IFS Insights 5/2019

Vårt digitale fundament

av Bjørn Svenungsen

Vårt samfunn og vår velstand hviler i dag på digitale fundament. Alt vi omgir oss med i det daglige og som sørger for at samfunnet fungerer er på ulike måter avhengig av digitale nettverk. Kraftforsyning, landbruk, vannforsyning, finanstransaksjoner, media, helsetjenester, politi, forsvar og etterretning, transportavvikling, myndighetsutøvelse, valg og demokratiske prosesser. Og så videre. Dette er kjent. Men hva er egentlig dette digitale fundament? Hvordan trues det? Hvordan forsvares det?

Hovedpunkter

- **Samfunnet hviler på digitale fundament. Et velfungerende cyberspace er i dag en forutsetning for et velfungerende samfunn**
- **Det skisseres tre utviklingstrekk som særlig former cyberspace og med det våre digitale fundament: *digitalisering, trusselbildet* og *militarisering***
- **Diskursen om cyberspace handler i stor grad om *sikkerhet*. Den bør også handle om *muligheter***

Et nylig avholdt seminar om cyberforsvar i regi av Institutt for forsvarsstudier (IFS), Forsvarets høgskole (FHS) indikerte at en kortfattet og overordnet klargjøring av utviklingstrekk og sammenhenger i cyberspace, rettet mot ikke-eksperter på cyberfeltet, kan være nyttig.[1] Denne artikkelen er et forsøk på en slik klargjøring. Som alle klargjøringer vil den være preget av forfatterens syn.

Denne publikasjonen utgis som en del av Planprogrammet. Mer om programmet på siste side.

CYBER: EN BEGREPSAVKLARING

Aller først, cyber er et vidt begrep som brukes ulikt i ulike sammenhenger. Det er også et prefiks, så ordet «cyber» sier egentlig ingenting når det står alene. Først når det kobles på andre ord gir det mening, som for eksempel cyberspace, cybervåpen, cyberforsvar, cyberpolitikk eller cybersikkerhet. I dagligtale og i media hører vi likevel ordet «cyber» bli brukt alene svært ofte. Det er upresist men viser som regel til digitale nettverk eller IKT-utstyr på en eller annen måte.

Videre er *cyberspace* et begrep som gjør seg dårlig på norsk. Samtidig finnes det ikke noe godt norsk ord for cyberspace. «Det digitale rom» brukes ofte som ensbetydende med cyberspace men det er også upresist. «*Det* digitale rom» indikerer at vi snakker om *ett* digitalt rom, hvilket ikke er tilfellet. Du trenger i prinsippet bare to IKT-enheter med en digital forbindelse seg imellom for å etablere et digitalt rom. Det finnes antagelig millioner av digitale rom. En ubestemt form, «digitale rom», ville vært mer presist men er lite brukt. Begrepet *cyberdomenet* brukes også på norsk som ensbetydende med cyberspace og er mer presist selv om det ofte knyttes til militære operasjonelle domener, hvor cyberspace sidestilles med luft-, sjø- og landdomenet. I denne artikkelen brukes begrepet cyberspace.

Uansett hva man velger å kalle det er cyberspace enkelt sagt et *menneskeskapt* miljø bestående av informasjon, data og IKT-infrastruktur.[2] Dette miljøet benyttes daglig av mange hundre millioner mennesker for å kommunisere, søke etter informasjon, styre og kontrollere ulike prosesser og foreta forretningstransaksjoner.

Det desidert største og viktigste digitale rom er *internett*, en fysisk infrastruktur som i realiteten er et nettverk av titusenvis av sammenkoblede nettverk. Men cyberspace inkluderer også data og IKT-infrastruktur som ikke er en del av internett. Det kan for eksempel være lukkede militære nettverk knyttet til våpensystemer eller etterretning, nettverk i styringssystemer for industri eller kraftforsyning, egne nettverk i helsesektoren, og svært mye annet som ikke nødvendigvis er koblet til internett. Cyberspace og internett er altså ikke det samme, men internett er en stor og viktig del av cyberspace.

Dersom alle digitale nettverk ved et trylleslag hadde sluttet å virke samtidig ville kaos, samfunnskollaps og menneskelige lidelser vært resultatet. Et slikt trylleslag er i dag helt usannsynlig, men likefullt; digitale nettverk er ryggraden i moderne samfunn. Sikre, robuste og velfungerende digitale nettverk er følgelig ensbetydende med et sikkert, robust og velfungerende *samfunn*. Det kan i denne sammenheng være hensiktsmessig å trekke fram tre utviklingstrekk som hver for seg og sammen bidrar til å forme cyberspace, og med det forme samfunnet.

