FFI-rapport 2013/02712

Cyberdomenet, cybermakt og norske interesser

Torbjørn Kveberg og Siw Tynes Johnsen

FFI Forsvarets forskningsinstitutt

Cyberdomenet, cybermakt og norske interesser

Torbjørn Kveberg og Siw Tynes Johnsen

Forsvarets forskningsinstitutt (FFI)

5. mars 2014

FFI-rapport 2013/02712

1260

P: ISBN 978-82-464-2340-1
E: ISBN 978-82-464-2341-8

Emneord

Cyberdomenet

Cybermakt

Sikkerhetspolitikk

Utenrikspolitikk

Godkjent av

Ronny Windwik	Prosjektleder
Anders Eggen	Avdelingssjef

Sammendrag

Formålet med denne rapporten er å belyse hvordan cyberdomenet og cybermakt er relevant for norske interesser i en globalisert verden. Denne kunnskapen skal bidra i prosjektets videre arbeid med Forsvarets mulige fremtidige roller.

Rapporten er tuftet på lærdommer fra cybermaktstudiens kartleggingsrapport hvor cyberdomenet defineres og dets egenart, samt sentrale trender beskrives. I likhet med foregående maktstudier ved FFI, drar denne rapporten veksel på arbeidene gjort i Utenriksdepartementets Refleksprosjekt siden 2006. Refleksprosjektet ble etablert av daværende utenriksminister Jonas Gahr Støre for å fremme en bredere debatt om norsk utenrikspolitikk. Foregående helhetlige gjennomgang av norsk utenrikspolitikk i statlig regi ble gjort i 1989. Refleksprosjektet ble derfor etablert med sikte på å holde debatten gående også etter en ny stortingsmelding om norske interesser i verden. Debatten har så langt munnet ut blant annet i boken Norske Interesser. Utenrikspolitikk for en globalisert verden og Stortingsmelding 15 (2008-2009) Interesser, ansvar og muligheter. Hovedlinjer i norsk utenrikspolitikk. Disse verkene tjener som forankringspunkt for temaene som tas opp i denne rapporten.

Cybermaktstudien er nybrottsarbeid, og domenet i seg selv abstrakt og komplisert å forstå. En unik utfordring kommer av at det ikke foreligger et erfaringsgrunnlag for utøvelse av cybermakt mellom stater sammenlignbart med det vi har i de øvrige domenene. Så langt har det ikke vært noen cyberkrig, ei heller har mellomstatlige konflikter inkludert åpenlys bruk av cybermakt sammen med konvensjonell militærmakt. Den ondsinnede aktiviteten som foregår er primært etterretning og kriminelle handlinger. Rapporten går derfor bredt ut og søker å relatere cyberdomenet og cybermakt til norske interesser der det er mulig – uavhengig av om emnet har en umiddelbart åpenbar relevans for Forsvaret.

Det er mange emner som skal dekkes og antagelig ennå fler det kunne være interessante å ta opp eller gå dypere inn i. På bakgrunn av erfaringene med arbeidet så langt vil mer forsvarsrelaterte emner velges ut til en dypere og mer analytisk gjennomgang i en ny rapport. Sannsynlige emner vil da være etterretning og spionasje, bistandsinstruksen og nasjonalisering eller regionalisering av Internett.

English summary

This report sheds light on how cyberspace and cyber power relates to Norwegian national interests in a globalized world. This effort will allow the project to continue discussing the potential future role of the Norwegian Armed Forces in cyberspace.

The report is based on knowledge from a former report by FFIs project on cyber power, where the cyber domain was defined, and its unique traits and central trends described. As with similar studies for the other domains carried out by FFI, this report draws on the written works of the Norwegian Foreign Ministry's "Refleksprosjekt" since 2006. Refleksprosjektet was founded by then Minister of Foreign Affairs, Jonas Gahr Støre, in an effort to inspire a broader debate on Norwegian foreign policy. Prior to this, the last broad study of Norwegian foreign policy was done in 1989. Refleksprosjektet thus aimed not only to renew this effort, but to keep the debate going also after new policies were established based on their findings. The two most prominent works of the project so far has been the book Norwegian interests. Foreign policy for a globalized world as well and the now passed draft resolution Stortingsmelding 15 (2008-2009) Interests, responsibilities and opportunities. Guidelines for Norwegian foreign policy. These are the two primary works serving as anchor points for this report.

