtalt og utviklet når frem til det statlige nivået. Den tekniske kunnskapen som blir utarbeidet forblir dermed for ofte hos privat sektor, og muligheten til disse initiativene å bli reelle multistakeholder-initiativer forblir begrenset.

Maktkonflikt i styringen av cyberspace

I praksis skal alle interessenter være med i lære- og utviklingsprosessen og i avgjørelsene som blir tatt i et multistakeholder-initiativ og de forskjellige sektorer skal jobbe mot et felles mål. I denne åpne formen for samarbeid hvor partene er likeverdige er det felles målet å legge best mulig til rette for samarbeid mellom privat og offentlig sektor og sivilsamfunnet. I de såkalte multistakeholder-initiativene som blir implementert og promotert internasjonalt i dag ser vi derimot en maktkamp i strukturene og beslutningsprosessen som blir initiert for å sikre cyberspace. Dette påvirker de forskjellige aktørenes ståsted og mulighet til å påvirke prosessen. Istedenfor å overkomme interessekonflikter og bygge en felles forståelse mellom staten og privat sektor om hvordan styre cyberspace, fungerer multistakeholderinstitusjonene som en politisk slagmark, hvor det strides om definisjonen på hva cyberspace er og hvordan det burde bli sikret. Et faktisk forsøk på å bringe de rette tekniske ekspertene til bordet blir utelatt.

I en neo-liberalistisk tankegang initierer stater multistakeholder-initiativer for å oppnå effektivisering. De gir vekk statlig makt til privat sektor, som i gjengjeld stiller med sin ekspertise. I cyberspace er det privat sektor som har utviklet og tilrettelagt for utviklingen av cyberspace, og dermed er det også dem som har makten og ekspertisen. Statens rolle blir slik mindre sentralisert og mer nettverksbasert. Multistakeholder-initiativene kan dermed bli oppfattet som at de blir initiert, ikke for å gjøre styringen mer effektiv og økonomisk nyttig for staten, men fordi det er den eneste måten staten kan ha innflytelse på sikringen av cyberspace. Det blir dermed en interessekonflikt når staten implementerer multistakeholderinitiativer uten å ha med privatsektoren. Ved at staten ser på cyberspace som alle andre områder staten sikrer, uten å ta hensyn til at privat sektor har en større rolle her enn på de andre områdene

[13] Ingen statlige representanter var tilstede på den årlige konferansen i Berlin 2015.

hvor staten initierer slike initiativer, oppstår det en maktkonflikt. Til grunn for denne konflikten er at interessene til de forskjellige partene bare er delvis konvergente. Hvor staten ser det som sin oppgave å sikre staten, samfunnet og individet, er privatsektoren fokus på profittmaksimering og sikring av seg selv. Privat sektor opererer for det meste på tvers av landegrenser, og som Dunn Cavelty & Suter (2012) argumenterer, er det dermed bare delvis nødvendig for de å samarbeide med staten. Cybersikkerhet blir sett i et business-perspektiv og dermed er det å sikre en kontinuitet av business første prioritet, ikke sikkerhet (ibid). Det forskjellige fokuset kan gjøre at de ser forskjellig på cybersikkerhet og dermed handler forskjellig. Interessene til privat sektor og staten i multistakeholder-initiativer er slik bare delvis sammenfallende.

Stater er avhengige av et funksjonelt og sikkert cyberspace, og dermed av privatsektoren som er den som har kapasiteten og kunnskapen til å sikre dette. I sikringen og styring av cyberspace samfaller ikke staten og privatsektors interesser. Dette resulterer i at fokuset i samarbeidsformen blir på forvaltning av ressurser, og utviklingen av forhandlingsprosesser blir skjøvet i bakgrunnen (Eeten & Mueller 2013). Når alle partene som er en del av å sikre cyberspace ikke blir involvert (skaperne, eierne og lovgiveren), står disse tiltakene i fare for å bli rene diskusjonsfora, og informasjonsutveksling «nav» innenfor de forskjellige områdene. Konsekvensen er at den private sektorens rolle i de statlig initierte initiativene er minimal, og grunnleggende kunnskap om hvordan teknologien bak cyberspace fungerer i praksis når dermed ikke frem til dem som vedtar lovene for å sikre det. Dette påvirker igjen lovgivernes og statens evne til å påse at loven som lages for å sikre cyberspace omfatter det som er relevant. På samme måte resulterer den manglende inkluderingen av offentlig sektor i de private initiativene deres mulighet til å påvirke utformingen av lover som kan følges opp i praksis. De som har mulighet til å handle på begge sider, trekkes dermed ikke inn, men blir stående på sidelinjen som tilskuere. Uten at både offentlig og privat sektor er involvert i initiativene som oppstår, får avgjørelsene som blir tatt minimale ringvirkninger. De internasjonale foraene som vokser frem i arbeidet for å styre cyberspace internasjonalt, kan dermed ikke rettferdiggjøres som vellykkede multistakeholder-initiativer.

Uenighet om hva de forskjellige aktørene ønsker å få ut av samarbeidet resulterer i at sikringen av cyberspace internasjonalt utvikler seg langs to spor: ett for den private sektoren og ett for den statlige. Selv om disse seperasjonene også forekommer i andre sektorer, er det annerledes i cyberspace. I for eksempel energisektoren har det vært en privatisering, men her har staten beholdt lovgivende makt samt eierandeler. I cyberspace er det derimot ikke slik. Det har ikke forkommet en privatisering på samme måte, siden cyberspace i hovedsak har utviklet seg utenfor statens styring. Ved at staten har begrenset kontroll og innflytelse på utviklingen og sikringen av cyberspace, er det lite som gjør at privat sektor engasjerer seg i statlige initiativer. De som er nærmest «the bleeding edge of the technology», som Carr (2015) kaller det, er dermed ikke involvert i avgjørelsene som statlige aktører tar. På samme måte blir det tekniske samfunnets beslutninger tatt uten å først bli samkjørt med eventuelle policy beslutninger. Dette ser vi tydelig i praksis gjennom staters etablering av forum som IGF, WSIS og ICANN, mens privat sektor arbeider for å bygge opp organisasjoner som FIRST.

