Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 77, Nummer 3, side 225-240, 2019, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert september 2019

Fokus: Cybersikkerhet

Internett som geopolitisk arena?

Bjørn Svenungsen
Gjesteforsker, Institutt for Forsvarsstudier

Sammendrag

Internett er i dag verdens viktigste infrastruktur. Dets formidable suksess er bygget på prinsipper om åpenhet, frihet, robusthet og sikkerhet. Dette er prinsipper som viser seg stadig vanskeligere å forene. Internetts grunnleggende arkitektur er i liten grad konstruert for å ta hensyn til geografiske grenser. Staters behov for suverenitetshevdelse, kontroll og sikkerhet har likevel skapt en utvikling i retning av «cybersuverenitet» som er i ferd med å endre internett slik vi kjenner det, hvor nettverkene og deres underliggende arkitektur i økende grad inngår i staters geopolitiske ambisjoner. Dette er fortellingen om den viktigste globale konflikten du aldri har hørt om.

Nøkkelord: internett · cybersikkerhet · suverenitet · geopolitikk · internettforvaltning · cyberspace · Russland · Kina · USA

Internett er ryggraden i global handel og kommunikasjon og utgjør i dag verdens viktigste infrastruktur. Man hører tidvis argumenter for at internett er et «globalt fellesområde» på linje med luft og hav. Det er det ikke. Stater har jurisdiksjon over den fysiske infrastrukturen som utgjør internett og den informasjonen som flyter gjennom det. Men internett er en infrastruktur som ikke er designet for å ta hensyn til geografiske grenser. Det er nettverkene som utgjør «grensene».

Tradisjonelt er prinsipper om suverenitet knyttet til statens selvbestemmelse innenfor et geografisk definert område. For internett er det hovedsakelig ikke-statlige aktører som besørger eierskap, utvikling og forvaltning. Like fullt er internett det desidert største og viktigste digitale rom for utøvelse av staters cybermakt. Men hva innebærer egentlig statlig suverenitet over internett? Kan et grunnleggende

*Kontaktinformasjon: Bjørn Svenungsen, e-post: bjorn.svenungsen@ifs.mil.no

Citation: Bjørn Svenungsen (2019). Internett som geopolitisk arena?. Internasjonal Politikk, 77(3): 225–240. http://dx.doi.org/10.23865/intpol.v77.1403

anti-westfalsk internett tilpasses tradisjonelle westfalske prinsipper og inngå i en geopolitisk logikk?

Artikkelen argumenterer for at statsmaktens behov for suverenitetshevdelse, kontroll og sikkerhet har trumfet internetts grunnleggende prinsipper om åpenhet frihet og vil være førende for fremtidens internett. Cybersuverenitet, hvor enn paradoksalt det er, har kommet for å bli.

For å forstå hvorfor bør vi først forstå hvordan internett startet og utviklet seg.

Begynnelsen

Reklamemannen Neal Hosler McElroy fra Ohio gjorde suksess hos såpeprodusenten Procter & Gamble på 1930- og 1940-tallet ved å koble såpereklame til radioprogram myntet på hjemmeværende kvinner. Radioprogrammene ble kjent som såpeopera (Bing, 2009). McElroy var avbildet på forsiden av Time Magazine i 1953 som en reklameguru i sin tid. Da han i 1958 for andre gang preget forsiden var han forsvarsminister, utnevnt av President Eisenhower året før som USAs første forsvarsminister uten militær bakgrunn. Såpeindustrien hadde lært McElroy verdien av uavhengig forskning, en erfaring han tok med seg til Pentagon.

Omtrent samtidig hadde Sovjetunionen sendt verdens første ubemannede satellitt ut i verdensrommet. Den ferske forsvarsministeren måtte legge fram en plan for kongressen for hvordan USA skulle møte denne utfordringen. McElroys plan inkluderte å etablere et sivilt forskningsbyrå under Forsvarsdepartementet for å finansiere langsiktig forskning av militær relevans. Byrået fikk navnet Advanced Research Projects Agency (ARPA) (Bing, 2009).

ARPA etablerte samarbeid med dataforskningssentre ved flere universitet i USA, som etterhvert etterlyste mer datakraft. Rob Taylor ved ARPA foreslo en løsning som gikk ut på å etablere elektroniske linker som koblet datamaskinene ved de ulike sivile forskningsinstitusjonene sammen for å kunne dele kunnskap og unngå duplisering av arbeid (Bing, 2009). Det ble starten på ARPANET som begynte med fire sammenkoblede datamaskiner ved like mange universitet. ARPANET var operativt fra høsten 1969.

Nettverket av tilkoblede forskningsinstitusjoner vokste raskt. Innen 1973 var 35 noder koblet til. Samme år ble Norge, som det første land i verden utenfor USA, koblet til nettverket.

Nye nettverk ble etablert og koblet til ARPANET samtidig som det ble utviklet bedre løsninger for kommunikasjon mellom datamaskinene i nettverkene. PCer ble koblet sammen i lokale nettverk (LAN – Local Area Network) og LANer ble koblet sammen gjennom ARPANET[1] (Bing, 2009, s. 34).

[1] I 1973 utviklet selskapet Xerox PARC et lokalt nettverk mellom egne maskiner som de kalte Ethernet. I august 1981 lanserte IBM sin første PC, som førte til en rask økning av antall datamaskiner både i offentlig og privat sektor.

Pentagon finansierte utviklingen av ARPANET fordi de ønsket et system som kunne gjøre militært personell i stand til å kommunisere sømløst uavhengig av hva slags infrastruktur eller fysisk medium som ble benyttet (Mueller, 2017, s. 8).

I begynnelsen fokuserte man i liten grad på sikkerhet i nettverkene. En av prosjektlederne for ARPANET skal angivelig ha sagt at å stille sikkerhetskrav til nettverket ville være som å kreve at Wright brødrenes aller første flyvning skulle være minst 50 miles og ha med 20 passasjerer. De hadde mer enn nok med å få nettverket til å virke (Kaplan, 2016).