This report is breaking new ground in terms of relating issues of cyberspace to Norwegian foreign policy, and the domain itself is both abstract and complicated to understand. One unique challenge stems from the fact that we have no prior experience with cyber power on the state level comparable to that of the other domains. There has not been a cyber war to date, nor have any interstate conflicts seen an actor openly using cyber weapons along with conventional forces. Thus, this report approaches the topic in broad terms seeking to relate cyberspace and cyber power to Norwegian national interests where possible – even if the topic seems unrelated to the Norwegian Armed Forces.

There are a lot of topics to cover, and most likely many more which would be interesting to delve deeper into. A selection of the most interesting topics will be chosen on the basis of the experiences with this report, and analyzed more deeply in a following report. Likely subjects include intelligence and espionage, military assistance to the civilian sector and the nationalization or regionalization of the Internet.

Innhold

1 Oppsummering

Landegrenser eksisterer ikke i cyberdomenet, og samtidig er mesteparten av det privateid. Dette gjør at Forsvaret ikke kan gjennomføre en form for suverenitetshevdelse sammenlignbar med den vi finner i de øvrige domenene. Den nærmeste analogien til et statlig sikkerhetstilbud mot ondsinnede handlinger finnes hos Nasjonal Sikkerhetsmyndighets (NSM) dataovervåkingssenter NorCERT først og fremst for objekter underlagt Sikkerhetsloven. Utover dette er cybersikkerhet i stor grad opp til den enkelte sektor/virksomhet. Spesielt på Internett står derfor alle ansikt til ansikt med et globalt trusselbilde.

Cyberforsvaret støtter opp under nasjonal sikkerhet først og fremst igjennom å sikre Forsvarets egne systemer i en tid hvor operativ evne og effektivitet knyttes stadig tettere opp mot informasjonsteknologi. I årene som kommer vil Forsvaret og få et økende behov for å føre tilsyn med store havområder i nord, blant annet igjennom teknologiske løsninger for overvåking av for eksempel skipsfart. Som tilrettelegger for effektiv maktutøvelse i de øvrige domenene bidrar derfor spesielt defensiv cybermakt til ivaretagelsen av norsk territoriell suverenitet.

Det arbeides iherdig for å få de resterende to tredjedelene av verdens befolkning på Internett. Ivaretagelsen av et fritt og åpent Internett støtter opp under en rekke norske interesser, hvorav de viktigste antagelig er økt statlig sammenknytning og økonomisk vekst igjennom Internettøkonomien og bedre kår for demokratiske verdier slik som ytringsfrihet. Samtidig innebærer dette at utfordringer knyttet til kriminelle handlinger i cyberdomenet vil bli større i årene som kommer.

Nye muligheter for kommunikasjon, organisering og potensielt ondsinnede handlinger i et globalt domene uten meningsfulle landegrenser byr på nye muligheter og utfordringer for Forsvarets evne til å innhente informasjon om omverdenen. Edward Snowdens avsløringer om amerikanske etterretningsprogrammer i cyberdomenet illustrerer hvordan innhenting og deling av informasjon i cyberdomenet aksentuerer utfordringer knyttet til balansegangen mellom sikkerhet og individets rettigheter, samt juridiske skiller mellom egne og andre staters borgere.

Igjennom nasjonalt lovverk kan stater på en skjult måte bedre egne forutsetninger for å projisere makt i eller igjennom cyberdomenet. Dette innebærer nødvendigvis og at et tydelig lovverk kan benyttes på en åpenlys måte til å gjøre Norge mer attraktivt for både virksomheter og deres kunder.

Utøvelsen av cybermakt kan ha negative konsekvenser for andre interesser. Edward Snowdens avsløringer har for eksempel hatt negativ innvirkning på dialogen mellom USA og Kina vedrørende spionasje og ført til at flere stater nå tar til orde for økt nasjonal kontroll over Internett. En nasjonalisering eller regionalisering av Internett vil ha negative innvirkninger på norske økonomiske interesser, men potensielt også mykere verdier som ytringsfrihet som Norge anser som understøttende for en mer stabil verdensorden.