DIGITALISERING SOM SAMFUNNSTREKK

Det første og åpenbare utviklingstrekk er *digitalisering*. En utvikling som har pågått siden nettverkenes spede begynnelse på slutten av 1960-tallet og har eksplodert siden begynnelsen av 2000-tallet. Alt digitaliseres. Det påvirker oss som enkeltmennesker ved at nær sagt alt vi gjør krever en digital tilstedeværelse. Hvilket igjen betyr at nær sagt alt vi gjør er avhengig av velfungerende digitale nettverk. Digitaliseringen de fleste av oss forholder seg til i det daglige er relatert til digitale nettverk koblet til *internett*. Når vi bruker nettbanken, signerer dokumenter via mobiltelefonen, søker om barnehageplass, leverer selvangivelsen, bruker e-post eller websider, strømmetjenester, fjernstyrer ovnen på hytta, varmeapparatet i bilen, når vi bruker apper på mobilen, når bedrifter holder oversikt over regnskap, salg, varer og tjenester – og en uendelig lang rekke andre aktiviteter, er det i all hovedsak internett vi benytter oss av.

Internett er i dag antagelig verdens viktigste infrastruktur. Det er et komplekst økosystem som er avhengig av en rekke aktører og tekniske løsninger for å fungere. Det blir for omfattende å gå inn på alt dette i denne artikkelen men det er etter min mening særlig to momenter man bør kjenne til i denne sammenheng for å forstå betydningen av

internett hva gjelder å trygge våre digitale fundament.

Den første handler om *informasjonsflyt*. Svært forenklet kan man si at all informasjonsflyt på internett foregår ved hjelp av en teknologi som evner å pakke informasjon inn i en kapsel og sende denne kapselen fra en digital enhet via ethvert nettverk som er koblet sammen i dette enorme nettverket av nettverk, til en annen digital enhet, uavhengig av infrastruktur. Altså uavhengig av hva slags digitalt nettverk kapselen passerer gjennom så lenge nettverket har et koblingspunkt, en gateway, til et annet nettverk som igjen har koblingspunkt til andre nettverk, som igjen har koblingspunkt, o.s.v. Dette systemet for informasjonsflyt – det første ble kalt Transmission Control Protocol (TCP) og var utviklet av amerikanerne Vincent Cerf og Robert E. Kahn på 1970-tallet – gjør at «utsiden» av kapselen kan leses på veien gjennom nettverkene, slik at koblingspunktene vet hvor kapselen kommer fra og hvor den skal, mens innholdet i kapselen kun kan leses av sender og mottager. Jon Bing ved Universitetet i Oslo sammenlignet TCP med en shipping-container som kan være pakket med hva som helst.[3] Så lenge containeren er riktig merket vil den komme fram, selv om den sendes via bil, jernbane, fly og tog på den samme reisen.

Det andre handler om internetts *grunnleggende arkitektur*. Hver digitale enhet som er koblet til et datanettverk har en unik IP-adresse. Det er nødvendig for at de ulike digitale enheter skal kunne finne hverandre i nettverket. I dag er flere titalls milliarder enheter koblet til internett og tallet er raskt økende. IP står for Internet Protocol og håndterer rutingen av informasjon. IP forteller oss altså hvor de nevnte kapslene, altså informasjonen, skal sendes og hvor de kommer fra. Systemet som håndterer hver enhets unike identifikasjon kalles DNS, Domain Name System.

DNS er kort fortalt et hierarkisk system for å kartlegge, fordele og registrere domenenavn, for eksempel .no eller .com. DNS oversetter domenenavn til numeriske adresser (IP-adresser) slik at enhetene 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». 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. I tillegg finnes hundrevis av speilservere som fortløpende kopierer innholdet fra rotserverne. Speilservere er lokalisert over hele verden. Administrasjon av rotserverne og dets filer, den såkalte IANA-funksjonen, er tillagt en stiftelse i California som heter ICANN (Internet Corporation for Assigned Names and Numbers) som inntil 2016 formelt var underlagt amerikanske myndigheter.[4]

Det store utvalget av tjenester og muligheter vårt digitaliserte samfunn er avhengig av er, enkelt sagt, bygget på og avhengig av disse systemene. Følgelig, for at vårt digitaliserte samfunn skal fungere er vi avhengig av at både systemet for informasjonsflyt (TDC/IP og senere protokoller) og identifikasjon (DNS) fungerer. I tillegg, selvsagt, til den grunnleggende digitale infrastrukturen, som kabler, satellitter og basestasjoner. Og mye annet jeg ikke kommer inn på her.

Digitaliseringen av samfunnet skyldes ikke bare internett. Vi har også gjort oss avhengig av digitale nettverk som ikke nødvendigvis er koblet til andre nettverk overhodet. Det kan som nevnt være lukkede nettverk i industri og næringsliv, politi, forsvar eller andre i privat eller offentlig sektor. Men systemene som brukes for informasjonsflyt og identifikasjon er i grove trekk de samme. Alle digitale nettverk, enten de er koblet til internett eller ikke, er sårbare for infiltrasjon og ondsinnede handlinger. Hvilket leder oss til det andre utviklingstrekket som nevnes i denne artikkelen.

TRUSSELBILDET I CYBERSPACE

På et overordnet nivå tar *trusselbildet* i cyberspace tre former. Noen vil sikkert hevde at det er mange flere, men i denne sammenheng hvor fokus er på å trygge vårt digitale fundament mener jeg det er hensiktsmessig

å trekke fram tre overordnede former. De to første er de formene som i hovedsak omtales i media og litteratur og som vi forholder oss til i det daglige.