Men utviklingen skjøt fart. Helt avgjørende var Vinton G. Serf og Robert E. Kahns utvikling av den tekniske standarden Transmission Control Protocol (TCP) i 1977. Jon Bing sammenlignet TCP med en fraktcontainer som kan bli pakket med hva som helst og hvor det ikke spiller noen rolle om den fraktes med tog, skip, lastebil eller noe annet. Det eneste som trengs er utstyr som kan flytte containeren fra en transportmåte til en annen og at containeren er merket på riktig måte med riktig adresse. På samme måte kan TCP pakke hvilken som helst informasjon og bevege seg på tvers av nettverk på sin vei fra sender til mottaker, hvor gateway-computere sørger for å motta dataene fra én infrastruktur og sende de videre ved hjelp av en annen. TCP gjorde det enkelt å sende informasjon gjennom nettverket. Året etter ble standarden Internet Protocol (IP) lagt til TCP [2]. Fra 1983 ble kun systemer som brukte TCP/IP akseptert på ARPANET (Bing, 2009)[3].

Internettets æra hadde begynt. Kommersiell virksomhet var imidlertid ikke tillat over internett før i 1991 da de siste restriksjonene ble fjernet (Bing, 2009, s. 37). Det åpnet for en bruk av nettverkene som senere skulle få stor betydning for global handel og økonomi.

Samme år lanserte CERN-forskeren Tim Berners-Lee et system som muliggjorde deling av informasjon over internett på helt nye måter. Han kalte systemet World Wide Web. To år senere ble den første nettleseren (Mosaic 1.0) lansert og i 1995 den første søkemotoren (Alta Vista) (Bing, 2009). Berners-Lees innovasjon ble en suksess, for å si det forsiktig. I dag er det over 1,7 milliarder nettsider på World Wide Web (Internet Live Stats 2018).

Det er ikke uvanlig å høre web og internett bli omtalt om hverandre, som om det skulle være en og samme ting. Det er det altså ikke. World Wide Web er en (av mange) måter å kommunisere over internett på. Internett er en fysisk infrastruktur.

Fra ett nettverk med fire sammenkoblede enheter i 1969 består internett i dag av over 40 000 ulike nettverk (Lee, 2018) og rundt 25 milliarder tilkoblede enheter

[2] IP tok seg av rutingen av datapakkene, TPC tok seg av pakking, feilkontroll og utpakking. Enhver digital enhet som er tilkoblet internett har en unik IP-adresse.

[3] I 1982 hadde det amerikanske forsvaret gjennomført omfattende testing av TCP/IP som standard for kommunikasjon mellom militære enheter, blant annet gjennom øvelser hvor FFI på Kjeller deltok (Hagen, 2007, s. 145). E-post var allerede fra tidlig på 70-tallet muliggjort gjennom en egen protokoll, Simple Mail Transfer Protocol – SMPT.

(Statista, 2018)[4] som alle kan kommunisere med hverandre.[5] Taylors spede forsøk på slutten av 60-tallet har utviklet seg til å bli verdens viktigste infrastruktur.

Det frie, åpne internett

Internetts suksess, vil mange hevde, skyldes fraværet av en styrt utvikling og liten grad av innblanding fra statlige myndigheter. Både utviklere og forvaltere av internett har i all hovedsak delt oppfatningen om at internett skal være basert på åpne standarder, transparens og samarbeid, samt produkter og infrastruktur med spredt eierskap og kontroll. Selvregulering har vært idealet. Frihet er et annet nøkkelord i «the Internet Community». Ikke bare frihet til innovasjon, utvikling og ytringer men også frihet fra det etablerte. Science-fiction forfatteren Bruce Sterling formulerte det slik i 1993:

> *Why do people want to be "on the Internet?" One of the main reasons is simple freedom. The Internet is a rare example of a true, modern, functional anarchy … There are no official censors, no bosses, no board of directors, no stockholders … The Internet belongs to everyone and no one.* (Sterling, 1993)

På større konferanser om internett kan man fortsatt møte mennesker som oppgir «the internett» når man spør hvor de kommer fra. Mennesker med en ide om at man på internett tilhører et fellesskap på utsiden av det etablerte, hvor individuell frihet og selvregulering er normen. Den kanskje mest kjente talsmann for dette er John Perry Barlow som i sin ikoniske Declaration of Independence of Cyberspace fra 1996 skrev:

> *Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.* (Wikipedia, 2018)[6]

«Governments of the industrial world» fulgte ikke Barlows oppfordring. Tvert imot. I dag forsøker stater i økende grad å etablere «suverenitet» etter territorielle prinsipper over internett og det er censors, bosses, board of directors og stockholders som i betydelig grad kontrollerer nettverk og innhold.

---

[4] Antall tilkoblede enheter vokser raskt og forventes å nå rundt 75 milliarder i 2025.

[5] Hovedsakelig ved hjelp av TCP/IP standarden. Det har riktignok blitt utviklet flere standarder etterhvert, for eksempel User Datagram Protocol (UDP), men grunnprinsippene – å sende pakker med data – er de samme. Det er utenfor denne artikkelens hensikt å beskrive forskjeller mellom de ulike internettprotokoller.

[6] Barlow, kjent bl.a. som poet og aktivist var også med å grunnlegge Electronic Frontiers Foundation (EFF) i 1990 hvor han satt i styret til sin død i 2018. EFF arbeider for digitale rettigheter og skulle blant annet ta opp "inevitable conflicts that have begun to occur on the border between Cyberspace and the physical world".

Samtidig, og dette er et viktig poeng, *forvaltes* internett fortsatt av et komplekst økosystem av organisasjoner, enkeltindivider, private selskap, myndigheter og løst sammensatte ad-hoc grupperinger, ofte med uklare grenser og løse eller ingen formelle mandat.[7] Internett forvaltes av «the multistakeholder community», som kort fortalt betyr alle som ønsker å engasjere seg.[8]

Det er heller ingen internasjonal konvensjon eller avtale som regulerer hvordan internett skal forvaltes. Privatrettslige forhold har en fremtredende plass.

Global forvaltning – USA «gir bort» internett

Den raske veksten i antall nettverk og computere på 70- og 80-tallet var en utfordring. (Bing, 2009, s. 35)[9] Hver datamaskin måtte ha en unik identifikasjon for å kunne finne hverandre i nettverket. Løsningen ble DNS, Domain Name System, utviklet i 1983.

DNS er kort fortalt et hierarkisk system for å kartlegge, fordele og registrere domenenavn, for eksempel .no eller .com. Det oversetter domenenavn til numeriske adresser slik at datamaskiner kan finne hverandre i nettverket. Kjernen i systemet er en database med informasjon over hvilke domenenavn som huser den enkelte IP-adresse. Filene med denne informasjonen kalles «rot» og serverne hvor disse filene er lagret kalles «rotservere» (Bygrave et al., 2009, s. 150). I dag har internett 13 rotservere som drives av ulike private selskap og organisasjoner. 10 av disse er lokalisert i USA, de øvrige tre i Japan, Nederland og Sverige.