Det er store utfordringer knyttet til kriminelle handlinger i cyberdomenet, enten disse er ordinær vinningskriminalitet eller rettet spionasje i statlig og ikke-statlig regi for å fremme egne økonomiske interesser. Anslag på kostnadene dette påfører både ofre og samfunn er svært usikre. Konsekvensene kan være at viktige næringslivsaktører i vår nasjonale økonomi mister sitt konkurransemessige fortrinn, eller på sikt en mer helhetlig utkonkurrering av for eksempel teknologiområder. Forsvaret og forsvarsteknologi er her mål som kan gi motparten informasjon med både sikkerhetspolitisk og økonomisk verdi.

En forholdsvis brå økning i etterspørselen etter kompetanse innen cybersikkerhet i både offentlig og privat sektor gjør at det er stor etterspørsel etter kvalifisert arbeidskraft. Dette behovet går igjen også i flere andre stater hvilket kan gjøre det utfordrende å trekke til seg slik kompetanse fra utlandet, samtidig som Norge er et forholdsvis lite land med begrenset rekrutteringsbase. Flere stater setter nå i gang tiltak for å øke tilgjengeligheten på slik kompetanse nasjonalt. Forsvaret er her en av de aktørene som også må leve med krav om sikkerhetsklarering og konkurrere på lønn med private sektor. Både Cyberforsvaret, NSM og FFI har her bidratt til å etablere ett fagmiljø innen cybersikkerhet ved Høgskolen i Gjøvik.

Siden virksomheter står ansikt til ansikt med et globalt trusselbilde kan et velfungerende nasjonalt cybersikkerhetsregime og tilgang på kompetanse gi Norge et komparativt fortrinn som gjør oss attraktive for investeringer og virksomhetsetableringer fra utlandet. Flernasjonalt samarbeid og informasjonsdeling er og svært viktige komponenter i kampen mot kriminelle handlinger i cyberdomenet.

Tiltak som støtter opp under norske økonomi- og miljøinteresser ved hjelp av cyberdomenet kan ha implikasjoner for norsk sikkerhet. For eksempel gir outsourcing av bank- og teletjenester gir økt kostnadseffektivitet i næringen og smarte strømnett mer effektiv bruk av tilgjengelig elektrisitet. Samtidig blir samfunnsviktig og kritisk infrastruktur i større grad knyttet opp mot Internett og avhengig av cybersikkerhetsregimer i andre land, så vel som hos de aktørene som tar over hele eller deler av driften.

Norge har en interesse av å fremstå som en pålitelig leverandør av energi og samtidig balansere rollen som energinasjon med andre hensyn til klima og miljø. Å sørge for gode cybersikkerhetsrutiner for alle operatører på norsk sokkel kan bidra til å vise at Norge tar dette på alvor. Et rettet angrep for å forårsake produksjonsstans, anleggsskade eller miljøutslipp er antagelig svært krevende. Det foreligger allikevel eksempler på produksjonsstans andre steder i verden som følge av at en ansatt uforvarende infiserer systemer som deretter må slås av for å renses.

Det er en overgripende norsk interesse at cyber integreres i det internasjonale systemet og organisasjonene Norge ønsker skal styrkes i fremtiden, som for eksempel FN og Nato. Hvilke stater man bør samarbeide med er et vanskelig spørsmål, og man kan velge å hovedsakelig samarbeide med stater som er fysisk nære, fysisk fjerne, eller med et utvalg av stater fra begge leire. De man skal samarbeide med må man nødvendigvis dele informasjon med, og i

cyberdomenet ser man ofte et motsetningsforhold mellom ønsket om å dele informasjon om trusler og sårbarheter for å gjøre «fellesskapet» sikrere, og ønsket om å holde egne kapasiteter, kapabiliteter og sårbarheter hemmelige. Informasjonsdeling, spesielt om et så sensitivt felt som cyberdomenet, kan være utfordrende selv innenfor etablerte rammer, og når man samarbeider med partnere utenfor de tradisjonelle fellesskapene vil dette blir stadig mer utfordrende.

Norsk engasjementspolitikk er i stor grad fokusert på arbeid for menneskerettigheter, og Norge har i FN-systemet promotert både ytringsfrihet og personvern i cyberdomenet. Norge har argumentert for så få restriksjoner som mulig på informasjonsflyten på nettet, og at alle slike restriksjoner må være i overensstemmelse med internasjonale menneskerettigheter.