Den første formen handler om *inntrengning* og bevisste eller ubevisste ondsinnede handlinger i nettverkene som sådan. Det kan være hacking av websider eller betalingsløsninger, plassering av ondsinnet programvare, offensive cyberangrep ved hjelp av cybervåpen, nettverksinntrengning for etterretningsformål, lav-skala sabotasje gjennom distribuerte tjenestenektangrep (*Distributed Denial of Service*, eller DDOS-angrep), «ransomware» og andre former for kriminalitet og annet som kan manipulere informasjon, stjele verdier, eller sette styringssystemer og infrastruktur ute av spill. Det er tilsiktede handlinger fra aktører som potensielt har vilje, evne og kapasitet til å gjennomføre et cyberangrep. Aktørene kan være stater, kriminelle, aktivister eller andre med ulike motiv. Andre stater utgjør den største cybertrusselen mot samfunnskritiske funksjoner. Noen angrep kan være svært krevende å oppdage. For eksempel kan det plasseres ondsinnet programvare i et nettverk uten at programvaren aktiveres. Aktivering kan skje lang tid senere og da kunne sette nettverket ut av spill. Det kan for eksempel skje i forbindelse med en konvensjonell krigs- eller konfliktsituasjon.

Cybersikkerhetstiltak blant private, i bedrifter og i det offentlige, og den raskt voksende bransjen av private tilbydere av cybersikkerhet, er først og fremst rettet mot denne første formen for trusler. Utfordringer knyttet til leverandørindustrien faller også inn under denne formen for trusler. Den pågående diskusjonen om bruk av kinesiske Huawei som leverandør i utbyggingen av nytt mobilnett i Norge er et eksempel.[5] I teorien kan man påvirke kodelinjer, plassere skadevare eller klargjøre for plassering av skadevare i IKT-komponenter, som det i praksis vil være tilnærmet umulig å oppdage før skadevaren blir aktivert.

Svært overforenklet kan man si at et cyberangrep kan utløses ved å legge noe uønsket i den kapselen Jon Bing sammenlignet med en shipping-container, og å merke containeren på en måte som gjør at både innhold og avsender virker tilforlatelig slik at «grensevaktene» slipper den inn. Grensevaktene er altså nettverkets brannmur og andre cybersikkerhetssystemer. Gode cybersikkerhetssystemer vil avsløre «containeren» og fjerne eller uskadeliggjøre innholdet.

Det produseres stadig nye virus og annen ondsinnet programvare etter hvert som sårbarheter i nettverk, programvare og IKT infrastruktur oppdages. Og det oppdages stadig nye sårbarheter. Hvilket er årsaken til at vi stadig må oppdatere operativsystemer, apper og annet på våre digitale enheter som PC og mobiltelefon.

Dersom en sårbarhet oppdages av andre enn produsenten av programvaren kalles det gjerne en zero-day. For eksempel om en hacker finner en måte å bryte seg inn i operativsystemet på en iPhone som produsenten, i dette tilfellet Apple, ikke selv er klar over. Såkalte «white hackers» gjør dette, ofte på oppdrag fra produsenten, for å finne og varsle om sikkerhetshull som dermed kan tettes. Andre kan selge zero-day sårbarheter, til produsenten, til kriminelle eller til myndigheter. Det er allment antatt at etterretningstjenester og sikkerhetstjenester i flere stater sitter på zero-day sårbarheter de ikke tilkjennegir for å kunne benytte disse i en gitt situasjon.

Prinsippet om «containeren» som stanses gjelder enkelt sagt også ved et såkalt digitalt grenseforsvar (også omtalt som tilrettelagt innhenting av grenseoverskridende elektronisk kommunikasjon). Det vil gi etterretningstjenesten mulighet til å sjekke «utsiden» av alle «containere» som sendes fra nettverk som befinner seg utenlands gjennom koblingspunkt til nettverk i Norge og dermed kunne sjekke om de er mistenkelige eller har skadelig innehold. Det vil gjøre det enklere å stanse og uskadeliggjøre cyberangrep og ondsinnet programvare fra å nå nettverk i Norge. Samtidig muliggjør det å åpne «containerne» for å kontrollere innholdet. Altså overvåking av innhold. Det kan være problematisk av flere grunner som jeg ikke skal gå inn på her, og leder oss til den neste formen for trusler i cyberspace.

Den andre formen for cybertrusler handler om ulovlig eller ondsinnet *distribu-*

sjon av innhold, men hvor man ikke nødvendigvis benytter seg av ulovlig inntrengning i nettverk, avanserte tekniske kapasiteter eller skadelig programvare. Det kan for eksempel dreie seg om distribusjon av overgrepsbilder, rekruttering eller propaganda for terrororganisasjoner, salg av våpen, mennesker og narkotika, politiske påvirkningsoperasjoner, svindelforsøk («Nigeriabrev»), med mer. Man benytter seg altså her av cyberspace, som regel internett, på måter som cyberspace legitimt er konstruert for, men med ondsinnede eller kriminelle motiv. Distribusjonen kan foregå på mange måter, både som åpen og kryptert informasjon og via det såkalte «dark web» som kort fortalt er websider som ikke er tilgjengelig via ordinære nettlesere.