Fra 1986 ble DNS tatt i bruk av alle nettverk etter krav fra ARPA året før. The Internet Assigned Number Authority (IANA) ble etablert på 1980-tallet, lokalisert ved Universitetet i Sør-California. Gjennom en kontrakt med ARPA sørget IANA for tildeling av globale unike navn og nummer i internettprotokollene og tildeling av IP-adresser. IANA administrerer således internetts rotfiler.

---

[7] Med forvaltning i denne sammenheng menes i hovedsak forvalterne av de såkalte grunnleggende internettressurser, altså kjernearkitektur og infrastruktur for kommunikasjon over internett, altså den tekniske delen som ligger i bunn for alt vi kan gjøre med og i internett, som det er nødvendig å ha en viss forståelse av også når vi diskuterer geopolitikk i det digitale rom. I tillegg til de nedenfor nevnte IANA og ICANN er noen av de viktigste aktørene Internet Architecture Board (IAB), Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C) og Internet Society (ISOC). Det blir for omfattende for denne artikkelen, og det er heller ikke dens hensikt, å beskrive de mange organisasjoner og grupperinger som i dag håndterer den globale forvaltningen av internett. Det er imidlertid viktig å være klar over at det ikke er én «styrer» eller øverste forvalter av internett.

[8] Internet Engineering Task Force (IETF) for eksempel, har individuelle medlemskap hvor enhver som ønsker det kan delta på møtene. Mottoet deres er *rough consencus and running code*. Overordnet er et åpent, velfungerende og stabilt internett.

[9] Problemene begynte å bli åpenbare da antallet datamaskiner tilkoblet nettet oversteg 2000.

ARPANET ble delt i en sivil og en militær del i 1984[10]. I årene som fulgte vokste det fram en rekke nye sivile nettverk og private internett-tilbydere. Et forslag fra National Telecommunications and Information Administration (NTIA) i 1998 om å privatisere DNS-forvaltningen førte til etableringen av Internet Corporation for Assigned Names and Numbers (ICANN) i september samme år.[11] Fra 1. januar 1999 overtok ICANN IANA-funksjonen i tillegg til sivile registreringsoppgaver National Science Foundation hadde hatt ansvar for. (Bing, 2009)

ICANN er en non-profitt stiftelse registrert i California og følgelig underlagt amerikansk lov. ICANNs avtale var med NTIA/Handelsdepartementet[12] som formelt skulle godkjenne enhver beslutning av betydning. Med andre ord hadde den til enhver tid sittende amerikanske administrasjon *i teorien* kontroll over internetts rotfiler og toppdomenene i DNS.

Da Clinton-administrasjonen etablerte ICANN var den angivelig bekymret for at dersom internett ble forvaltet av en multilateral organisasjon[13] ville det bli sårbart for myndighetskontroll og sensur, og samtidig risikere en oppdeling i regionale eller nasjonale nettverk uten felles DNS-rot og følgelig ikke lenger være ett globalt internett. Denne multistakeholder-tilnærmingen ble samtidig ansett som attraktiv for den amerikanske administrasjonen da internettforvaltningen allerede var dominert av amerikanske teknologiselskap, forskningsmiljøer og sivilsamfunn (Raustiala, 2017). ICANN ble gitt stadig mer autonomi i kontrakten med NTIA og etterhvert var amerikanske myndigheters rolle mest av symbolsk karakter. Obama-administrasjonen besluttet å avslutte kontrakten med ICANN og med det fullføre privatiseringsprosessen av DNS-forvaltningen som startet i 1998 (NTIA, 2014, se også Bygrave & Michaelsen, 2009, s. 106).[14]

President Obama møtte kritikk fra høyresiden i amerikansk politikk for å «gi bort» internett til det internasjonale samfunn. John Bolton, President Trumps

[10] National Science Foundation (NSF) etablerte et eget nettverk (Computer Science Research Network, CNET) som førte til delingen mellom et sivilt og et militært nettverk. MILNET for ugradert militær kommunikasjon og ARPANET heretter kun til forskning og ikke-militær bruk. I 1985 etablerte NSF et nettverk mellom fem super- data-sentre i USA, NSFNET, et «backbone network» akademiske institusjoner kunne koble seg til. Snart var langt flere computere koblet til NSFNET enn ARPANET som bare ble ett av hundrevis av nettverk. ARPANET ble nedlagt i 1989, 20 år etter oppstarten.

[11] NTIA er et direktorat under Handelsdepartementet (U.S. Department of Commerce). I årene forut for etableringen av ICANN var det nedlagt et betydelig politisk arbeid for å utvikle og fremme internett og å privatisere IANA funksjonen. Særlig aktiv var senator, senere Visepresident Al Gore.

[12] Altså ikke med ARPA, som nå hadde fått tilføyd en D for Defence og het DARPA, slik tilfellet var da Universitetet i Sør-California besørget IANA-funksjonen.

[13] International Telecommunications Union (ITU) var mest nærliggende etter ulike initiativ derfra i siste halvdel av 1990 tallet. ITU er et FN-organ for global standardisering innen telekommunikasjon, med hovedkontor i Genéve.

[14] Nyheten ble offentliggjort i en pressemelding i mars 2014. Allerede i januar 2008 ba ICANN om at avtalen med NTIA ble avsluttet og at amerikanske myndigheter ga fra seg all formell kontroll over stiftelsen og DNS-forvaltningen.

nåværende sikkerhetsrådgiver, karakteriserte Obamas beslutning som «a mistake of such colossal proportions …». Senator Ted Cruz sa: «Like Jimmy Carter gave away the Panama Canal, Obama is giving away the internet». (Raustiala, 2017, s. 140)

Republikansk kritikk og forsøk på rettslige skritt til tross, den 1. oktober 2016 utløp kontrakten med ICANN samtidig som organiseringen av ICANN ble noe justert. «The internet community» hyllet Obamas beslutning som en triumf for det frie, åpne nettet.

Amerikanske myndigheters formelle kontroll over rotfilene kombinert med internetts voksende økonomiske og sikkerhetspolitiske betydning har vært gjenstand for misnøye blant flere stater, noe særlig Russland og Kina har gitt uttrykk for. Også de ønsket Obamas beslutning velkommen men tilstreber en større grad av statlig kontroll over alle nivå av internettforvaltningen.[15]

Mot Cybersuverenitet?