Evnen dagens internasjonale initiativer har til å oppnå cybersikkerhet er med andre ord fragmentert. Ved at stater ikke forstår verken sin egen, eller privatsektorens rolle i cyberspace, forbigås det sentrale spørsmålet om ekspertise og autoritet i iveren etter å implementere multistakeholder-initiativer. Dette forsterkes i at staten bruker multistakeholder-forum som en arena for striden om hva styring av cyberspace innebærer. Den private sektorens betydelige innflytelse og ansvar er ikke synlig i statens implementering av multistakeholder-initiativer i dag. Den nødvendige forståelsen av det tekniske og politiske bildet som gjør at multistakeholder-initiativer kan fungere, er ikke til stede. Både en politisk og teknisk forståelse trengs. Arbeidet med cybersikkerhet internasjonalt kan dermed sees er i stor grad *ad hoc*. De som har den faktiske ekspertisen og autoriteten til å utøve og forme cybersikkerhet, blir ekskludert fra dette arbeidet. Avgjørelser blir tatt uten å involvere de dette faktisk påvirker. Uten en slik involvering blir lovene staten skaper som rammeverk for å sikre cyberspace overfladiske og ufokuserte, og legitimiteten og muligheten til å påvirke de forskjellige aktørene og avgjørelsene blir minimal.

Med rollen både statlige og ikke-statlige aktører har for sikkerheten og styringen av cyberspace er det viktig å diskutere cybersikkerhet også utenfor rammen av internasjonal politikk. Internett er globalt og grenseoverskridende, men spørsmål vedrørende regulering og implementering av tiltak i cyberspace kommer fra det nasjonale nivået. Hvorfor multistakeholder-initiativer ikke fungerer på det internasjonale nivået er en omfattende diskusjon (DeNardis & Raymond 2013), men den beveger seg ikke fremover uten at vi også ser på det nasjonale nivået og forskjellene innad i stater. Hva som skjer på den hjemlige arena i den enkelte stat påvirker hvordan aktørene oppfatter styring av cyberspace, og dermed hva slags modell de velger å promotere internasjonalt. Samtidig vil modeller som blir brukt nasjonalt for å styre internett påvirke hvordan de argumenterer for at dette burde gjøres internasjonalt. For å forstå hvorfor multistakeholder-initiativer ikke fungerer internasjonalt må vi bevege oss til det nasjonale nivået. Samarbeidet om cybersikkerhet mellom offentlig og privat sektor i Norge blir sett på som avansert internasjonalt, og Norges nasjonale strategi viser tydelig at staten ønsker å samarbeide med privat sektor gjennom multistakeholder-initiativer (Departementene 2012: 17–23). Selv om regjeringen ikke bruker ordet multistakeholder i den nasjonale strategien, skrives det tydelig gjennom dokumentet at det trengs en helhetlig tilnærming, hvor myndighetene, næringslivet og den enkelte bruker samarbeider for å løse utfordringene i IKT-sektoren (ibid. 16). I tillegg bruker både Utenriksdepartmentet, Justisdepartementet, og Nasjonal Sikkerhetsmyndighet begrepet multistakeholder når de snakker om Varslingssystemet for digital infrastruktur (VDI) og samarbeidsmodellen i Norge internasjonalt og nasjonalt.[14] Konseptene brukes om hverandre, men det er helt klart at multistakeholder-begrepet er viktig i forankringen av samarbeid for å sikre cyberspace i Norge.

[14] Dette har kommet frem gjennom en rekke formelle og uformelle samtaler forfatteren har hatt med representanter fra Forsvarsdepartementet, Utenriksdepartementet, Justisdepartementet, Nasjonal sikkerhetsmyndighet og NorCERT.

Nasjonal cybersikkerhet – en studie av Norge

Norge presenterer seg selv internasjonalt som et forbilde for fungerende multistakeholder-initiativer i sikringen av cyberspace. Begrunnelsen ligger i det tette samarbeidet i Norge på det operasjonelle nivået, som er et resultat av VDI. Internasjonalt blir VDI presentert som Norges løsning på utfordringer knyttet til offentlig-privat samarbeid for å sikre cyberspace nasjonalt.[15] Norge var ett av de første landene i verden som installerte et slikt varslingssystem, og den gjensidige tilliten som har utviklet seg mellom privat og offentlig sektor som følge av dette systemet, blir betraktet som helt unik i internasjonal sammenheng (Kibar 2015).

VDI styres og kontrolleres av Norwegian Computer Emergency Response Team (NorCERT), som er underlagt den Nasjonale sikkerhetsmyndigheten (NSM), og er statens førstelinje i forsvaret av cyberspace. De fleste land har en CERT. Disse kan sammenlignes med en brannstasjon som oppdager en brann (i cyberspace skadelig programvare) når den har oppstått, og deretter bidrar til å slukke den (Sveinbjørnsson 2012). Internasjonalt fungerer alle CERTer forskjellig og NorCERT bruker VDI. Dette apparatet består av sensorbokser som er utplassert av NorCERT, som overvåker nettverkstrafikken til alle de private bedriftene i Norge som har valgt å være medlemmer.[16] Sensorboksene setter NorCERT i stand til å lese hva slags datatrafikk som går ut og inn av medlemsbedriftene. VDI forsyner på denne måten NorCERT med informasjon som viser hvilke former for skadevare de private bedrifter blir angrepet av, slik at de det gjelder kan bli informert. VDI gir dermed NorCERT anledning til å fange opp nettverkstrafikk som inneholder eller er infiltrert av skadevare, dersom de har nettverkssignaturer som kan oppdages. Dette inkluderer «deep packet inspection», som innebærer at NorCERT kan kontrollere på filnivå hva som blir sendt inn og ut av et firmanettverk. De firmaene som velger å være en del av VDI betaler 200.000 kroner i medlemskontingent (Kirknes 2010). VDI er dermed ikke pålagt fra staten, men er en statlig tjeneste tilbudt privat sektor. Hvem som er medlem er hemmeligholdt av hensyn til medlemmenes sikkerhet, men Telenor – som kanskje er den viktigste nasjonale privatsektoroperatøren og leverandøren av internetttjenester – har meldt seg ut (Kibar 2015; Telenor 2015). Begrunnelsen er at det de anser det for å være en konflikt mellom personvernloven og VDIs kapabilitet til å overvåke alt som går inn og ut av selskapets nettverk.