En form for digitalt grenseforsvar, hvor man altså kan åpne «containerne» og sjekke innholdet, vil også kunne bidra til å bekjempe denne form for trusler.[6] Samtidig skaper det et krevende terreng i grenseområdet mellom individers rettigheter og statens sikkerhet. Ettersom TCP/IP og DNS som forklart ovenfor vil kunne hjelpe «grenseforsvaret» med å identifisere hvem avsender og mottager potensielt kan være, så kan man lett forestille seg at et digitalt grenseforsvar kan identifisere kommunikasjon fra for eksempel terrorister eller fremmede staters etterretningstjenester og følgelig legitimere innholdskontroll. Flere og flere stater har innført eller er i ferd med å innføre denne type kontroll. I vestlige demokratier vil det være krav om rettslig kjennelse før man kan gå til det skritt. Andre steder, som i Kina, kontrolleres all elektronisk kommunikasjon systematisk for innhold og sensureres eller stanses dersom det inneholder uønsket informasjon, for eksempel kritikk av myndighetene. Kina har for øvrig et meget avansert digitalt grenseforsvar, gjerne omtalt som «Den store brannmur».[7]

Den siste og minst omtalte formen for trusler mot cyberspace handler om *trusler mot internett* sin arkitektur og form som sådan. Den er i hovedsak politisk motivert. Et velfungerende internett er tuftet på prinsippene om *åpenhet, sikkerhet, robusthet og frihet*.[8] Nettet må gi alle lik tilgang gjennom internasjonale konsensusbaserte standarder, det må sikre informasjonen vi deler og henter, det må være stabilt og tillitsvekkende, og det må sikre fundamentale menneskerettigheter som ytringsfriheten og retten til informasjon. Dette er prinsipper som har vært gjeldende siden de første nettverkene ble etablert og har vært helt avgjørende for den innovasjon og utvikling internett representerer. Trusselen mot disse prinsippene, som dagens internett er tuftet på, er følgelig av en helt annen karakter enn de to foregående. Det er her snakk om en trussel mot dagens digitale fundament som system. Denne utfordringen er i stor grad knyttet til at staten som aktør for alvor har fått øynene opp for betydningen av internett.

Statens rolle i utviklingen av internett har vært begrenset. Hvis man ser bort fra rene militære kapasiteter har innovasjon, utvikling og eierskap i all hovedsak vært knyttet til privat sektor og forskningsmiljøer (som kan være statlige). Dette har endret seg raskt de senere årene, hvor staten som aktør har engasjert seg sterkere i utviklingen av internett, og for så vidt cyberspace som sådan. Denne utviklingen har skutt fart i takt med samfunnets økende digitale avhengighet og medfølgende digitale trusler. Økt statlig cyberengasjement er en utvikling vi ser i de fleste stater i dag. Trenden går i retning av økt suverenitetshevdelse også i cyberspace, selv om særlig internett i liten grad er konstruert for å ta hensyn til tradisjonelle geografiske grenser.

For noen stater utgjør imidlertid prinsippene for et velfungerende internett en utfordring, og en trussel i seg selv. Dette gjelder særlig autoritære stater. Fri informasjonsflyt og ytringsfrihet er ikke alltid akseptabelt for autoritære og illiberale regimer. Kinas «store brannmur» er kanskje det beste og mest kjente eksempelet på at en autoritær stat forsøker å sensurere og kontrollere internett. Videre er det enkelte stater, blant annet Russland, som ønsker egne DNS, altså egne nasjonale rotservere.[9] Dermed vil informasjonsflyten i nasjonale eller regionale nettverk ikke være avhengig av å gå via ICANNs rotservere eller speilservere. Disse statene hevder blant annet at USAs fysiske kontroll over rotserverne er problematisk da USA i

en gitt situasjon vil kunne misbruke denne kontrollen til å manipulere eller hindre informasjonsflyten.[10] Frykten for at USA skal tukle med rotserverne er antagelig ubegrunnet, men med et «internett» basert på egne rotservere vil en stat enklere kunne kontrollere informasjon som flyter gjennom nettverkene og enkelt kunne sensurere utenlandske nettsider, og utestenge utenlandske nettverk. Årsaken til ønsket om nasjonale eller regionale nettverk med egen DNS er følgelig mer å kunne kontrollere og sensurere egne borgere enn frykt for USAs dominans.

Rent teknisk er det ingenting i veien for å etablere egne DNS, det er gjort en rekke steder både i lokal og nasjonal målestokk. En nasjonal DNS vil for eksempel kunne sikre kommunikasjon over nasjonale nettverk i en krisesituasjon. Problemet er, iallfall i denne sammenheng, at nasjonale eller regionale nettverk med et eget rotsystem ikke lenger vil være en del av internett. Eller rettere, det vil etablere separate internett som kommuniserer med det globale internett vi kjenner i dag kun etter myndighetenes forgodtbefinnende. En slik utvikling, ofte omtalt som splinternett, eller balkanisering av internett, vil potensielt kunne undergrave dagens åpne, frie internett og være til hinder for innovasjon og global kommunikasjon, handel og økonomi.