Den eneste måten for en stat å oppnå fullstendig suverenitet over «internett» er å etablere egne nettverk med en egen statskontrollert DNS-rotserver. Det er fullt mulig[16]. Men nettverk uten kontakt med ICANNs DNS-rotservere er ikke lenger en del av det åpne, globale internett vi kjenner i dag. Dersom et land stenger tilgangen til DNS-roten vil man samtidig stenge landet ute fra internasjonal luftfart, skipsfart, osv. Selv de mest kontrollivrige diktaturer i verden har neppe noe ønske om det. (Mueller, 2017, s. 41)

Det har imidlertid vært flere forsøk fra stater på å endre den globale internettforvaltningen til et mer statskontrollert DNS uten samtidig å koble seg permanent fra det eksisterende DNS, slik at myndighetene selv har kontroll på rotservere som håndterer internettrafikken i eget land. Dagens rotservere er «speilet» i hundrevis av servere verden over som dupliserer informasjonen på rotserverne. Det gjør blant annet at rutingen og informasjonsutvekslingen går mye raskere og at internett fungerer dersom en eller flere av rotserverne faller ut. «Speilserverne» er imidlertid ikke nok til å berolige myndighetene i land som Kina, Russland og Iran, som frykter at amerikanske myndigheter i en gitt situasjon kan påvirke rotfilene slik at for eksempel informasjon og internettrafikk rutet til eller fra disse landene blir påvirket.

---

[15] For å forklare den globale forvaltningen av internett (digital governance) kan det være hensiktsmessig å vise til tre ulike nivå, nederst et infrastruktur-nivå (kabler, satellitter, etc.), deretter et logisk nivå (det som gjør at internett fungerer, DNS, rotservere, Internet Protokoller, etc.) og øverst et økonomisk- og samfunnsnivå (ap-plikasjoner og innhold). For en oversikt, se: https://www.slideshare.net/icannpresentations/three-layers-of-digital-governance-infographic-english

[16] Det finnes alternative DNS-røtter, såkalte *alt root* tilbydere som drives av idealistiske, ideologiske og kommersielle årsaker eller internt av en organisasjon for egen bruk for lukkede eller graderte nettverk. I praksis er det en svært liten andel av internettilbydere (ISPer) som bruker *alt root*-tilbydere, de holder seg i all hovedsak til de ICANN-spesifiserte rotserverne.

I 2012 foreslo kinesiske ingeniører i Internet Engineering Task Force (IETF)[17] en løsning med autonome internett. «DNS extention for Autonomous Internet» skulle gi hver stat et uavhengig domenenavnhierarki og DNS-rotservere. Det ville gitt stater mulighet til å dele ut toppdomener uten at det var koordinert med ICANN eller noen annen internasjonal organisasjon. Det samme toppdomenet kunne da i teorien blitt gitt i alle verdens stater og ledet til like mange forskjellige adresser. Forslaget innebar at hvert autonome internett (hvert land) skulle ha en unik identifikasjon som skulle koordineres internasjonalt, på samme måte som hvert land har en landkode for telefon. (Mueller, 2017).

Et autonomt/nasjonalt DNS ville blant annet gitt Kina (og alle andre land) en betydelig større mulighet for sensur og informasjonskontroll, for blokkering av utenlandske nettsider – og utenlandske nettverk – og for å tilgodese eget næringsliv. Samtidig ville det gjort det svært vanskelig for bedrifter og andre som ønsker å nå et internasjonalt publikum. Konsekvensene for internettbasert handel og kommunikasjon ville vært enorme.

Forslaget fikk ingen *rough consencus* i IETF og ble ikke fulgt den gang. Eksempelet viser imidlertid hvilke konsekvenser endringer i den grunnleggende internettarkitekturen kan få. Internettets nåværende arkitektur er ikke designet for å tilpasse seg staters territorielle grenser.

Mot slutten av 2017 meldte russiske medier at President Putin etter anbefaling fra den russiske føderasjonens sikkerhetsråd hadde instruert Kommunikasjonsdepartementet og Utenriksdepartementet om å starte arbeidet med å utvikle en egen DNS-rot for BRICS-landene (RBC, 2017)[18]. Dersom instruksen blir gjennomført vil det i realiteten etablere et alternativt internett i BRICS-landene.

Samtidig har russisk-kinesiske forbindelser blitt styrket hva gjelder samarbeid om internetts fremtid. Våren 2015 undertegnet Putin og Kinas president Xi Jinping det som har blitt omtalt som en bilateral ikke-aggresjonspakt for cyberspace (Roth, 2015). Avtalen inkluderer imidlertid også språk som fremmer konseptet *cybersuverenitet*. Det kan med styrke hevdes at kjernen i samarbeidet gjelder det siste, et felles ønske om å utfordre den amerikanske dominansen over internett (Wei, 2016).

Den kinesiske ideen om cybersuverenitet ble først omtalt i en rapport fra kinesiske myndigheter i juni 2010 (Information Office of the State Council, 2010) og har siden blitt spesifisert og forsterket av President Xi Jinping ved flere anledninger[19]. I korte trekk går det ut på at internett i realiteten er et fysisk område og følgelig også innenfor en stats territorium. Således skal internett ikke være gjenstand for

[17] Internet Engineering Task Force (IETF) utvikler og promoterer Internett-standarder, i nært samarbeid med World Wide Web Consortium (W3C) og standardiseringsorganisasjonene ISO og IEC, og befatter seg spesielt med standardene innen TCP/IP.

[18] BRICS er gruppen av verdens største fremvoksende økonomier og består av Brasil, Russland, India, Kina, Sør-Afrika.

[19] For eksempel ved BRICS toppmøtet i 2014 og World Internet Conference i Wuzhen i 2015.

påvirkning fra andre stater og hver stat skal ha rett til å kontrollere det digitale rom innenfor egne grenser. Cybersuverenitet betyr følgelig at enhver regulering av internett, inkludert statlig kontroll over innhold, er legitimt. Etter at Xi kom til makten i 2012 har også Kinas internasjonale engasjement for å fremme cybersuverenitet akselerert og de har aktivt søkt internasjonale partnere som støtter den samme ideen. En slik partner har de funnet i Russland.