NorCERT har vært en sentral pådriver for å skape et offentlig-privat samarbeid i Norge gjennom implementeringen av VDI. Informasjonen NorCERT får igjennom VDIen lar de være et knutepunkt slett mellom de forskjellige offentlige og private bedriftene som er medlemmer. VDI bidrar slik til at NorCERT kan drive informasjonsutveksling mellom privat og offentlig sektor og deling av viktig informasjon om trusler og angrep – problemer den private sektoren sjelden er interessert i å opplyse om (Dunn & Mauer red. 2006; Dunn Cavelty & Suter 2009; Campbell et al.

[15] Forfatteren har observert dette ved flere anledninger internasjonalt hvor VDI blir presentert slik av representanter for Utenriks- og Justisdepartementet og NorCERT.

[16] VDI er en variasjon av klient / server-datamodellen, noen ganger kalt «server-based computing».

2013). Ved å være et knutepunkt i det offentlig-private samarbeidet om cybersikkerhet har NorCERT det nasjonale hovedansvaret for den daglige sikkerheten ved bruk av cyberspace.[17] VDI legger i teorien til rette for at staten igjennom NorCERT både kan beskytte og varsle private bedrifter om cyberangrep, ved å få innsikt i potensielle og aktuelle trusler i Norge igjennom VDI. Samtidig innebærer utplasseringen av sensorboksene at medlemsbedriftene må stole på at informasjonen ikke blir misbrukt. VDI leser alt som går inn og ut av bedriftene over nettet. Ikke noe annet land i verden har et tilsvarende varslingssystem som er basert på en så høy grad av tillit.

Ett av argumentene som ofte brukes i diskusjonen om hvorfor offentlig-private samarbeid ikke fungerer på nasjonalt nivå, er at privat sektor ikke ønsker å dele informasjon om angrep de opplever i åpne forum, da de er bekymret for de økonomiske konsekvensene dette kan medføre (Cavelty & Suter 2009). Private firmaer frykter ofte at sensitiv informasjon som blir gitt til staten, ikke blir behandlet med tilstrekkelige sikkerhetstiltak da det ikke er garantert at staten har den nødvendige sikkerheten i sine systemer. Om slik informasjon lekker ut, kan det føre til skade både for deres omdømme og fremtidige avkastning. Denne bekymringen er ikke ubegrunnet, da flere studier viser en negativ korrelasjon mellom offentlige sikkerhetstiltak og markedsverdien av de bedriftene som er berørt (ibid.). I Norge derimot synes den private sektoren å være villig til å samarbeide med det offentlige for å gjøre cyberspace trygt, men mangler kanaler og strukturer for å gjøre det. Den direkte kommunikasjonen og tilliten som har oppstått mellom staten og privat sektor som et resultat av VDI, blir tolket av staten som at de har lykkes i å bringe offentlig og privat sektor sammen i et samarbeid for cybersikkerhet. Dette blir lagt merke til internasjonalt, og presentert som en suksesshistorie (Kibar 2015). Ved at NorCERT deler informasjon med medlemmene sine om angrep blir de oppfattet som et bindeledd mellom det offentlige og private. I praksis, derimot, er ikke de grunnleggende premissene for en multistakeholder-modell – dialog, koordinering, åpenhet mellom partene innenfor en ramme av forståelse for maktdynamikken – på plass i Norge. Alle interessenter er ikke involvert i lærings- og utviklingsprosessen av et samarbeid for å sikre cyberspace. De forskjellige partene har ikke en lik forståelse av problematikken og maktdynamikken i området, og det arbeides dermed heller ikke mot et felles mål. Ved å være medlem i VDI tar medlemmene del i et arbeid for i sikre cyberspace, men majoriteten av arbeidet ligger tydelig hos NorCERT i implementeringen og vektleggingen på VDI som et bindeledd mellom offentlig og privat sektor. Samtidig er hovedansvaret hos privat sektor selv å reparere etter et mulig angrep. Makt- og konfliktelementene blant aktørene blir ikke anerkjent. Det er heller motsatt: det presenteres et bilde av at gjennom VDI er alle medlemmer på lik fot og informasjon deles mellom offentlig og privat sektor.

[17] For en detaljert oversikt over hvem som har ansvar for å styre hva på den statlige siden i cyberspace, se Langø & Sandvik (2013). Denne artikkelen fokuserer kun på VDI, da det er her offentlig og privat sektor samarbeider tettest.

