Norwegian Institute of International Affairs

Policy Brief
[7 / 2019]

Forebygging av krig og konflikt i cyberdomenet

Bjørn Svenungsen

Innledning

Cyberdomenet representerer kanskje en av vår tids største trusler mot internasjonal fred og sikkerhet men er viet lite oppmerksomhet hva gjelder forebygging av krig og konflikt. Det er behov for internasjonale forpliktende kjøreregler som hever blikket over IKT-forvaltning, digitalisering og cybersikkerhetstiltak og fokuserer på fredelige relasjoner mellom stater i cyberdomenet. Skal en slik diskusjon ha effekt må den tas i FNs Sikkerhetsråd.

Vår samfunnsstruktur og vår velstand hviler i dag på digitale fundament. Moderne samfunn er i dag så avhengig av digitale nettverk at det økonomiske skadeomfanget og de potensielle menneskelige lidelsene som vil kunne oppstå dersom nettverkene settes ut av spill vil tendere mot skadeomfanget ved en konvensjonell krig.

Internasjonal cybersikkerhet handler følgelig om mer enn summen av alle staters digitale risiko, digitale trusler og digitale sårbarheter. Det handler også om forebygging av konflikt og ivaretagelse av fredelige relasjoner mellom stater.

I vår tradisjonelle forståelse av krig og fred er forebyggende diplomatisk arbeid, dialog fremfor konflikt, langt å foretrekke. Men mens vi har en lang tradisjon i Norge for å arbeide for dialog og forebygging av konflikt over store deler av verden hva gjelder konvensjonelle konflikter, har vi et svært begrenset engasjement hva gjelder internasjonalt konfliktforebyggende arbeid i cyberdomenet.

Det kan synes som vi ikke helt har tatt inn over oss at digitale nettverk i dag utgjør ryggraden i samfunnet. Vi er helt avhengig av dem på nær sagt ethvert område. Dersom alle digitale nettverk ved et trylleslag hadde kollapset ville samfunnskollaps, kaos og menneskelige lidelser vært resultatet.

Et slikt trylleslag er i dag helt usannsynlig. Men vi vet med sikkerhet at konsekvensene av storstilte cyberoperasjoner kan gi virkninger langt utover digitale rom. Det er ikke science-fiction med et scenario hvor cyberoperasjoner fører til stans i matleveranser, vannforsyning, lufttransport, kraftforsyning og finanstransaksjoner. Samtidig. Enten man befinner seg i 20 kuldegrader et sted i Norge eller et hvilket som helst annet sted i verden så vil man fort kunne skimte konturene av en humanitær katastrofe og en sivilbefolkning som vil lide på høyst konvensjonelle måter.

Samtidig er vi helt i begynnelsen av den digitale revolusjonen. Internett er ikke engang 40 år gammelt men har allerede endret samfunnet på fundamentale måter. Kanskje mer enn de fleste av oss innser. Nye teknologier vil skape endringer som er betydelige større. Vi skimter allerede blokkjedeteknologi, kunstig intelligens, quantecomputing og tingenes internett som er i ferd med å gjøre seg gjeldende. Hva det videre farvann vil bringe er det ingen som vet. Men vi vet dette: Det som er lite sannsynlig i dag vil bli mulig i fremtiden. Vi vil stå ovenfor trusler vi i dag ikke kan forestille oss, like lite som vi kunne forestille oss internett for 50 år siden. Samtidig vil den digitale revolusjonen fortsette å skape løsninger til det gode for mennesker og samfunn. Innovasjon, åpenhet og fri informasjonsflyt i digitale rom vil fortsette å gjøre verden til et bedre sted. Det er avgjørende at de grep vi tar for å forebygge digitale trusler ikke stanser den utviklingen.

Poenget er dette: Mens vi på konvensjonelle områder arbeider aktivt gjennom internasjonalt diplomati og militært samarbeid for å unngå at vi selv eller andre havner i en situasjon hvor krig og lidelse truer så synes vi å være uforstående til at en slik tilnærming også bør inkludere digitale rom. Globale trusler i og mot den digitale sfære kan forebygges med tekniske løsninger alene like lite som konvensjonell krig og konflikt kan forebygges med militære styrker alene.

I Norge har vi etterhvert et betydelig fokus på cybersikkerhet og cyberforsvar. Det er bra. Et effektivt og operativt forsvar for å avskrekke og eventuelt møte og uskadeliggjøre trusler er helt nødvendig, både i den analoge og den digitale verden.