Norge er en av verdens mest sentrale leverandører av fredsdiplomati og en av landets viktigste merkevarer i fredspolitikken er fortrolighet. Mens cyberdomenet kanskje ikke er det man intuitivt forbinder med freds- og forsoningsarbeid kommer det i denne sammenheng frem som en viktig forutsetning for suksess, i form av godt utviklet cybersikkerhet. Skal Norge fortsette å være en fortrolig partner i sårbare fredsprosesser, må partene kunne stole på at Norge har god nok cybersikkerhet til at sensitiv informasjon om både partene selv og prosessen vil forbli fortrolig. Cybermakt i denne sammenheng vil derfor være å demonstrere at man tar cyberdomenets sårbarheter og utfordringer på alvor, og på den måten få større betydning innen internasjonalt fredsdiplomati enn landets størrelse skulle tilsi. Samtidig kan denne rollen gjøre Norge til et mål for fremmede etterretningstjenester som bruker cybermakt for å få innsyn i disse prosessene.

Identitetskonflikten mellom religiøs fundamentalisme og sekularisme som har preget dette årtusenet så langt spinner seg og ut i debattspalter, nettfora og sosiale medier på Internett. Enkeltpersoner kan fronte forestillinger om omverdenen på Internett som oppfattes som krenkende av enkelte andre steder i verden som i verste fall kan få konsekvenser for norsk samfunnssikkerhet. Også her kompliserer domenet avveininger mellom forebyggende samfunnssikkerhet og individets rettigheter som for eksempel ytringsfrihet.

En interessant observasjon hva gjelder identitet og Internett er at enkelte grupperinger har vokst frem hvor Internett i seg selv er en kjerneinteresse og kilde til identitet. Dette er ingen "konflikt" sammenlignbar med den mellom religiøs fundamentalisme og sekularisme, men like fullt et knippe interessenter unike for Internett hvor segmenter kan søke innflytelse både på lovlig (Piratpartier) og ulovlig (Anonymous) vis.

2 «Megatrendene»

2.1 Bort fra en unipolar verdensorden

Vi lever ikke lenger i en bipolar eller unipolar verdensorden med tydelige konsentrasjoner av makt på kloden. I noe varierende grad spås nå slutten på vestens dominans i verdenspolitikken ved at vi forbipasseres av de kommende økonomiske kjempene, også kjent som BRIK/BRIKS[1] landene. Vi er på vei inn i det som kalles «den fjerde bølgen av globalisering». Ifølge estimater fra 2009 ville Kina forbigå USAs produksjon innen 2027 og være dobbelt så stor i 2050. To år senere, og litt lenger ut i finanskrisen, anslo OECD at den kinesiske økonomien ville være større allerede innen 2017. I 2009 ble det og estimert at BRIK-landene vil være på nivå med vestens samlede produksjon innen 2032.[2] Selv om prediksjonene endrer seg noe fra analyse til analyse er den overordnede trenden den samme; verdens økonomiske tyngdepunkt skifter unektelig fra vest mot øst. Nøyaktig hva slags form maktbalansen vil ta er det noe mer usikkerhet rundt, og den beskrives både som multipolar og «en verden uten sentrum».[3]

Historisk sett skjer selve skiftene i maktbalansen brått, og fører med seg økt uro frem til en ny maktbalanse oppstår.[4] Verdenen i dag er imidlertid forskjellig fra den som eksisterte under forrige multipolare periode fra 1815 til 1914. Globaliseringsprosessen har vevet stater sammen og gjort dem gjensidig avhengige av hverandre. Konflikter påfører kostnader i denne veven, ikke bare for parter i konflikten men også andre i veven, og dermed kan terskelen for å gå til krig være høyere. Makten er mer spredt ut, både vekk fra ren militærmakt og vekk fra stater. Stater må i stadig økende grad forholde seg til et vell av ikke-statlige aktører, alt fra transnasjonale virksomheter og organisasjoner til sub-nasjonale aktivist- og terroristorganisasjoner.[5] Informasjonsalderen har i stor grad bidratt til dette. [6] I siste stortingsmelding om utenrikspolitikk understrekes det derfor at norske utvidede interesser i denne globale veven gjør idealpolitikken til et viktigere virkemiddel for å fremme norske interesser.[7]