I det norske caset kan vi observere en grunnleggende interessekonflikt mellom det offentlige og private. VDI tilrettelegger for kommunikasjon fra «medlem-til-medlem», men dette er på et teknisk og operativt nivå. VDI utgjør slik i praksis et enveis kommunikasjonsmiddel som lar staten samle inn informasjon om cyberangrep den private sektoren opplever. Kommunikasjonen mellom medlemmer på det strategiske nivået, og mellom aktører fra privat sektor og staten blir på denne måten minimal. Dette kan imidlertid ikke sies å være fordi aktører fra privat sektor ikke ønsker å dele informasjon eller kommunisere. Det at kommunikasjonen kun finner sted på et operasjonelt nivå, betyr ikke at disse aktørene ikke er villige til å dele mer informasjon med den offentlige sektoren. Aktører i privat sektor viser interesse for å samarbeide med staten (noe VDI-medlemskapet i seg selv viser), men muligheten for dette hindres av mangelen på en organisert kommunikasjonsplattform der informasjon kan deles, tillit kan bygges og samarbeidsmekanismer utvikles. Det at informasjon i dag hovedsakelig deles via VDI, gjør at dette kun skjer direkte mellom medlemmene og NorCERT. Det oppstår dermed ikke en naturlig toveis kommunikasjon mellom NorCERT og aktørene i privat sektor, eller disse aktørene seg mellom på et strategisk nivå. Da de som har den faktiske makten i cyberspace, dvs. privat sektor, kun kommuniserer med hverandre på et operasjonelt nivå gjennom det nåværende systemet, kan VDI dermed betraktes som et miljø som gir staten færre insentiver til å etablere kommunikasjonskanaler mellom seg og privat sektor. I stedet for å tilrettelegge for samarbeid, begrenser statens tilnærming til cybersikkerhet gjennom VDI for kommunikasjon mellom partene. Selv om NorCERT ser informasjonen de samler inn som en mulighet til å hjelpe andre, er lite dialog og koordinering mellom aktørene et biprodukt av ordningen. Motstridende interesser mellom det offentlige og de private kan sees å legge grunnlaget for dette.

Maktkamp, lovgivning og regulering

Interessekonflikter mellom de forskjellige sektorene i offentligheten påvirker statens styringsevne i cyberspace. Å bestemme hvem som skal styre hva, og sikre hvilke områder, blir gjort omvendt av hva staten vanligvis gjør i en neo-liberal styringsrasjonale. Problemet for staten er at ulikt andre områder staten har gitt vekk kontroll og styring gjennom en neo-liberal tankegang, har staten aldri hatt kontroll over cyberspace. Den grunnleggende kontrakten mellom staten og privat sektor som er nødvendig for å kunne implementere denne formen for styring har dermed ikke vært etablert. Innenfor et neo-liberalt styresett er en av statens viktigste oppgaver å regulere og opptre i henhold til lovverket. For at et multistakeholder-initiativ skal kunne lykkes, må det finnes tydelig lovgiving og regulering (DeNardis & Raymond 2013), men fordi utviklingene i cyberspace skjer i høyt tempo sliter stater generelt med å opprettholde et oppdatert lovverk. Norge har ikke utviklet dekkende lovgivning og regulering i dette området, noe som påvirker mulighetene og evnen til å gjennomføre offentlig-privat samarbeid gjennom multistakeholder-initiativer. Steg har allikevel blitt tatt mot dette i 2016 ved at NORCERT og VDI ble forankret i lovverk slik det skisseres i stortingsproposisjon. 97 L (2015)–(2016) og Innstilling 352 L, vedtatt i Stortinget i juni 2016. Her oppfordres det også til opprettelse av

egne bransje-CERTer. Ved å oppfordre til dette ser vi en tydeliggjøring av ansvar i cyberspace fra statens side. Samtidig er konsekvensen at privat sektor får mer ansvar for sin egen cybersikkerhet, og dermed blir fortsatt NorCERT og VDI de viktigste instrumentene for cybersikkerhet på nasjonalt nivå. Istedenfor å jobbe for en forbedring av offentlig-privat samarbeid, kommunikasjon og dialog, blir NorCERT og VDI bindeleddet mellom sektorene. Initiativer for å forstå og overkomme maktdynamikken som oppstår i mellom partene blir ikke implementert.

VDI blir dermed det eneste offentlige tiltaket for offentlig-privat samarbeid for å sikre cyberspace. Om privat sektor ønsker å samarbeide med myndighetene for å beskytte offentlig infrastruktur, må de gjøre det ved å bli medlem av VDI-samarbeidet initiert av NSM. Samtidig står det tydelig i Personopplysningsloven fra 2000 at privat sektor ikke skal overvåke eller misbruke informasjon de kan få fra de tjenestene de yter. Ettersom VDI i praksis gir staten mulighet til å overvåke all datatrafikk som går ut og inn av medlemsbedriftenes nettverk, gir VDI i teorien også myndighetene tilgang til personinformasjon som kan samles fra denne datatrafikken. Den private sektoren står dermed overfor en direkte konflikt mellom statens ønske og oppfordring til å bruke VDI for å samarbeide med myndighetene på den ene siden, og lovgivning som sier at privat sektor må beskytte brukerne fra overvåkning på den andre (Personopplysningsloven - popplyl 2015). Resultatet av denne konflikten er at mange bedrifter, for eksempel NRK og Telenor, har meldt seg ut av VDI (Kibar 2015). Staten i sitt forsøk på å styre forstår ikke maktdynamikken og ender opp med å kontrollere for mye. Dette leder til at sentrale nasjonale bedrifter melder seg ut. Med store nasjonale bedrifter ute av det eneste samarbeidet som staten tilbyr, skapes det enda større avstand mellom offentlig og privat sektor i styringen av og sikkerheten av cyberspace. Ideen om multistakeholder-initiativer, altså at flere aktører går sammen for å arbeide mot et mål, blir dermed motarbeidet av statens egne reguleringer og lovverk.[18] Det er klart at mangelen på en tydelig ansvarsfordeling når det gjelder cybersikkerhet fører til at evnen til å styrke sikringen av cyberspace blir svekket.