Vestlige sanksjoner som følge av Russlands intervensjon i Øst-Ukraina i 2014 økte den russiske bekymringen for amerikansk kontroll over internett. En talsmann for Kreml uttalte den gang at Russland kunne ta grep for å forhindre utenlandsk innblanding i «deres internett» (Razumovskaya & Sonne, 2014). En slik posisjon sammenfalt med det kinesiske konseptet om cybersuverenitet og ble altså inkludert i «ikke-aggresjonspakten» året etter som et strategisk grep for å utfordre amerikansk dominans. Putins instruks fra 2017 om en egen DNS-rot for BRICS landene bør ses i denne sammenheng.

Russiske myndigheter har de siste årene vist betydelig interesse for kinesisk internettforvaltning. Særlig har de vært interessert i ideene til Fang Binxing, mannen bak det omfattende kinesiske digitale sensursystemet, gjerne omtalt som den store kinesiske brannmur, og en sterk talsmann for cybersuverenitet (Kommersant, 2018).

I følge Fang er suverenitet på internett basert på fire prinsipper: Staten må ha full kontroll over alle segmenter av internett (infrastruktur og innhold); staten må være i stand til å beskytte disse segmentene mot angrep utenfra (cybersikkerhet); alle stater må ha lik tilgang til grunnleggende internettressurser; andre stater skal ikke kontrollere DNS-rot som gir tilgang til kinesiske nettverk.

Fang har tatt til orde for et system med direkte dataoverføring mellom BRICS og SCO-landene[20] basert på egne DNS-rotservere, for å unngå at informasjon kan bli sendt via rotservere plassert i USA eller hos deres allierte (hvilket gjelder alle dagens 13 rotservere). Det kan synes som om Putins instruks fra oktober 2017 forfølger dette forslaget. Det er ikke meningen at en egen DNS-rot for BRICS og SCO skal erstatte dagens DNS, ifølge Fang, men det vil være et nyttig tillegg (Kommersant, 2018). I praksis vil et slikt system muliggjøre informasjonsflyt over et nytt internett bestående av Kina, Russland og deres samarbeidspartnere, uavhengig av eksisterende DNS. Det er imidlertid usannsynlig at noen av disse landene noensinne vil bli «koblet fra» eksisterende DNS selv om forholdet til USA skulle bli svært anspent. Til det er konsekvensene for store. Initiativet bør følgelig ses som et ledd i økt informasjonskontroll myntet på egne borgere mer enn et tiltak for å sikre et stabilt og velfungerende internett i en krisesituasjon. Samtidig vil en egen DNS-rot

[20] SCO = Shanghai Cooperation Organization, en regional sikkerhetspolitisk samarbeidsorganisasjon etablert i 2001. Medlemmer er Kina, Kasakhstan, Kirgisistan, Russland, Tadsjikistan, Usbekistan, India og Pakistan.

for BRICS og SCO-landene kunne bety et eget forvaltningsregime i tråd med prinsippene om cybersuverenitet.

På multilaterale arenaer vil vi se nye initiativ til fordel for statlig suverenitet over forvaltningen av internetts kritiske ressurser. USA har tradisjonelt stått i bresjen for et fritt og åpent internett og hatt lederrollen blant demokratiske stater hva gjelder tilnærmingen til global internettforvaltning. Under Trump-administrasjonen fremstår det som mer uklart hvor høyt dette er prioritert og tiden vil vise om USA igjen ønsker og evner å påta seg en global lederrolle for internetts fremtid. I dag er det Kina som har initiativet.

Helt uavhengig, men omtrent samtidig med etableringen av ICANN høsten 1998 fremmet Russland for første gang en resolusjon under FNs generalforsamlings første komité om det digitale roms betydning for internasjonal fred og sikkerhet[21]. Resolusjonen ble vedtatt uten avstemming. Siden den gang har en tilsvarende resolusjon blitt fremmet hvert år, hvor praktisk talt alle medlemsstater har stemt for, med unntak av USA ved enkelte anledninger.

En resolusjon i FNs generalforsamling har liten praktisk betydning men signaliserer en retning og kan være begynnelsen på en prosess mot bindende konvensjoner. Flere stater ønsker nye internasjonale konvensjoner og en sterk rolle for FN i spørsmål knyttet både til statlig oppførsel i det digitale rom og til global internettforvaltning. Russland har særlig vært en målbærer for denne gruppen som argumenterer for at det er *stater* som bør avgjøre internettets fremtid. For eksempel har de foreslått en internasjonal konvensjon om global internettforvaltning[22] og en konvensjon om internasjonal informasjonssikkerhet.[23]

Det fremmes også initiativ fra privat sektor. Microsoft foreslo i januar 2017 å utarbeide en digital Genèvekonvensjon for å beskytte innbyggere online i fredstid ved å regulere staters oppførsel i det digitale rom (Ciglic, 2017). Forslaget har fått mye oppmerksomhet og støtte fra en rekke store teknologiselskap. Selv om henvisningen til Genèvekonvensjonene er misvisende er det verdt å merke seg at store multinasjonale teknologiselskap ønsker globale reguleringer for å unngå at statlige aktører misbruker sårbarheter i selskapenes produkter. Argumentene mot Microsofts forslag er i grove trekk de samme som vestlige argumenter mot russiske og kinesiske forslag om en ny konvensjon (Jacobsen, 2018).

Informasjonskontroll og suverenitet på internett

Valutaen på internett, og for så vidt i hele det digitale rom, er *informasjon*. Det er primært ved å kontrollere, hindre, overvåke eller påvirke informasjonen – data og

[21] *Resolution on Developments in the field of information and telecommunications in the context of international security*, FN, ref.: 1998 – A/RES/53/70.

[22] Bl.a. uttalt under Russlands hovedinnlegg under ITU Plenipotentiary, Busan i 2014.

[23] Som en av Russlands uttalte prioriteringer slik det bl.a. fremkommer i *Basic Principles for State Policy of the Russian Federation in the field of International Information Security to 2020*, som ble signert av president Putin i juli 2013.

innhold – som flyter gjennom infrastrukturen at suverenitetshevdelse på internett kan foregå.

Enkelt sagt handler det om statens suverene rett til å stanse eller kontrollere det Jon Bing sammenlignet med containere, når containerne befinner seg innenfor statens territorielle grenser. Motivene for å kontrollere informasjonsflyten er ikke annerledes enn ved analog informasjonskontroll og kan spenne fra terrorbekjempelse til politisk overvåkning. Suverenitetshevdelse i den forstand er følgelig ikke noe nytt, selv om mengden med informasjon er mye større enn i pre-internett tiden. Men gir det egentlig mening å hevde nasjonal suverenitet, eller cybersuverenitet, over internett? Det byr i alle fall på flere paradokser. Professor Milton Mueller ved Georgia Institute of Technology er blant de som har påpekt dette.