Nøyaktig hva implikasjonene av dette maktskiftet vil være, og i hvilken hastighet det vil skje er derfor omdiskutert, men skiftet vil være minst like betydningsfullt som foregående skifter.[8] De prosessene som driver frem nettopp dette skiftet er, slik tallene ovenfor illustrerer, relativt langsomme og langtekkelige prosesser som strekker seg over flere tiår. Siden vi går over i en multipolar periode, en periode med fravær av tydelige maktpoler på verdenskartet, vil mer makt flyttes over i regionale fora fremfor internasjonale.[9] Ifølge Halvard Leira og Ole Jacob Sending ved Norsk Utenrikspolitisk Institutt (NUPI) kan dette innebære et dilemma for Norge hvor norske

[1] Brasil, Russland, India, Kina og, enkelte ganger, Sør-Afrika.
[2] Lunde og Thune, 2013:43
[3] Lunde og Thune, 2013
[4] Lunde og Thune, 2013:67
[5] Leira, Halvard og Ole Jacob Sending, 2013
[6] Lunde og Thune, 2013
[7] Stortingsmelding 15 (2008-2009):20
[8] Lunde og Thune, 2013. Se kap. 2
[9] Se Leira og Sending, 2013

interesser bør fremmes i slike fora, samtidig som dette i seg selv kan bidra til å svekke global styring i for eksempel FN.[10]

Den vedvarende finanskrisen har rammet vesten kraftig, da kanskje aller tydeligst sør i Europa. Store redningspakker lanseres for å redde euro-samarbeidet, det snakkes om «den syke mannen Europa» og tilliten til unionen faller i flere land, da kanskje spesielt blant unge som rammes hardt av arbeidsledigheten.[11] Under en tale i Stortinget i februar 2013 gjorde daværende utenriksminister Espen Barth Eide det klart at finanskrisen nå er gått over i en arbeidsledighetskrise.

For Norges del innebærer dette at vi må se fremover og ta høyde for at flere stater, og regionale fora, utenfor vesten vil bli stadig viktigere samarbeidspartnere i årene som kommer.[12] USA er klar over det pågående skiftet og flytter sin oppmerksomhet fra landene på tvers av Atlanteren til de på den andre siden av Stillehavet. Utvikling innen petroleumsteknologi har gjort at USA er godt på vei mot å bli selvforsynt, noe som letter deres avhengighet av land i Midtøsten.[13]

2.2 Cyberdomenets fremtid

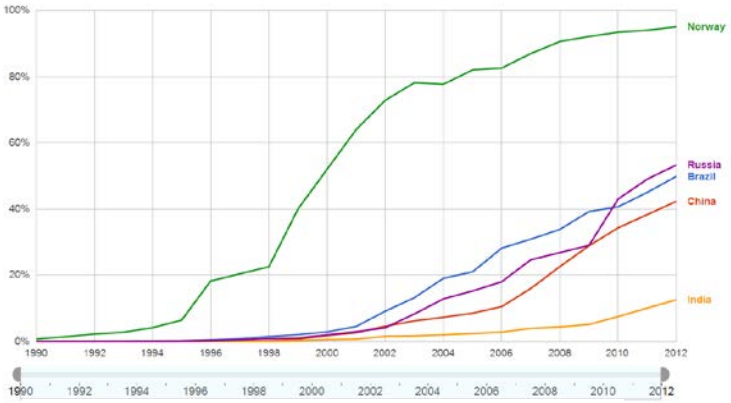
De såkalte «megatrendene» skissert så langt i dette kapittelet utgjør på mange måter grunnlaget for å vurdere hvordan Norge bør manøvrere det kommende politiske landskapet til fordel for egne interesser. En parallell til dette i cyberdomenet er utbredelsen av Internett. Det gjenstår her betydelig vekst, da spesielt i landene utenfor vesten. Antallet interessenter i domenet, hvilke interesser de har og hvor sterke disse interessene er vil derfor endre seg i årene som kommer. Det vil være nye brukermønstre fra privatpersoner, nye interesser fra næringsliv og ny politikk fra statene som søker å fremme sine interesser.