For å sikre opprettholdelsen av et velfungerende globalt internett kreves internasjonalt samarbeid og dialog hvor både stater og nøkkelaktører fra privat sektor og akademia deltar. Ingen land kan løse denne utfordringen alene.

MILITARISERING AV CYBERSPACE

Det tredje utviklingstrekket er *militariseringen*, eller «våpenifiseringen», av cyberspace. Militariseringen tar to former. Den ene er innføringen av stadig mer avanserte offensive cybervåpen som er i stand til å skade eller ødelegge objekter i cyberspace. Altså cybervåpen hvis hensikt er å skade eller ødelegge andre cyberkapasiteter.
Den andre formen handler om at cyberspace i seg selv i økende grad blir ansett som en militær ressurs. Dagens våpensystemer er ofte svært avhengig av en velfungerende IKT-infrastruktur og cyberspace har derfor blitt et mye omstridt militært domene. Betydningen av cyberspace som militært domene ble understreket av det amerikanske forsvarsdepartementet allerede i 2006 da de fastslo at det amerikanske forsvaret ville vurdere kinetiske militære anslag som virkemiddel for å kunne bevare sin handlingsfrihet og sine strategiske fordeler i cyberspace[11]. En lignede, dog mer defensiv uttalelse, ble gitt av NATOs ledere i 2016 hvor de anerkjente cyberspace som «et operasjonelt domene hvor alliansen må forsvare seg like effektiv som den gjør i luften, på land og på sjøen».[12] Enkelte, herunder forfatteren, argumenterer for at «våpenifiseringen» av cyberspace innebærer en betydelig høyere risiko for internasjonale konflikter og følgelig kan utgjøre en trussel for internasjonal fred og sikkerhet. Altså at man kan nå et nivå som rettmessig kan kalles *cyberkrig*.

Cyberkrig er et begrep som i media og litteratur ofte benyttes om nær sagt enhver av de to første trusselformene nevnt ovenfor. Det er svært upresist. Som nevnt huser cyberspace et bredt spekter av trusler mot stater og individer. Selv om dette er ondsinnede og kriminelle handlinger er det svært sjelden de når et nivå som kvalifiserer for krigshandlinger – *acts of war*. For å være en krigshandling i cyberspace må den ondsinnede handlingen være gjennomført, kontrollert eller godkjent av statlige myndigheter, det må benyttes cybervåpen og hensikten må være å påføre alvorlig skade eller ødeleggelse. Mette Eilstrup-Sangiovanni har i sin definisjon fra 2018 formulert det slik: «Cyberkrig er tilsiktet og ondsinnet bruk av cybervåpen av en stat med den hensikt å påføre skade eller død til personer og/eller i betydelig grad forstyrre, skade eller ødelegge en annen stats strategiske ressurser eller kritisk nasjonal infrastruktur».[13]

Definisjonen er presis og utelukker mange av de trusler som i dagligtale ofte omtales som «cyberkrig», herunder ulovlig nettverksinntrengning for økonomisk vinning og annen IKT-kriminalitet, etterretningsvirksomhet, industrispionasje eller politiske påvirkningsoperasjoner.

Militariseringen av cyberspace vil fortsette. Kombinert med utviklingen av kunstig intelligens (AI) og andre teknologier er det sannsynlig at vi i fremtiden vil stå overfor cybervåpen som evner å gjennomføre operasjoner vi i dag ikke kan forestille oss. Samtidig er det verdt å huske at selv om det i dag er stor forskjell på staters cyberkapasiteter er forskjellen mellom staters evne til å projisere makt gjennom cyberdomenet mye mindre enn i konvensjonelle domener. Hvilket betyr at selv mindre stater som ikke utgjør noen konvensjonell trussel kan være, eller bli, i stand til å gjennomføre svært alvorlige cyberopera-sjoner hvor som helst i verden.

Erkjennelsen av den potensielt ødeleggende effekt cybervåpen kan ha på samfunn og mennesker har drevet fram diskusjonen om behovet for internasjonale kjøreregler som regulerer staters bruk av cyberspace. Det foreligger en generell enighet om at folkerettens prinsipper for maktanvendelse også gjelder i cyberspace, men det er ingen enighet om hvordan folkerettens bestemmelser skal tolkes i denne sammenheng. Det er også gjort forsøk på å fremforhandle normer, ikke-bindende retningslinjer, som konfliktforebyggende tiltak i cyberspace. Noen har også tatt til orde for en ny og separat bindende konvensjon for å regulere staters bruk av cybervåpen,[14] eller for en egen forpliktende resolusjon fra FNs Sikkerhetsråd med muligheter for å sanksjonere stater som bryter resolusjonen.

Vi er i dag svært langt unna enighet om et internasjonalt regelverk for staters bruk av cyberspace. Diskusjoner om dette har ennå ikke funnet en konstruktiv og endelig form. Hvorvidt det internasjonale samfunn vil lykkes med å komme fram til enighet om et sett regler for å forebygge cyberkrig utover en generell henvisning til eksisterende folkerett er meget uvisst.