Men forbyggende arbeid for å unngå å komme i en situasjon som truer staten eller samfunnet er langt å foretrekke. Vi kjenner dette fra den analoge verden. Mellomstatlige avtaler som forplikter partene til å avstå fra aggresjon og å samarbeide fordi det er i alle parters interesse.

Strengt tatt er hele den liberale verdensorden som har vokst fram etter andre verdenskrig tuftet på slike avtaler. FN-pakten, Verdens Handelsorganisasjon med dens forgjengere og Den Europeiske Union, for å nevne noen av fundamentene, har i seg selv og gjennom avtaler de har fremforhandlet bidratt til en verden med økt forutsigbarhet, økt mellomstatlig samarbeid, færre trusler og mindre krig. Norge har aktivt bidratt til å få på plass slike avtaler fordi multilateralt samarbeid i all hovedsak tjener Norge og norske interesser.

For cyberdomenet finnes ingen slike avtaler. Ingen internasjonale konvensjoner. Ingen avtaler som forplikter stater til å avstå fra aggresjon og å samarbeide fordi det er i alle parters interesse. Vi, særlig i Vesten, liker å si at jo, det finnes avtaler fordi folkerettens prinsipper for maktanvendelse også gjelder i digitale rom, og viser til enighet i en arbeidsgruppe i FN-regi fra 2013 hvor blant annet alle stormaktene deltok. Vel og bra. Men gjeldene folkerett, for eksempel havretten eller menneskerettighetene, ble skrevet i en tid da man knapt kunne forestille seg digitale nettverk. Enda mindre hvor kritisk avhengig samfunnet skulle bli av dem. Og selv om man tolker gjeldene folkerett i en digital virkelighet – og det gjøres – så er vi svært langt unna noe som kan ligne på en enighet om hvordan folkeretten kommer til anvendelse i digitale rom. Har man jobbet med denne tematikken en stund er man smertelig klar over at man aldri vil komme fram til noen enighet. Til det er perspektivene fra blant annet Kina, Russland og USA for ulike, og egeninteressene for store.

Folkeretten og den liberale verdensorden ble etablert av mennesker som hadde opplevd hva som kunne skje når verden ikke tok fatt i de virkelig store problemene før de ble uhåndterlige. Mennesker som på nært hold hadde opplevd ekstrem fattigdom under depresjonen, fremveksten av diktaturer i Europa og de grusomheter andre verdenskrig førte med seg. Man sa «aldri mer» og så til fortidens feil for å skape en bedre fremtid. Vi som lever i dag har mye å takke disse menneskene for.

Vil menneskene som lever om 70 år kunne takke dagens beslutningstagere for å ha gjort like kloke valg? Si det. Det vi står overfor er fundamentalt annerledes. Like fullt kreves det (enn så lenge) mennesker for å iverksette cyberoperasjoner, det er mennesker som har mulighet for å bli enige om internasjonale kjøregeler i digitale rom, og det er mennesker som beslutter om kjøreregelene skal overholdes. Det vesentlige i denne sammenheng er altså ikke hva computere, algoritmer og programvare er i stand til å gjøre, men hva mennesker kan gjøre mot andre mennesker i og gjennom digitale rom.

Vi snakker altså her om regler for hvordan stater skal forholde seg til hverandre i digitale rom. Kriminell virksomhet er noe annet. Kriminalitet vil vi antagelig aldri helt bli kvitt hverken i den analoge eller i den digitale sfære. Bekjempelse av digital kriminalitet er for øvrig det ene området hvor det faktisk finnes en konvensjon for internasjonalt samarbeid, en Europarådskonvensjon om politisamarbeid. Og, ja, det er krevende gråsoner mellom kriminell virksomhet og statlig virksomhet. Det synes heller ikke ønskelig å regulere etterretningsarbeid i det digitale rom, hvilket praktisk talt alle stater utøver.

Men det er behov for å opprettholde internasjonal fred og sikkerhet. Det fordrer internasjonale forpliktende avtaler som spesifikt inkluderer digitale rom. Forståelsen for det behovet synes å være fraværende eller i beste fall lite uttalt. Hvorfor er det slik?

Svaret, tror jeg, ligger i den antatte kompleksiteten. Og i USA.