I 1991 var om lag 5 000 nettverk i tre dusin land koblet sammen i Internett og brukertallet var om lag 4 millioner mennesker.[14] I skrivende stund er om lag 40 prosent av verdens befolkning på Internett. Den internasjonale telekommunikasjonsunionen (ITU)[15] har som mål at 60 prosent av verdens befolkning skal være på Internett i løpet av 2015. Antallet enheter i nettverk passerte den globale populasjonen allerede i 2011, og kan passere en trillion innen 2025.[16] Figur 1 viser at vi i dag, etter 20 år med kommersielt Internett, er godt på vei mot 3 milliarder mennesker med Internettilgang. Internett er i dag den mest tydelige delen av cyberdomenet, en del vi i stadig flere land ikke kan se for oss en hverdag uten. Selv om man som privatperson skulle klare å isolere seg helt og holdent fra hele domenet er man fortsatt avhengig av tjenester som driftes av det.

[10] Leira og Sending, 2013 S 34
[11] Pew Research Global Attitudes Project, 2013
[12] Lunde og Thune (2013) kapittel 1 & Leira og Sending, 2013b
[13] Lunde og Thune, 2013:53
[14] Internet Society (1)
[15] ITU ble stiftet i Frankrike i 1865 i tiden hvor telegraflinjene begynte å knytte kontinentene sammen. ITU er nå en del av de Forente Nasjoner, og tar sikte på å koble sammen mennesker verden rundt blant annet med Internettilgang. ITU omtales videre i kapittelet om internasjonal organisering.
[16] ITU Broadband Commission, 2013

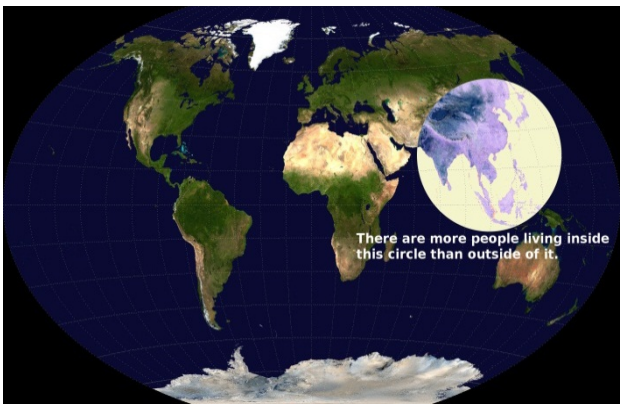
Figur 2.1 viser tall for utbredelsen av Internett i Norge og BRIK-landene i prosentandelen av populasjonen med tilgang. De fleste vestlige land følger en kurve lignende den norske. Ifølge ITUs Bredbåndskommisjon har i gjennomsnitt 77 prosent av husholdninger i europeiske land Internett, mot 61 prosent i Nord- og Sør-Amerika, 46 prosent i CIS[17], 34 prosent i Asia/Stillehavsregionen, 33 prosent i arabiske stater og til sist 7 prosent i Afrika.[18] Det går og frem av figur 2.1 at Russland, Brasil og Kinas utvikling er noen år på etterskudd sammenlignet med Norge, og at India ligger noe etter disse igjen.[19]