Endringer i lovverket er et steg mot ansvarsfordeling, men mangelen på overordnet nasjonal organisering for cybersikkerhet er fortsatt tydelig. Dette leder til at interessekonflikter og en uklar fordeling av roller internt blant norske myndigheter med tanke på hvem som har ansvar for å gjøre hva i sikringen av cyberspace. Myndighetene har erkjent at staten må ta en større rolle i styringen av cyberspace. Dette er et relativt nytt område som øker i betydning, men effektiviteten i denne styringen hindres av forvirring rundt hvem som skal utøve den. Manglende klarhet gir staten begrenset beslutningsevne og kapasitet til å samarbeide med privat sektor. Myndighetene er avhengig av at de respektive departementene og deres

[18] Det private næringslivet spiller en viktig rolle i nasjonal cybersikkerhet. Telenor har her en unik rolle som eier av kritisk infrastruktur og innehaver av fagekspertise. Med bakgrunn i sitt forhold til det private næringslivet og sensorer i sitt nettverk, kan de oppdage angrep først og i enkelte tilfeller spille rollen som første forsvarslinje. Samtidig finnes det utfordringer når det gjelder informasjonsdeling mellom offentlig og privat sektor. Aktører i næringslivet har i lengre tid etterlyst mer informasjon fra offentlige myndigheter.

underliggende etater samarbeider på *ad hoc*-basis (Langø & Sandvik 2013). Et eksempel på dette finner vi i rapporten fra Lysneutvalget, der det påpekes at det er behov for et nasjonalt cybersenter, men at det fortsatt er stor uenighet i alle leirer om hva dette betyr og hvem som skal med (Justis- og beredskapsdepartementet 2015). For aktører fra privat sektor fører denne usikkerheten og mangelen på lederskap til at det er vanskelig å vite hvem i det offentlige de skal og kan kommunisere med. Det er tydelig at slike maktkamper mellom de forskjellige sektorene, og internt i staten leder til frustrasjon. Når staten fører en neo-liberal tankegang, uten at de samme premissene ligger til grunn som i andre domener, blusser uante og uforventede maktkamper opp.

Uten klare retningslinjer blir fordelingen av ansvar for sikkerheten mellom offentlig og privat sektor diffus. I det nåværende miljøet er privat sektor henvist til selv å tolke det eksisterende juridiske rammeverket i utformingen av sin egen rolle i arbeidet med cybersikkerhet. Hver enkelt bedrift blir slik overlatt til selv å avgjøre hva de vil gjøre og hvordan, ut fra egne økonomiske hensyn og kapasitet. I stedet for at staten tilrettelegger for samarbeid gjennom lovgivning, må privat sektor påta seg denne rollen, i den grad de selv ønsker å gjøre det. Sikkerheten i cyberspace er dermed avhengig av private bedrifters vilje til og interesse for å sikre sine egne tjenester – en avveining som ofte blir gjort i lys av lønnsomhetshensyn. Dette leder til at private sektoren tar ledelsen i utviklingen av cybersikkerhet, noe som fører til at markedet og den tekniske utviklingen fungerer som pådrivere for utviklingen som skjer og de avgjørelsene som blir tatt vedrørende cybersikkerhet. Dette er ikke unikt for Norge, det er en klar global trend at cyberspace får utvikle seg fritt, med kun marginal involvering av myndigheter på det tekniske og strategiske nivået. Ut fra et ønske om å la cyberspace utvikle seg fritt, har økonomisk lønnsomhet vært en sterk drivkraft. Regulering og lovgiving betyr ikke nødvendigvis at staten ønsker å begrense den private sektorens handlingsrom. Det kan derimot tydeliggjøre ansvars- og rollefordelingen og slik bidra til bedre cybersikkerhet. Staten og privat sektor arbeider fortsatt begge med cybersikkerhet, men dette er ukoordinert. En overordnet strategisk planlegging og tilrettelegging for samarbeid mangler, som fører til lite progresjon i styringen og sikringen av cyberspace.

Neo-liberalistisk tankegang, ide og i praksis

Statens utfordringen med å oppnå en multistakeholder tilnærming i arbeidet med cybersikkerhet ligger i statens ønske å ta ansvar for et område som hovedsakelig eies og driftes av privat sektor, samtidig som man bygger på eksisterende samarbeid og lovgivning for å skape og utvide et samarbeid. En svekket situasjonsforståelse og mangel på ansvar, kombinert med lovgivning som er vanskelig å tolke, fører til utilstrekkelig cybersikkerhet. Staten hevder at den legger til rette for samarbeid igjennom multistakeholder-initiativer, ved at samarbeid med privatsektor eksisterer igjennom VDI og ad hoc-møter. Det grunnleggende målet med multistakeholder-initiativer, nemlig å bringe de forskjellige aktørene sammen i dialog med hensikt å overkomme interessekonflikter og en kollisjon av ideer av hva det vil si å sikre cyberspace blir imidlertid ikke oppnådd. VDI er ikke ment til å være en multistakeholder-tilnærming til sikringen av

cyberspace, men det blir ofte presentert og referert til av staten, som bevis for godt samarbeid mellom staten og privat- og sivilsamfunnet.

Hovedproblemet ligger i hvordan styring utøves i praksis. Dette påvirker både aktørenes handlekraft, tilliten og samarbeidet dem imellom, noe som igjen resulterer i svekket samarbeid. Ved at staten betrakter cybersikkerhet som hovedsakelig et statlig problem, tilrettelegges det ikke for å bringe inn de ulike aktørene i privat og sivil sektor, for på denne måten å fostre samarbeid mellom partene. Samarbeidet mellom partene er ukoordinert. Dette påvirker alle nivåer av det som utgjør cybersikkerhet. Internt i staten er det en tydelig mangel på klarhet om hvem som har ansvar for hva innenfor cyberspace, og hvordan dette ansvaret skal utføres. Resultatet er en svak styring og retning i sikringen av cyberspace, som påvirker statens evne til å samarbeide med både privat sektor og sivilsamfunnet i en multistakeholder tilnærming.