Evne å heve blikket

Internett er verdens desidert største og viktigste digitale rom. Rent teknisk er internett et komplekst økosystem med en arkitektur som i liten grad passer inn i vårt tradisjonelle bilde av mellomstatlige forhold. Internett består i dag av titusenvis av selvstendige men sammenkoblede digitale nettverk, nettverk som ofte krysser geografiske landegrenser. Teknikk, politikk, markedskrefter, statlige reguleringer, innovasjonsmiljøer og akademiske institusjoner er alle med på å forvalte dette globale økosystemet hvor eierskap og utvikling i all hovedsak er lagt til privat sektor og akademia, altså hos ikke-statlige aktører. Statens rolle i utvikling, kontroll og eierskap over internett har vært svært begrenset, selv om dette nå raskt er i ferd med å endre seg.

I en multilateral diskusjon om cyberdomenets betydning for internasjonal fred og sikkerhet er det lett å bli opphengt i internetts kompleksitet og forvaltning, og på tekniske tiltak som fokuserer på cybersikkerhet. De spede forsøk som er gjort på å nærme seg globale kjøreregler for stater, for eksempel den nevnte arbeidsgruppen i FN-regi, har i stor grad endt opp med å anbefale tiltak som egentlig ikke berører internasjonal fred og sikkerhet.

Blant annet foreslår FN-gruppen å styrke nettverkenes motstandsdyktighet nasjonalt, bedre nasjonal opplæring i cybersikkerhet og styrking av den nasjonale IKT-forvaltningen. Det har strengt tatt lite med internasjonal fred og sikkerhet å gjøre, men adresserer derimot myndigheter ansvarlig for nettverk, digitalisering og koordinering av cybersikkerhet. For Norges del er det i dag Samferdselsdepartementet, Kommunal- og Moderniseringsdepartementet og Justis- og beredskapsdepartementet. Altså departementer som er ansvarlig for cybersikkerhet nasjonalt men som i liten grad er eksponert for globale dialoger om internasjonal fred og sikkerhet. Den eksponeringen finner man primært i Utenriksdepartementet og Forsvarsdepartementet.

I regjeringens nylig fremlagte Nasjonal Strategi for Digital Sikkerhet lanseres en rekke gode tiltak for å gjøre Norge tryggere. De aller fleste handler om ulike digitale tryggingstiltak i Norge men for første gang er internasjonalt samarbeid for enighet om statlig adferd i digitale rom nevnt i en nasjonal strategi om digital sikkerhet. Det er gledelig, om det følges opp med handling. Men hvordan gjør man det?

Skal det internasjonale samfunn lykkes med å oppnå en allment akseptert forståelse av hvordan digitale rom truer internasjonal fred og sikkerhet bør vi fokusere på nettopp det; opprettholdelse av internasjonal fred og sikkerhet gjennom forebygging av krig og konflikt i en cyberkontekst. Vi må med andre ord evne å heve blikket over IKT-forvaltning, digitalisering og nasjonale sikkerhetstiltak, uten at disse forsømmes. Det kan bety dialog også med stater vi ikke har noe sikkerhetspolitisk samarbeid med og som vi ikke stoler på. Selv om det i dag fremstår som utopisk ville en bindende internasjonal avtale med et velfungerende sanksjonsregime som fokuserer på staters bruk – og bare det – av cyberdomenet kunne bidra til å redusere risikoen for alvorlige cyberangrep fra statlige aktører.

Uten å trekke sammenlikningen for langt kan vi trekke paralleller til havretten. Havretten gjør det mer forutsigbart å ferdes på verdenshavene. Ville en Cyberrett gitt oss et mer forutsigbart cyberdomene? Kanskje ikke. Per i dag er det iallfall en lang rekke krevende utfordringer som måtte løses. Blant annet knyttet til attribusjon (identifisere hvem som står bak angrep) og sanksjoner. Dessuten, mens verdenshavene er relativt uforanderlige endrer cyberdomenet seg i rekordfart. De utfordringer og trusler vi står overfor i dag vil være erstattet av noe helt annet innen en eventuell avtale ville sett dagens lys. Multilaterale forhandlinger er langsomme prosesser.

Men det er ikke bare utfordringene og den tekniske utviklingen det står på. Det er viljen. FNs Sikkerhetsråd er verdens desidert viktigste organ for internasjonal fred og sikkerhet og har hovedansvaret for FNs arbeid på dette feltet. Med unntak av en resolusjon om bekjempelse av terrorisme har Sikkerhetsrådet så langt vist liten interesse for cyberdomenets betydning for internasjonal fred og sikkerhet. Det er det flere grunner til. Den viktigste er USA.