DET NORSKE BILDET

Jeg har ovenfor grovt skissert et bilde hvor (1) digitaliseringen har gjort samfunnet helt avhengig av et velfungerende cyberspace hvor internett er det desidert største og viktigste element, hvor (2) trusselbildet er stort, bredt og svært alvorlig, og har potensiale til å ødelegge cyberspace slik vi kjenner det, og hvor (3) militariseringen av cyberspace har potensiale til å true internasjonal fred og sikkerhet.

Det er tre distinkte utviklingstrekk som samtidig henger tett sammen og ofte er vanskelig å skille fra hverandre. For å håndtere utfordringene dette representerer er det behov for utstrakt samarbeid på tvers av alle sektorer i samfunnet. Det krever offentlig-privat samarbeid, sivilt-militært samarbeid, og internasjonalt samarbeid. Og det krever koordinering. Hvem i Norge er pålagt oppgaven med å se hele dette kompliserte bildet i sammenheng, og har evne og myndighet til å ta de nødvendige grep for å sikre at vårt digitale fundament består?

Det korte svaret er mange. Veldig mange.

Justis- og beredskapsdepartementet(JD) har samordningsansvaret for sivil digital sikkerhet og er i en særstilling. Nasjonal sikkerhetsmyndighet, (NSM) er det nasjonale fagmiljøet for digital sikkerhet og understøtter JDs ansvar på området. NorCERT er den operative delen av NSM, med et koordinerende ansvar for IKT-sikkerhetshendelser og generell hendelseshåndtering på cyberfeltet. De rapporterer også til Forsvarsdepartementet (FD) som sammen med underliggende etater har en viktig rolle hva gjelder digital sikkerhet i forsvarssektoren.[15] Etterretningstjenesten (E-tjenesten) har ansvaret for «tidlig varsling av mulige ytre cybertrusler fra fremmede stater, organisasjoner eller individer». [16] Cyberforsvaret har ansvaret for å beskytte Forsvarets IKT-systemer mot digitale trusler. I tillegg kan Forsvaret gi bistand til sivil sektor ved behov.

Andre aktører i justissektoren er også svært viktige i denne sammenheng. Politiets sikkerhetstjeneste (PST) er en nøkkelaktør hva gjelder overvåkning og etterforskning av ulike cybertrusler fra både statlige og ikke-statlige aktører. Politidirektoratet (POD), Kripos og politidistriktene etterforsker ulike former for IKT-kriminalitet. Samferdselsdepartementet (SD) og det underliggende Nasjonal kommunikasjonsmyndighet (NKOM) er en nøkkelaktør for

å sikre et velfungerende internett i Norge. Utenriksdepartementet deltar i den internasjonale debatten om folkerettens anvendelse i cyberspace og en rekke andre diskusjoner om internasjonal cyberpolitikk. Kommunal- og moderniseringsdepartementet og Direktoratet for forvaltning og IKT (Difi) har et betydelig ansvar hva gjelder utvikling av, og sikkerhet i, statlige digitale tjenester. Viktige oppgaver også tillagt Direktoratet for samfunnssikkerhet og beredskap (DSB) og Datatilsynet for å nevne noen. Det er med andre ord ganske mange.

I tillegg kommer en rekke private virksomheter som har nøkkelroller i å drifte og opprettholde digitale nettverk, som for eksempel Telenor AS, eller i forvaltningen av internett, som for eksempel UNINETT Norid AS. Det er også slik, hvis vi snevrer det inn til kun å handle om digital sikkerhet, at den enkelte virksomhet, enten det er et multinasjonalt konsern eller et enkeltmannsforetak med hjemmekontor, selv er ansvarlig for å foreta risikovurderinger og å gjennomføre tilstrekkelig tiltak.

Likevel, Norge er relativt sett blant de bedre i klassen internasjonalt hva gjelder digital sikkerhet og robuste nettverk. Vi har et stort og økende fokus på cybersikkerhet både i offentlige og private virksomheter, og vi har folk med høy kompetanse, selv om vi trenger mange flere. I Norge har vi også en tydelig ansvarsdeling mellom ulike sektorer i samfunnet. Det gjør at den enkelte sektor, for eksempel finans- eller helsesektoren, evner å identifisere hvilke digitale sikkerhetsutfordringer man har og ta spesifikke grep for å løse disse som er tilpasset sektorens krav og behov, og som forener digital sikkerhet og funksjonalitet.

Samtidig er denne ansvarsdelingen kanskje vår største svakhet. Når alle har fokus på egen sektor mangler vi noen som kan se helheten.[17] Se utviklingstrekkene i cyberspace i sammenheng. Noen som evner å se hele bildet av trusler og muligheter samtidig. Og som har myndighet til å ta beslutninger over sektornivå. Det som er best for den enkelte sektor er ikke nødvendigvis best for landet som helhet.