Offentlig-privat samarbeid har en lang tradisjon. Det som er nytt i denne typen samarbeid i cyberspace er måten det blir omtalt på. Vi ser en diskurs som bryter med avgrensinger på et nasjonalt plan mot en vektlegging på innovasjon og fleksibilitet, hvor multistakeholder blir forbundet med gjensidig ansvar og tillit (Carr 2016). Selv om staten til en viss grad har vært involvert i utviklingen av internett, har det fra tidlig av vært en forventning om at staten bare skal spille en minimal rolle i utviklingen av teknologien. Problemet er at det er en gjennomgående manglende tydelighet på hva og hvordan rollen til staten skal være i dette forholdet. Dunn Cavelty og Brunner (2007) har observert at teknologiske utviklinger forsterker to trender som minsker statens rolle, som begge har implikasjoner for nasjonal cybersikkerhet: økt internasjonalisering og privatisering. Disse trendene er tydelige i Norges utvikling av cybersikkerhet, og kan sees å ha manifestert seg i forsøkene på å oppnå multi-stakeholder initiativer. Spenningen vi ser i dag i initiativene omhandler et helt sett med oppfatninger om de respektive rollene staten og privat sektor skal ha, og om forholdet mellom økonomisk utvinning og nasjonal sikkerhet.

Fordi cyberspace i stor grad har blitt utviklet og drevet av privat sektor, er det vanskelig å finne klare eksempler på privatisering av cyberspace. Styringsrasjonaliteten som blir implementert i dag er ikke et resultat av en endret logikk eller en ny rasjonalitet. I motsetning til andre områder der staten fungerer som en tilrettelegger, har staten aldri hatt noen direkte kontroll over cyberspace. Implementeringen og bruken av multistakeholder-initiativer for cybersikkerhet er dermed ikke et klart tilfelle av privatisering. Staten påtar seg en rolle som tilrettelegger for samarbeid og samhandling mellom staten og privat sektor, men uten å ta hensyn til sin egen eller privat sektors rolle og makt. Maktdynamikken i cyberspace er forskjellig fra andre områder hvor staten og privat sektor samarbeider gjennom multistakeholder initiativer, da staten aldri har hatt kontroll i cyberspace. Dermed er det vanskelig for staten å prøve å styre cyberspace igjennom multistakeholder-initiativer. Ved at maktdynamikken mellom de forskjellige partene ikke blir tatt hensyn til i de statlige multistakeholder-initiativene er suksessen og innflytelsen deres på sikringen av cyberspace begrenset.

Konklusjon

For å iverksette samarbeid mellom staten, privat sektor og det sivile samfunn om sikkerhet i cyberspace, blir multistakeholder-initiativer i dag initiert som en del av et neo-liberalistisk styresett. Allment betraktes dette av politikere som et universalmiddel for å oppnå cybersikkerhet, og tilnærmingen blir implementert både nasjonalt og internasjonalt. Det siste tiåret har multistakeholder-initiativer blitt så fremholdt i cyber-sammenheng at de nesten har blitt et synonym for styringen av det. Som et styringsverktøy for å oppnå cybersikkerhet regnes multistakeholder-initiativer ikke bare av mange som den beste måten å organisere seg rundt problemet på; de holdes også opp som en mal for hvordan vi best kan håndtere andre utfordringer som oppstår som følge av globalisering (Carr 2015). Denne artikkelen har imidlertid vist at i stedet for å være basert på en dypere analyse av maktdynamikk, er det *konseptet* multistakeholder som former, om ikke definerer, dagens tilnærming til arbeidet med cybersikkerhet. Maktdynamikken mellom partene blir ikke tatt hensyn til i implementeringen av multistakeholder-initiativene, noe som igjen påvirker deres funksjon. Ved å se nærmere på initiativene for multistakeholder-samarbeid i Norge, har denne artikkelen tatt et steg mot å forstå hvorfor modellen ikke fungerer i arbeidet med cybersikkerhet. Gjennom en analyse av maktforholdet mellom offentlig og privat sektor i styringen av cyberspace, har jeg satt fokus på de politiske faktorene rundt det tekniske miljøet. Videre har det blitt tydelig at det pågår en maktkamp internt i staten, og at dette igjen leder til problemer i implementeringen av en multistakeholder-tilnærming til cybersikkerhet. Multistakeholder-initiativer kan være et godt grunnlag for en styringsrasjonale i forhold til cybersikkerhet, om den blir fulgt, men den må ikke bli betraktet som en verdi i seg selv (Dunn Cavelty & Suter 2012).

Stater søker naturlig mot sentraliserte, formaliserte institusjoner. I den grad disse institusjonene blir betraktet som dominerende plattformer for styringen av cyberspace og internett, får de en mer betydningsfull tilstedeværelse og en økende innflytelse på stater. Både myndigheter og ikke-statlige aktører villedes av antagelsen om at internasjonale multistakeholder-initiativer slik som IGF faktisk forbedrer cybersikkerheten. Omfanget av saker som blir satt på dagsorden fortsetter derfor å øke, til tross for institusjonenes begrensede mandat og evne til å gjennomføre tiltak. Dette har konsekvenser for forståelsen av statens rolle i styringen av cyberspace. Konsekvensen av dette er at «feil» aktører sitter ved bordet, og at de som har den faktiske tekniske ekspertisen og autoriteten i cyberspace blir utestengt. Resultatet er uklarhet om hvem som skal inkluderes i de ulike tiltakene som i dag finnes på området cybersikkerhet både nasjonalt og internasjonalt og svake institusjoner for å styre og sikre cyberspace.