America first?

Flere av de stater vi normalt anser som potensielle trusler mot Norge, som Russland og Kina, har i lang tid ivret for en internasjonal avtale i FN-regi som regulerer staters bruk av cyberdomenet. En konvensjon om cyberspace. Vår nærmeste allierte har vært en sterk motstander av dette. Det skyldes ikke bare USAs generelle skepsis mot forpliktende internasjonale avtaler.

USA er i en særstilling hva gjelder digital dominans. Internett ble oppfunnet i USA. Amerikanske myndigheter og selskap har kontrollert internetts kritiske ressurser og har i stor grad diktert hvordan den globale forvaltningen av internett skal foregå. Videre har amerikanske teknologiselskap vært suverene på utvikling og innovasjon, og amerikansk sivilsamfunn, institusjoner og akademia har i stor grad dominert den internasjonale diskursen om cyberdomenet. Gjennom Snowden- avsløringene og avanserte cyberoperasjoner blant annet i Midtøsten har vi også fått et lite innblikk i hva amerikansk etterretning og militære enheter er i stand til å gjennomføre av kontroll, overvåkning og sabotasje i og gjennom digitale nettverk hvor som helst i verden.

I den grad man kan snakke om hegemoni i cyberdomenet, både teknisk og politisk, har USA tronet alene på toppen. I stedet for internasjonale avtaler har USA argumentert for utvikling av normer for cyberdomenet. Altså ikke-bindende retningslinjer for hva stater kan tillate seg å gjøre i og gjennom digitale rom i fredstid. Argumentet er kort fortalt at dersom alle parter har interesse av og er tjent med å overholde en norm så vil den bli overholdt uten at det er behov for noen bindende avtale. For eksempel å avstå fra cyberangrep mot hverandres kritiske infrastruktur, som kraftforsyning.

Norge følger i all hovedsak amerikanske posisjoner når cyberdomenet som arena for krig og konflikt en sjelden gang blir diskutert i globale multilaterale fora, som i FN. I likhet med de fleste liberale demokratier fremmer vi normutvikling fremfor globale konvensjoner og legger vekt på at åpenhet, sikkerhet, frihet og robuste nettverk må være de prinsipper en global felles forståelse av cyberdomenet må bygges på. Dette har vært kjerneverdier i amerikansk cyberpolicy helt siden internett for alvor ble et globalt anliggende.

Det er viktige prinsipper som bør forsvares. Samtidig er det prinsipper som har tjent amerikanske interesser og bidratt til å opprettholde USAs dominans og hegemoni i cyberdomenet. Sett med norske øyne har det vært positivt. USA er vår nærmeste allierte, vi har et tett sivilt og militært samarbeid og vi deler i all hovedsak de samme liberale, demokratiske grunnverdiene.

Men ting er i ferd med å endre seg, raskt. USAs hegemoni i cyberdomenet svekkes. Både politisk og teknisk. Innovasjon og teknisk overlegenhet både militært og sivilt er ikke lenger like overbevisende jamført med andre stater, særlig Kina som er i ferd med å bli en formidabel digital supermakt. Også andre stater har i dag kapasitet til å gjennomføre avansert kontroll, overvåkning og sabotasje i og gjennom digitale nettverk, og gjør det. Amerikanske myndigheter har ikke lenger formell kontroll over den globale internettforvaltningen – for øvrig et bevisst valg fra Obama-administrasjonen. Autoritære stater deler ikke USAs verdenssyn og demokratiske prinsipper om åpenhet og frihet. De forvalter og bruker cyberdomenet etter helt andre prinsipper og mål. Kort sagt, stater som ikke deler våre demokratiske grunnverdier.

Dersom USAs respons er å make America great again også i cyberdomenet vil det ha begrenset effekt for internasjonal fred og sikkerhet. Avskrekking er svært krevende og lite effektivt i cyberdomenet. Å utvikle stadig mer avanserte cyberoperasjoner, forbedre digitale forsvarsverk og styrke statens kontroll over nettverkene er kan hende nødvendig, men det vil ikke redusere risikoen for at en stat med vilje og evne iverksetter cyberoperasjoner som kan true internasjonal fred og sikkerhet.