For det første, hevder Mueller, vil statlig suverenitetshevdelse på internett normalt bli legitimert med henvisning til nasjonal sikkerhet. Det impliserer samtidig erkjennelsen av det digitale rom som et militært domene og en tilnærming til cybersikkerhet som et nasjonalt sikkerhetsproblem hvor sårbarhetene i nettverkene kombinert med samfunnets avhengighet av dem utgjør en trussel mot staten som sådan. Statens sikkerhet blir således det primære, sikkerheten til sluttbrukere og private nettverksoperatører blir sekundært (Mueller, 2017, s. 86–88). Altså et motsatt formål enn hva for eksempel Microsofts forslag om en digital Genèvekonvensjon tilstreber. Ved å henvise til nasjonal sikkerhet er det statens autonomi og militærmakt som vektlegges, som igjen er definert i forhold til andre stater – altså et stat-til-stat forhold basert på nasjonalstatens makt og territorielle grenser, gjerne omtalt som det westfalske prinsipp.

Denne form for suverenitetshevdelse tydeliggjøres ofte gjennom etablering av militære cyber-forsvar, cyberkommandoer eller tilsvarende, nasjonalisering og sentralisering av trusselrapportering og kapasiteter, for eksempel nasjonalt varslingssenter (CERT – Computer Emergency Response Team) under militær kommando og fokus på nasjonale/allierte standarder og teknologi fremfor teknologi produsert i stater som kan være potensielle motstandere (Mueller, 2017).

Men er disse grepene egentlig å hevde suverenitet? Mueller mener at de ikke er det. For det første, hevder han, så er nasjonens territorium irrelevant i denne sammenheng fordi evnen til å ha «nasjonal sikkerhet» i det digitale rom krever global tilstedeværelse og globale kapasiteter. Internett muliggjør dette. Når en stat utvikler offensive cyberkapasiteter, med henvisning til nasjonal sikkerhet, så forplikter den seg samtidig til en ekstraterritoriell virtuell eller fysisk tilstedeværelse i nettverk som befinner seg utenlands. Med andre ord, for å opprettholde «suverenitet» må den bryte med prinsippet om «suverenitet». I tillegg er dette svært ofte private nettverk som neppe kan sies å være et militært domene. Det digitale rom er radikalt anti-westfalsk hevder Mueller, fordi internett har senket barrieren for global maktutøvelse og gjort det relativt enkelt for enhver velorganisert aktør – statlig eller ikke-statlig – å projisere makt nær sagt hvor som helst på kloden. I den kinetiske verden er det kun

USA som har hatt kapasitet til å gjøre noe tilsvarende, gjennom militær tilstedeværelse. Selv om det er store forskjeller mellom stater hva gjelder kapasiteter for koding, angrep og evnen til å oppdage digitale trusler så er det ingen markant forskjell hva gjelder territorial tilgang (Mueller, 2017).

For det andre vil statlig suverenitetshevdelse på internett ofte fokusere på «territorialisering» av informasjonsflyten. Det kan inkludere både tekniske og juridiske grep som krav om geografisk lokalisering av data, filtrering og blokkering av innhold og internasjonal anerkjennelse av informasjonssuverenitet (Mueller, 2017, s. 77).

Enkelte stater har sågar fremstilt krav om geografisk datalagring som et tiltak for økt cyber-sikkerhet. Geografisk lokalisering har imidlertid liten eller ingen betydning for cybersikkerhet eller beskyttelse av data. Datasikkerhetsbrudd foregår i alle land. Det er ikke *hvor* dataene fysisk befinner seg som avgjør om de er sikre, men *hvordan* de er lagret.

En rekke stater filtrerer trafikken på internett. Storbritannia har for eksempel et «digitalt grenseforsvar» som filtrerer nettverkstrafikk til Storbritannia. Norge og andre er i ferd med å etablere noe tilsvarende. Kina har med «den store kinesiske brannmur» et omfattende system for å filtrere internettrafikk. Både Storbritannia og Kina legitimerer filtreringen ved å henvise til nasjonal sikkerhet. Men det er en signifikant forskjell i måten det gjøres på.

For igjen å bruke Bings metafor, Storbritannia sjekker utsiden av containeren, om den er mistenkelig merket, hvor den kommer fra og hvor den skal. Storbritannia filtrerer data, med fokus på falske websider, phishing-angrep og ondsinnet programvare men tillater fri flyt av innhold, fri meningsutveksling og fri tilgang til utenlandske websider. Kina derimot, åpner systematisk containeren for å sjekke hva som er inne i den. De filtrerer og blokkerer også innhold, som kritikk av myndighetene eller tilgang til utenlandske websider. For Storbritannia handler det om skadereduksjon, for Kina også om politisk stabilitet og trusler mot kommunistpartiet. Men forskjellen berører et krevende teknisk spørsmål om hvorvidt det er mulig å ha en internettarkitektur som gjør det mulig å gjenkjenne og filtrere ondsinnede data uten samtidig å kunne filtrere og påvirke innhold (Morgus & Sherman, 2018).

Blokkering av *tilgang* til internett foregår i økende grad også i demokratiske stater. Myndighetene i verdens største demokrati, India, stod i 2017 for 79 av de 108 kjente bevisste utkoblinger av internett og tallet synes å bli enda høyere for 2018 (Sanchez, 2018). Utkoblingene foregår primært i områder med uroligheter og med henvisning til nasjonal sikkerhet og skadereduksjon. Man kan lett forstå indiske myndigheters ønske om å avverge uroligheter. Samtidig er det interessant å merke seg at mange av de bevisste internettutkoblinger som har blitt gjennomført ikke har funnet sted i diktaturer som Hviterussland, Kina eller Iran, men i stater som opplever en rask økning av internettbrukere, altså hovedsakelig utviklingsland.

Kulturelt etterslep?