Man kan hevde at fordi digitale nettverk påvirker «alt» bør ikke cyberspace behandles som noe særskilt men heller som en integrert del av alle samfunnsområder, spesielt hva gjelder sikkerhet. Men det argumentet kan også snus rundt. Nettopp fordi cyberspace er så integrert og fundamentalt for alle samfunnsområder bør det ses i sammenheng. En sektortankegang gjør at vi risikerer å ikke se sammenhengene og kan miste oversikten over det store bildet.

Men vi er på riktig vei. Regjeringen lanserte i januar 2019 en ny nasjonal strategi for digital sikkerhet.[18] Gjennom en rekke tiltak søker den strategien å møte mange av de utfordringer som er skissert ovenfor. Og mer. Virkeligheten spiser som kjent strategier til frokost. Men dersom intensjonene og tiltakene gjennomføres vil denne strategien kunne være et viktig bidrag til å trygge våre digitale fundament også i fremtiden. Spesielt positivt er det at strategien tilsynelatende evner å se store deler av utviklingen i cyberspace i sammenheng og vektlegger samarbeid mellom privat og offentlig virksomhet, sivilt-militært samarbeid og internasjonalt samarbeid.

Det strategien *ikke* gjør er å etablere en myndighet med nødvendig makt over sektornivå hvis oppgave er å se utviklingen i cyberspace i sammenheng og koordinere politikk og tiltak på cyberområdet både nasjonalt og internasjonalt. En myndighet som ikke bare fokuserer på sikkerhet, men også på muligheter, marked, utvikling og innovasjon. Per i dag er en slik myndighet antagelig ikke ønsket fra myndighetenes side. Kanskje er den heller ikke mulig å etablere, gitt organisatoriske og konstitusjonelle forhold. Man kan tenke seg at en slik myndighet måtte kobles til Statsministerens kontor (SMK) for å kunne ha den nødvendige sektorovergripende makt, iallfall i offentlig sektor. Men SMK er ikke rigget til den type operativ virksomhet. I tillegg ville det budt på konstitusjonelle utfordringer.

Ett av tiltakene i strategien, etableringen av et Nasjonalt cybersikkerhetssenter, vil langt på vei kunne fylle den samme rollen og være den type myndighet forfatteren etterlyser. Senteret vil riktignok være underlagt Justis- og beredskapsdepartementet og Forsvarsdepartementet og følgelig ikke være

sektoruavhengig. Likevel, dersom det på sikt evner å trekke på kompetanse også utenfor rene sikkerhetsmiljøer for å kunne danne seg et bilde og se sammenhengene mellom sikkerhet og andre utviklingstrekk i cyberspace vil det være et stort skritt i riktig retning.

AVSLUTNING

Den gjengse oppfatningen av cyberspace er i dag i økende grad formet av sikkerhetsmiljøer. Den offentlige diskurs om cyberspace handler derfor ofte om sikkerhet og trusler, og hvordan vi skal trygge våre verdier og vårt samfunn. Det er en svært viktig diskusjon som vi må ta, og ta konsekvensene av. Å trygge vårt digitale fundament er kostbart, men kostnadene ved å ikke gjøre det vil være mye større. Samtidig må vi huske at cyberspace ikke først og fremt handler om *sikkerhet*. Det handler om *muligheter*. Nye og uante muligheter.

Med unntak av i militære sammenhenger kan man ikke sammenligne cyberspace med land-, sjø-, og luft-domenene. Det er særlig én stor forskjell. Cyberspace er menneskeskapt og i motsetning til naturen avhengig av mennesker for å eksistere. Men i likhet med landjorda, lufta og sjøen er cyberspace først og fremst en ressurs til det gode for mennesker. Skal vi nyttiggjøre oss av denne ressursen også i fremtiden må vi forstå betydningen av et bærekraftig cyberspace og hvilke implikasjoner cyberspace har på samfunnet. Det handler om årsaker og virkninger. Om historie, samfunnsfag, statsvitenskap og naturfag. Om ingeniørkunst og innovasjon. Og mye mer. Kan hende er det i dette landskapet nøkkelen til vår fremtidige eksistens ligger gjemt. Det gjelder å ikke kaste den bort.

REFERANSER:

[1] IFS seminaret "How to do Cyber Defence?" ble avhold i Oslo Militære Samfund 17. januar 2017. Innleggene er tilgjengelig på webadressen: https://forsvaret.no/hogskolene/how-to-do-cyber-defence [8. mai 2019].

[2] CCDCOE, Tallin Manual 2.0 (Talin: CCDCOE, 2017). Tilgjengelig online: https://ccdcoe.org/research/tallinn-manual/ [8. Mai 2019].

[3] Bing, Jon, «Building Cyberspace: A Brief History of Internet» in *Internet Governance: Infrastructure and Institutions* redigert av Lee A Bygrave og Jon Bing (Oxford: Oxford University Press, 2009), 26.

[4] Les mer på ICANS hjemmeside, https://www.icann.org/iana-transition-fact-sheet [8. Mai 2019].

[5] NRK, «Huawei kan bli utestengt fra norsk 5G-utbygging", NRK, 10. januar 2019. Tilgjengelig online: https://www.nrk.no/norge/huawei-kan-bli-utestengt-fra-norsk-5g-utbygging-1.14373969 [8. Mai 2019].