I tillegg til de aspektene av teknisk koordinering som i dag blir implementert i arbeidet med cybersikkerhet, må også de politiske og juridiske aspektene erkjennes og inkluderes i denne styringsrasjonaliteten. Samarbeid og koordinering er nødvendig, men dette må gjøres på grunnlag av en type forvaltning som er optimal for å fremme en balanse av samarbeid, hvor alle interessenter er bevisste på makt- og

konflikt-elementene blant aktørene. En åpen form for samarbeid må være basert på en idé om likeverdige partnere, med mål om å legge best mulig til rette for samarbeid mellom privat, offentlig sektor og sivilsamfunnet. Gitt at disse initiativene er vanskelige å få til i en nasjonal setting, er det lite som tyder på at det da skal kunne fungere internasjonalt. Om vi ikke får det til nasjonalt i Norge, hvor tilliten mellom offentlig og privat sektor er relativ høy, er det ikke rart at modellen ikke fungerer internasjonalt, der tilliten er lavere og det historisk har vært mindre samarbeid. For å lykkes i arbeidet med cybersikkerhet må både sivilsamfunnet og de som har teknisk kontroll over cyberspace – dvs. de som skaper, opprettholder og eier alt som utgjør det – forstås og inkluderes, både nasjonalt og internasjonalt, i avgjørelsene om hvordan dette domenet skal sikres og styres. Privatsektorens ideer og diskurs, påvirker hvordan systemet blir opprettet og bygd. Ved å være initiert av stater og med et fokus på myndigheter som hovedaktører på området cybersikkerhet, utestenger dagens tilnærminger de grunnleggende aktørene som kunne gjort dagens initiativer til å sikre cyberspace til virkelige multistakeholder-initiativer. De som utformer og regulerer Internett og sørger for at det fungerer ved hjelp av avtaler mellom internettleverandører (ISPs), rutere, statlig filtrering og kontroll av nettsøppel, opphavsrett og botnet, opererer på det nasjonale nivået, og blir verken inkludert eller forstått innenfor den globale styringsrasjonaliteten som i dag ledes i arbeidet med cybersikkerhet. Dette reflekterer dypere problemer forbundet med bruken av multistakeholder-initiativer som globale tiltak for å styre cyberspace.

Litteratur

Auerswald, Philip E. Lewis M. Branscomb, Todd M. LaPorte & Erwann O. Michel-Kerjan (2007) *Seeds of disaster, roots of response: how private action can reduce public vulnerability.* Cambridge: Cambridge University Press.

Balzacq, Thierry & Myriam Dunn Cavelty (2016) «A theory of actor-network for cyber-security», *European Journal of International Security / First View* Article. 1–23.

Bauer, Johannes M. (2005) «Internet governance: theory & first principles», Paper presented at the 33rd annual telecommunication policy research conference, Arlington, VA, September 23–25.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb & Lei Zhou (2003) «The economic cost of publicly announced information security breaches: Empirical evidence from the stock market», *Journal of Computer Security,* 11: 431–448.

Carr, Madelin (2016) «Public–private partnerships in national cyber-security strategies», *International Affairs*, 92 (1): 43–62.

Carr, Madeline (2015) «Power Plays in Global Internet Governance», *Millennium: Journal of International Studies*, 43 (2): 640–659.

Chakravarty, P. (2006) «Who Speaks for the Governed? World Summit on Information Society, Civil Society and the Limits of 'Multistakeholderism'», *Economic and Political Weekly*, 41 (3): 250–257.

Dahl, Robert A. (1957) «The concept of Power», *Behavioral Science*, 2 (3): 201–215.

DeNardis, Laura & Mark Raymond (2013) «Thinking Clearly about Multistakeholder Internet Governance.» Paper presented at eighth annual GigaNet Symposium, Bali, Indonesia, October 21.

Departementene. (2012). Nasjonal strategi for informasjonssikkerhet. Regjeringen. Lastet ned 10. august, 2015. https://www.regjeringen.no/globalassets/upload/fad/vedlegg/iktpolitikk/nasjonal_strategi_infosikkerhet.pdf

Drezner, Daniel W. (2004) «The global governance of the Internet: bringing the state back in», *Political Science Quarterly*, 119: 447–498.

———— (2007) *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton, NJ: Princeton University Press.

Dunn Cavelty, Myriam (2012) «The militarisation of cyber security as a source of global tension», in *Strategic Trends Study*, Daniel Möckli & Andreas Wenger (red.). Zurich: Center for Security Studies.

Dunn Cavelty, Myriam & Elgin M. Brunner (2007) «Introduction: information, power, and security—an outline of debates and implications», i Myriam Dunn Cavelty, Victor Mauer & Sai Felicia Krishna-Hensel (red.), *Power and security in the information age: investigating the role of the state in cyberspace*. Aldershot: Ashgate. 8–9.

Dunn Cavelty, Myriam & Manuel Suter (2009) «Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection», *International Journal of Critical InfraStructure Protection*, 2 (4): 179–187.

———— (2012) *Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection*. Zurich: Center for Security Studies.

Dunn, James A. (1999) «Transportation: policy-level partnerships and project-based partnerships», *American Behavioural Scientist*, 43: 92–106.

Dunn, Myriam & Victor Mauer (red.). (2006) «Analyzing Issues, Challenges, and Prospects», *International CIIP Handbook 2006, Vol. II*: 69–88. Center for Security Studies, Zurich.

Eeten, Michel J.G. & Milton Mueller (2013) «Where is the governance in Internet governance?» *New media & society*, 15 (5): 720–736.

Farrell, Maria (2016) «Quietly, symbolically, US control of the internet was just ended», The Guardian 14 mars. *ISSN 0261-3077. Retrieved 2016-03-17*

Froomkin, A. Michael (2003) «ICANN 2.0: meet the new boss», *Loyola of Los Angeles Law Review*, 36 (3): 1087–1102.

Garvin, Michael J. & Doran Bosso (2008) «Assessing the effectiveness of infrastructure public–private partnership programs and projects», *Public Works Management and Policy*, 13 (2):162–78.

Goldsmith, Jack & Tim Wu (2006) *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.

Hodge, Graeme A. & Carsten Greve (2007) «Public–private partnerships: an international performance review», *Public Administration Review*, 67 (3): 545–58.

Huijstee, Mariette V. (2012) *Multistakeholder initatives: A strategic guide for civil society organizations*. Stichting Onderzoek Multinationale Ondernemingen. Amsterdam: The Netherlands.