Vestlige demokratiers mantra har hele tiden vært at internett skal være globalt og ha åpenhet, sikkerhet, robusthet og frihet som styrende prinsipper[24]. Det er de prinsipper som ligger bak internetts formidable suksess. Samtidig kan det argumenteres for at det er de samme prinsippene som har gjort internett til en arena for påvirkningsoperasjoner, falske nyheter, phishing-angrep og hacking, økonomisk kriminalitet og annen alvorlig kriminalitet. For å nevne noe. Autoritære stater har som kjent hatt en annen tilnærming, hvor suverenitet, politisk stabilitet, sensur, overvåkning og informasjonskontroll har stått sentralt[25] (Morgus & Sherman, 2018). Dette er argumenter som finner gjenklang i mange utviklingsland. Det er stater som erkjenner behovet for og betydningen av internett for økonomisk og sosial utvikling, men som også ønsker å kontrollere det for uønsket innhold eller når internett utfordrer myndighetene politisk. Mange av de «nye» internettstatene, som i FN-sammenheng ofte koordinerer posisjoner i G77-gruppen, ser seg bedre tjent med et statskontrollert «suverent» internett enn et åpent, fritt internett som forvaltes og utvikles hovedsakelig utenfor statens kontroll.

Spørsmålet er om vi har kommet til det punkt hvor vestlige demokratier bør erkjenne at prinsippene om åpenhet, sikkerhet, robusthet og frihet ikke lenger fungerer i samspill slik internett har utviklet seg.

Svaret er at vi allerede har passert det punktet og at prinsippet om sikkerhet trumfer prinsipper om åpenhet og frihet, også i vestlige demokratier. Som eksempelet om filtrering i Storbritannia og Kina indikerer er det lite trolig at internettarkitekturen ivaretar prinsippet om åpenhet og prinsippet om sikkerhet samtidig, gitt sammenhengen mellom data og innhold på internett. Spørsmålet, som blant annet tenketanken New America har påpekt, bør følgelig heller være *i hvilken grad* vestlige demokratier er villige til å avvike fra prinsippene om åpenhet og frihet til fordel for sikkerhet. Det er vesentlige forskjeller mellom Storbritannias og Kinas praksis, men begge bryter prinsippene om åpenhet og frihet på internett.

Samtidig går den teknologiske utviklingen raskt videre og vil kunne skape nye løsninger og nye utfordringer som vi ikke kan forestille oss, like lite som vi kunne forestille oss internett på 1960-tallet. Utviklingen av quantemaskiner og kunstig intelligens, for eksempel, vil kunne endre det digitale mulighets- og trusselbildet på fundamentale måter og endre vår tilnærming til både sikkerhet og åpenhet i den digitale sfære. Men enn så lenge er det den fysiske infrastrukturen *internett* som ligger i bunn for den pågående fjerde industrielle revolusjon, hvor «alt» blir digitalisert og koblet til nettverk, og som medfører raske samfunnsendringer. Hvordan og av hvem

[24] Som for eksempel beskrevet i USAs, Storbritannias og Norges internasjonale cyberstrategier.
[25] Kina introduserte for eksempel «Golden Shield» prosjektet – forløperen til dagens «Great Firewall» - i 1998, da mindre enn 0,2% av befolkningen hadde tilgang til internett.

internett utvikles, forvaltes og kontrolleres handler følgelig også om hvordan og av hvem *samfunnet* utvikles, forvaltes og kontrolleres.

Den amerikanske sosiologen William Ogburn lanserte begrepet «kulturelt etterslep» – cultural lag – i 1923 for å forklare hvordan kulturen og verdensanskuelsen blir hengende etter ved raske teknologiske endringer i samfunnet, hvor man bruker gamle forklaringsmodeller og metoder for å forstå nye tider (Ogburn, 1923). Det er fristende å trekke paralleller mellom Ogburns teori om kulturelt etterslep og internasjonal politikk for å tilnærme seg det digitale rom og internett. Vi bruker tradisjonelle mekanismer i internasjonal politikk for å forstå en ny virkelighet og vi forsøker å løse konflikter i fora som ikke nødvendigvis er egnet. FN og andre multilaterale fora er basert på samarbeid mellom selvstendige stater hvor westfalske prinsipper om statens suverenitet og makt ligger til grunn.

Samtidig er det privat sektor og ikke-statlige aktører som utgjør grunnfjellet i internett. Rundt 80% av internettets infrastruktur er i privat eie. Private selskap, stiftelser og individer legger i stor grad rammene for hvordan internett fungerer og utvikler seg. Multilaterale fora har per i dag svært begrenset innflytelse hva gjelder internetts arkitektur, design eller bruk. Internasjonale disputter som angår internett kan følgelig i svært begrenset grad, om noen, løses gjennom tradisjonelle multilaterale metoder.[26] Med mindre cybersuverenitet blir normen.

Verden vil aldri få tilbake til det åpne, frie internett. Til det har internett blitt for viktig, og for farlig. Statlige grep for å oppnå cybersuverenitet gjennom militarisering av det digitale rom, krav om geografisk lagring av data og forsøk på å tilpasse kritiske internettressurser langs nasjonale linjer er trender som forsterkes, ikke svekkes. Amerikansk dominans over internett, både politisk og teknisk, er falmende. Kina har ambisjoner om å overta som verdens ledende cybermakt og har tilsynelatende både vilje og ressurser til å klare det[27].

I dette bildet avtegner internett seg som et globalt spenningsfelt som ikke vil bli mindre viktig i årene som kommer. Hvorvidt vi kaller det geopolitikk eller ikke er av mindre betydning.

Om forfatteren

Bjørn Svenungsen var i 2018 gjesteforsker ved Institutt for Forsvarsstudier (IFS), hvor han har forsket på internasjonale utfordringer relatert til cyberspace. Svenungsen har arbeidet som diplomat i Utenrikstjenesten siden 1999, hvorav flere år som

[26] En lang rekke møter og konferanser de siste ti årene har søkt å skape møteplasser hvor både statlige og ikke- statlige aktører møtes for å diskutere globale utfordringer knyttet til internett og det digitale rom For eksempel «The Global Conference on Cyberspace», den såkalte Londonprosessen, som sist møttes i New Dehli i 2017. Listen over slike møteplasser er svært lang. Slike møteplasser er viktige, men de har ingen reell beslutningsmyndighet.

[27] En redegjørelse for Kinas vekst og makt som aktør i internett vil kreve (minst) en egen artikkel. For en god innføring, se Adam Segal: *When China Rules the Web. Technology in Service of the State*, Foreign Affairs, September/October Issue 2018.

fagdirektør for internasjonal cyberpolitikk. Fra april 2019 har han vært selvstendig næringsdrivende.