Hvilket bringer oss tilbake til behovet for å heve blikket og ivareta fredelige relasjoner mellom stater for å unngå at krig og konflikt truer, også i cyberdomenet.

I Norge liker vi å vise til FN når sikkerhetsspørsmål av internasjonal karakter skal legitimeres. FN er et stort og mangfoldig vesen med en rekke underorganisasjoner og komiteer med varierende makt og myndighet. Russiske og kinesiske initiativ for en internasjonal cyberavtale har ikke vært reist i FNs Sikkerhetsråd men primært vært rettet mot FNs Generalforsamling og ulike FN-organisasjoner. Det er gode grunner til å være skeptisk til disse initiativene, som i stor grad søker å styrke statens kontroll over digitale rom og begrense fri informasjonsflyt.

I spørsmål om internasjonal fred og sikkerhet er det ene og alene FNs Sikkerhetsråd som har makt og myndighet til å vedta resolusjoner som forplikter stater, og som har mulighet til å sanksjonere stater som bryter resolusjonen. De stater som i størst grad evner å true internasjonal fred og sikkerhet i og gjennom cyberdomenet har vetorett i sikkerhetsrådet og ønsker ikke noe vedtak som kan begrense deres muligheter. Det gjelder altså ikke bare USA, men alle de såkalte P5 landene som også inkluderer Russland, Kina, Storbritannia og Frankrike.

Betyr det at Sikkerhetsrådet aldri vil ta opp en av de angivelig største truslene mot internasjonal fred og sikkerhet i vår tid? Den amerikanske sosiologen William Ogburn lanserte begrepet «kulturelt etterslep» - cultural lag - i 1923 for å forklare hvordan samfunnet bruker gamle forklaringsmodeller og metoder for å forstå nye tider ved raske teknologiske endringer. Ogburn er relevant fordi i cyberdomenet er det ikke bare de tradisjonelle stormaktene som har evne og mulighet til å ivareta internasjonal fred og sikkerhet, slik vi er vant til å tenke. Vi må, igjen, heve blikket.

Selv mindre aktører, som Iran, Nord-Korea, Israel og et raskt økende antall andre stater har angivelig evne og kapasitet til å gjennomføre storstilte cyberoperasjoner verden over. Operasjoner som selvsagt også kan ramme sikkerhetsrådets faste medlemmer, som de allerede har erfart om enn i begrenset skala. Alt tyder på at denne utviklingen vil fortsette, altså at forskjellen mellom staters evne til maktprojeksjon i cyberdomenet vil være betydelig mindre enn på andre arenaer.

Følgelig bør Sikkerhetsrådet søke å forsere «the cultural lag» og ta inn over seg at man befinner seg i en ny type sikkerhetspolitisk virkelighet hvor digitale nettverk utgjør fundamentene. Det burde da også være i P5 statenes interesse å etablere en felles forståelse av cyberdomenets betydning for internasjonal fred og sikkerhet, en enighet om hvilke felles kjøreregler man skal forholde seg til og om konsekvensene av å bryte de. Hvorvidt det per i dag overhodet er mulig er høyst usikkert. Men diskusjonen bør tas, nå. Før vi må se tilbake på feilene vi gjorde og nok en gang si «aldri mer». Og skal diskusjonen ha noen effekt finnes det per i dag ingen andre alternativ enn Sikkerhetsrådet.

Estland er i likhet med Norge kandidat til FNs Sikkerhetsråd i 2020. Deres president har varslet at dersom de blir valgt vil de bringe cybersikkerhet og kunstig intelligens som tema inn for Sikkerhetsrådet for første gang. Fordi det er der trusler mot internasjonal fred og sikkerhet adresseres. Det er ikke sikkert vår, og Estlands, viktigste allierte vil sette pris på et slikt initiativ. Men ofte er det dine beste venner som gir de beste rådene.

NUPI Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

Bjørn Svenungsen er gjesteforsker ved Institutt for forsvarsstudier (IFS) og har jobbet som diplomat i utenrikstjenesten siden 1999. Før han begynte ved IFS var han fagdirektør for internasjonal cyberpolitikk i Utenriksdepartementet.

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PB 7024 St. Olavs Plass, 0130 OSLO, Norway
www.nupi.no | post@nupi.no

Denne policy briefen er publisert av NUPI's Cyber Security Centre med finansiering fra forskningsprosjektet GAIA.

Prosjektet er finansiert av IKT+ programmet til Norges Forskningsråd.