ICANN (2014) "ICANN Bylaws" Lastet ned 30. juni 2015 https://www.icann.org/resources/pages/governance/bylaws-en

ICANN (2016a) "ICANN's Major Agreements and Related Reports", ICANN Lastet ned 30. juni 2016 https://www.icann.org/resources/pages/agreements-en

ICANN (2016b) "Inventory of ICANN Accountability Efforts." ICANN Lastet ned 30. juni 2016 http://learn.icann.org/mod/page/view.php?id=1197

ICANN (2016c) "IANA Functions Stewardship Transition Overview." ICANN Lastet ned April 21, 2016. https://www.icann.org/stewardship

Innst. 352 L. Innstilling til Stortinget fra utenriks- og forsvarskomiteen Prop. 97 L (2015–2016). Lastet ned 1. september 2016 https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2015-2016/inns-201516-352.pdf

Justis- og beredskapsdepartementet (2015) Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden. Regjeringen. Lastet ned 10. januar 2016 https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

Kibar, Osman (2015) «Får kopi av datatrafikken til store norske selskaper», *Dagens næringsliv.* 4. desember. Lastet ned 10. januar 2016 http://www.dn.no/magasinet/2015/12/04/2121/Teknologi/fr-kopi-av-datatrafikken-til-store-norske-selskaper?service=print

Kirknes, Leif M. (2010) «Flere kritiske til NSM-samarbeid», *Computer World*, December 1. Lastet ned 13, juni 2015. http://www.cw.no/artikkel/offentlig-sektor/flere-kritiske-til-nsm-samarbeid

Klein, Hans (2004) «Understanding WSIS: an institutional analysis of the UN world summit on the information society», *Information Technology & International Development*, 1 (3–4): 3–14.

Kleinwächter, Wolfgang (2004) «WSIS: a new diplomacy? Multistakeholder approach and bottom up policy in global ICT governance», *Information Technology & International Development*, 1 (3–4): 3–13.

Koppell, Jonathan G.S. (2005) «Pathologies of accountability: ICANN and the challenge of «multiple accountabilities disorder», *Public Administration Review,* 65 (1): 94–108.

Kummer, Markus (2013) «Multistakeholder Cooperation: Reflections on the emergence of a new phraseology in international cooperation, Internet Society», *Internet Society* May 14. Lastet ned 29. juni, 2015.

http://www.internetsociety.org/blog/2013/05/multistakeholder-cooperation-reflections-emergence-new-phraseology-international

Linder Stephen H. (1999) «Coming to terms with the public–private partnership: a grammar of multiple meanings», *American Behavioral Scientist*, 43 (1): 35–51.

Lindsay, Jon R., Tai Min Cheung & Derek S. Reveron (2015) *China and Cybersecurity.* New York: Oxford University Press.

Lukes, Steven (1974) *Power: A Radical Veiw*, Second edition. Palgrave.

Lukes, Steven (2001) «*Robert Dahl on power*», *Journal of Political Power*, 8 (2): 261–271

Mueller, Milton L. (2010). «Networks and States: The Global Politics of Internet Governance», *Networks and States: The Global Politics of Internet Governance*. MIT press.

Mueller, Milton L. (2013) Is there any hope for the internet governance forum? The internet governance forum. http://www.internetgovernance.org/2012/07/30/is-there-any-hope-for-the-internet-governance-forum/. Accessed November 5, 2016.

Muller, Lilly Pijnenburg (2016) Security for whom? Internet governance through the World Summit on the Information Society (WSIS), Working paper presented at the 41th annual British International Security Assosiation (BISA), Edinburg, June 15–17.

Neumann, Iver B. & Ole Jacob Sending (2010) *Governing the Global Polity.* Ann Arbor: University of Michigan Press.

Pavan, Elena & Mario Diani (2008) «Structuring online and offline discursive spaces of Internet governance: insights from a network approach to map an emerging field», Paper presented at the annual GigaNet symposium, Hyderabad, India, December 2.

Personopplysningsloven - popplyl 2015 Justis- og beredskapsdepartementet fra 01.10.2015

Pongsiri, Nutavoot (2002) «Regulation and public–private partnerships», *International Journal of Public Sector Management*, 15 (6): 487–95.

Sahel, Jean-Jacques (2016) «Multi-stakeholder governance: a necessity and a challenge for global governance in the twenty-first century», *Journal of Cyber Policy*, 1 (2): 1–19.

Sandvik, Kristin B. & Hans-Inge G. Langø (2013) «Cyberspace og sikkerhet», *Internasjonal Politikk*, 71 (2): 221–228.

Schaferhoff, Marco, Sabine Campe & Christopher Kaan (2009) «Transnational public–private partnerships in International Relations: making sense of concepts, research frameworks, and results», *International Studies Review*, 11 (3): 451–74.

Stevens, Tim (2016) «Cyber Secuirty and the Politics of time», Cambridge: Cambridge university press

Stiglitz, Joseph E. & Wallsten, Scott J. (1999) «Public–private technology partnerships: promises and pitfalls», American *Behavioral Scientist*, 43: 35, 57.

Sveinbjørnsson, S. (2012) «NRK kastet ut statens "spionboks"», *Digi.no*, 5. november 5. Lastet ned 1. august 2015. http://www.digi.no/sikkerhet/2012/11/05/nrk-kastet-ut-statens-spionboks

Telenor (2015) «Høring – forslag til endringer i sikkerhetsloven», ref: 2015-9042. Forsvarsdepartementet.

The Economist (2009) *Regulating the Internet: ICANN be independent*. ICANN September 24. Accessed July 2, 2015. http://www.economist.com/node/14517430

Wettenhall, Roger (2003) «The rhetoric and reality of public–private partnerships», *Public Organization Review: A Global Journal*, 3 (1): 77–107.