Litteraturliste

Barlow, J. P. (1996). A Declaration of the independence of cyberspace. Hentet fra https://en.wikipedia.org/wiki/A_Declaration_of_the_Independence_of_Cyberspace. (2018, 10. mai)

Bing, J. (2009). Building cyberspace: A brief history of internet. I L. A. Bygrave & J. Bing (Red.), *Internet governance. Infrastructure and institutions* (s. 8–47). Oxford: Oxford University Press.

Bygrave, L. A. & Michaelsen, T. (2009). Governors of internet. I L. A. Bygrave & J. Bing (Red.), *Internet governance. Infrastructure and institutions* (s. 92–125). Oxford: Oxford University Press.

Bygrave, L. A., Schjavetta, S., Thunem, H., Lange, A. B., Phillips, E. (2009). The naming game: Governance of the domain name system. I L. A. Bygrave & J. Bing (Red.), *Internet governance. Infrastructure and institutions* (s. 147–212). Oxford: Oxford University Press.

Ciglic, K. (2017). The evolution of international collaboration and law related to cyberspace and security. I S. Saran (Red.), *Our common digital future. Global Conference on Cyberspace Journal*, Observer Research Foundation (s. 36–41). Hentet fra https://www.orfonline.org/wp-content/uploads/2017/11/Our-Common-Digital-Future.pdf

Hagen, Ø. (2007). *Nettverk i arbeid.* (Hovedoppgave). Universitetet i Oslo.

Information Office of the State Council of the People's Republic of China. (2010, 8. juni). The internet in China. Hentet fra http://china.org.cn/government/whitepaper/node_7093508.htm (2018, 29. august)

Internet Live Stats. (2018). *Total number of websites*. Hentet fra http://www.internetlivestats.com/total-number-of-websites/(2018, 8. mai).

Jacobsen, J. T. (2018). En «digital Genèvekonvention» er ikke i Danmarks interesse. *Internasjonal Politikk, 76*(2), 73–88. https://doi.org/10.23865/intpol.v76.1041

Kaplan, F. (2016). *Dark territory. The secret history of cyber war*. New York: Simon & Schuster.

Kommersant (2018, 22. juli) *Russia goes online in the UN. Moscow will present two new initiatives to the world community*. Hentet fra www.kommersant.ru. (2018, 28. august)

Lee, T. B. (2014). *40 maps that explain the internet*. Hentet fra https://www.vox.com/a/internet-maps. (2018, 2. mai)

Ministry of Digital Development, Communications and Mass Media of the Russian Federation. (2014, 20. oktober). Policy statement by the head of the Russian delegation. Fremført under ITU Plenipotentiary i Busan, Sør-Korea. Hentet fra www.minsvyaz.ru

Morgus, R. & Sherman, J. (2018, 26. juli). A tale of two internets, *New America Weekly*, Edition 213. Hentet fra https://www.newamerica.org/weekly/edition-213/tale-two-internets/

Mueller, M. (2017). *Will the internet fragment?* Cambridge: Polity Press.

NTIA. (2014). NTIA announces intent to transition key internet domain name functions. Hentet fra https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition- key-internet-domain-name-functions. (2018, 30. april)

Ogburn, W. F. (1923). *Social change with respect to cultural and original nature*. New York: B. W. Huebsch Inc.

Rasumovskaya & Sonne (2014, 19. september). Moscow considers moves to secure and defend internet in Russia. *Wall Street Journal*. Hentet fra https://www.wsj.com/articles/moscow-considers-moves-to-secure-and-defend-internet-in-russia-1411145000?cb=logged0.21002391433612377 (2018, 28. august)

Raustiala, K. (2017). An internet whole and free: Why Washington was right to give up control. *Foreign Affairs*, Vol. 96 (Mar/Apr). s. 140–147.

RBC News Agency. (2017, 28. november). The Security Council of Russia instructed to create an "independent Internet" for the BRICS countries. Hentet fra https://www.rt.com/russia/411156-russia-to-launch-independent-internet/

Roth, A. (2015, 8. may). Russia and China sign cooperation pacts. *The New York Times*. Hentet fra https://www.nytimes.com/2015/05/09/world/europe/russia-and-china-sign-cooperation-pacts.html (2018, 30. august)

Russian Federation. (2013). Basic principles for state policy of the Russian Federation in the field of international information security to 2020. Hentet fra https://ccdcoe.org/sites/default/files/strategy/RU_state-policy.pdf

Sanchez, C. (2018, 22. august). The link between more internet access and frequent internet shutdowns. *Net Politics Blog*, Council of Foreign Relations. Hentet fra https://www.cfr.org/blog/link-between-more-internet-access-and-frequent-internet-shutdowns?sp_mid=57227575&sp_rid=YmpvcmVuc3ZlbnVuZ3NlbkBpZnMubWlsLm5vS0 (2018, 30. august)

Segal, A. (2018). When China rules the web. Technology in service of the state. *Foreign Affairs*, September/October Issue.

Sterling, B. (1993). A short history of the internet. Hentet fra http://sodacity.net/system/files/Bruce_Sterling_A_Short_History_of_the_Internet.pdf (2018, 9. mai)

Statista. (2018). Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Hentet fra https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (2018, 2. mai)

Time Magazine. (1953, 5. oktober). Procter & Gamble's McElroy.

Time Magazine. (1958, 13. januar). Defense Secretary McElroy.

United Nations. (1998). Resolution on developments in the field of information and tele- communications in the context of international security. FN, ref.: 1998-A/RES/53/70.

United Kingdom Government, Cabinet Office. (2016). *National cyber security strategy 2016 to 2021*. Hentet fra https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Utenriksdepartementet. (2017). *Internasjonal cyberstrategi for Norge*. Hentet fra https://www.regjeringen.no/no/dokumenter/cyberstrategi/id2569056/

Wei, Y. (2016). China-Russia cybersecurity cooperation: Working towards cyber-sovereignty. Henry M. Jackson School of International Studies, University of Washington. Hentet fra https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/

White House. (2011). *U.S. international strategy for cyberspace*. Hentet fra https://2009-2017.state.gov/s/cyberissues/strategy/index.htm

Abstract in English

The internet is the world's most important infrastructure. Its vast success has been built on principles of openness, freedom, resilience and security. These are principles that are increasingly difficult to combine. States' demand for control and security has developed the concept of "cyber sovereignty" which is about to change the internet as we know it, where the networks and their underlying architecture play an increasing role in the geopolitical ambitions of states.

Keywords: internet • cybersecurity • sovereignty • geopolitics • internet governance • cyberspace • Russia • China • USA