[6] Lysne II-utvalget, *Digitalt grenseforsvar* (DGF). Oslo: Forsvarsdepartementet, 2016.

[7] Bloomberg News, «The Great Firewall of China», *The Washington Post*, 5. November 2018.

[8] The White House. *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington D.C., The White House, 2011).

[9] Christiana Abella Matamoros og Naira Davlashyan, «Runet: Russia wants to «nationalise the inernet» but what does it mean?», *Euronews*, 13. Februar 2019. Tilgjengelig online: https://www.euronews.com/2019/02/12/new-russian-internet-bill-just-another-layer-of-censorship-says-tech-expert [8. Mai 2019].

[10] NTB, «Planer om russiske øvelser der internettkabler til utlandet stenges», *Aftenposten*, 12. Februar 2019. Tilgjengelig online: https://www.aftenposten.no/verden/i/5VXKPK/Planer-om-russiske-ovelser-der-internettkabler-til-utlandet-stenges [8. Mai 2019].

[11] US Department of Defense. «National Military Strategy for Cyberspace Operations» (Washington D.C.: US DoD, 2016). Tilgjengelig online: https://www.hsdl.org/?abstract&did=35693 [8. Mai 2019].

[12] NATO, «Cyber defence» (Brussel: NATO, 2018). Tilgjengelig online: https://www.nato.int/cps/en/natohq/topics_78170.htm [8. Mai 2019].

[13] Forfatterens oversettelse. Mette Eilstrup-Sangiovanni, «Why the World Needs an International Cyberwar Convention», *Philosophy and Technology* 31, nr. 3 (September 2018), 383.

[14] Eilstrup-Sangiovanni, «Why the World Needs an International Cyberwar Convention», 379–409.

[15] Forsvarsdepartementet, «Forsvarsdepartementets retningslinjer for informasjonssikerhet og cyberoperasjoner i forsvarssektoren» (Oslo: FD, 2014). Tilgjengelig online: https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf [8. Mai 2019].

[16] Forsvarsdepartementet, «Forsvarsdepartementets retningslinjer for informasjonssikerhet og cyberoperasjoner i forsvarssektoren», 17.

[17] Eivind Smith, «Ministerstyre» - et hinder for samordning?». *Nytt Norsk Tidsskrift* 32, nr. 3 (2015): 258–266.

[18] Regjeringen, *Nasjonal strategi for digital sikkerhet* (Oslo: Departementene, 2019).

IFS INSIGHTS

IFS Insights er et fleksibelt forum for artikler, kommentarer og papere innenfor Institutt for forsvarsstudiers arbeidsområder. Synspunktene som kommer til uttrykk i IFS Insights, står for forfatterens regning. Hel eller delvis gjengivelse av innholdet kan bare skje med forfatterens samtykke.

Redaktør: Kjell Inge Bjerga

INSTITUTT FOR FORSVARSSTUDIER

Institutt for forsvarsstudier (IFS) er en del av Forsvares høgskole (FHS). Som faglig uavhengig høgskole utøver FHS sin virksomhet i overensstemmelse med anerkjente vitenskapelige, pedagogiske og etiske prinsipper (jf. Lov om universiteter og høyskoler § 1-5).

Direktør: Kjell Inge Bjerga

Institutt for forsvarsstudier
Akershus festning, bygning 10
Postboks 1550 Sentrum
0015 OSLO
E-post: info@ifs.mil.no
ifs.forsvaret.no

OM FORFATTEREN

Bjørn Svenungsen har vært tilknyttet Utenriksdepartementet (UD) siden 1999. Han har tjenestegjort ved OSSE-delegasjonen i Wien og ambassaden i Ljubljana samt vært kommunikasjonsrådgiver/pressetalsmann i UD, Kommunikasjonsdirektør NVE og arbeidet som krisestabssjef i UD. Han var Cyberkoordinator og fagdirektør for internasjonal cyberpolitikk i UD 2013–2018 og gjesteforsker ved IFS fra januar 2018 til april 2019.

PLANPROGRAMMET

PLANPROGRAMMET er et forskningsprogram ved IFS i perioden 2018–2020. Gjennom programmet yter IFS forskningsbaserte bidrag til langtidsplanleggingen i forsvarsektoren. Programmet har en anvendt profil som arena for kunnskapsutvikling i samspill med nasjonal og internasjonal ekspertise. For det første bidrar programmet til Forsvarsdepartementets kontinuerlige langtidsplanlegging. Gjennom lukkede og åpne seminarer, orienteringer og policy-notater løftes de mest aktuelle problemstillingene frem og analyseres. For det andre bistår programmet med forskning som går i dybden av langsiktige og grunnleggende problemstillinger. Resultatene diskuteres og bekjentgjøres gjennom konferanser og akademiske publikasjoner.

PLANPROGRAMMET PÅ INTERNETT

https://forsvaret.no/ifs/Forskning/planprogrammet-langtidsplanlegging-forsvarssektor

Forsidefoto:
The Nato Cooperative Cyber Defence Centre of Excellence
Picture is taken from the cyber defence exercise «Locked Shields».