Figur 2.1 Prosentandel som bruker Internett



Kilde: ITU Public Data Explorer

Figur 2.2 Befolkningskonsentrasjon i øst



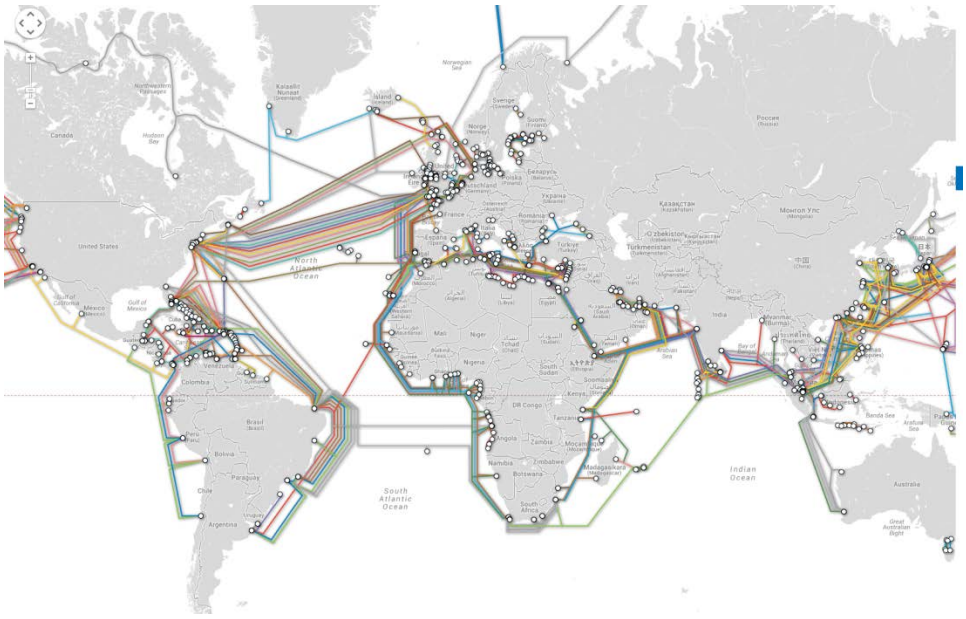
Kilde: The Washington Post

Vekstpotensialet i disse landene er kanskje ikke så ulikt mange andre stater i verden, men landene har bedre økonomiske forutsetninger for å øke utbredelsen kraftig i kommende år, og samtidig en stor befolkning og økt innflytelse i verdenspolitikken.

En av megatrendene som trekkes frem i Refleksprosjektet er de nye økonomiske stormaktene Brasil, Russland, India og Kina. Som figur 2.1 viser gjenstår det en betydelig utbygging i disse landene, og det er primært i ikke-vestlige land vi finner brorparten av fremtidens Internettbrukere. Spesielt vil mange brukere komme fra Asia. Figur 2.2 viser et kart hentet fra The Washington Post, og illustrerer noe av årsaken til dette. Om lag 3,6 milliarder mennesker bor innenfor sirkelen i figur 2.2 per i dag, altså flere enn utenfor.[20] I løpet av året vil det og være 2 milliarder brukere av mobilt bredbånd i verden, hvorav 895 millioner befinner seg i Asia-Stillehavsområdet.[21]

[17] Commonwealth of Independent States (CIS) består av Armenia, Azerbaijan, Hviterussland, Kazakhstan, Kirgisistan, Moldova, Russland, Tajikistan, Uzbekistan, Turkmenistan og Ukraina.
[18] ITU Broadband Commission, 2013:47
[19] ITU, 2013a
[20] Dewey, 2013
[21] ITU, 2013b

Siden bruk av domenet krever en betydelig produktbase, enten det er infrastruktur eller enhetene som bruker denne, har vestlige stater ligget foran i utviklingen. Dette reflekteres i den nåværende globale infrastrukturen som vist i form av sjøkabler i figur 2.3. Dette har gitt enkelte stater fordeler, for eksempel som knutepunkter med betydelig potensiale for etterretning. Dette bildet er ikke satt i sten, og stadig mer kapasitet vil bli nødvendig for å støtte fremtidens nye brukere og tjenester.



Kilde: TeleGeography (http://www.submarinecablemap.com/)

Figur 2.3 Sjøkabler med landingspunkter

Utbyggingen av cyberdomenet er langt fra ferdig. Etterhvert som flere stater får bedre økonomiske forutsetninger for å bygge ut i stor skala vil de mulighetene og truslene Norge står ovenfor i cyberdomenet også være i endring. Hva slags evne og interesse har disse statene av å bekjempe kriminalitet i cyberdomenet? Vil kriminell aktivitet være et like stort samfunnsproblem for disse statene som for vestlige stater? Hvordan vil disse regimene håndtere de nye mulighetene for informasjonsspredning blant egen befolkning? Hvordan vil disse statene forholde seg til militær cybermakt? Hva slags implikasjoner har nye trafikkmønstre og ny infrastruktur for cybermakt? Utviklingslinjene i cyberdomenet vil være viktige å følge med i årene som kommer slik at Norge igjennom utenrikspolitikken er best mulig forberedt på nye trusler og muligheter for norske interesser.

Med noen av cyberdomenets megatrender som bakteppe går rapporten videre til de norske interesseområdene slik inndelt i Refleksprosjektet. De kommende kapitlene vil omhandle sikkerhet, økonomi, energi, klima, miljø- og naturressurser, internasjonal organisering, engasjementspolitikk og identitet.

3 Sikkerhet

Refleksprosjektet[22] beskriver en samfunnsutvikling med tydelig økt oppmerksomhet på sikkerhet. Vi lever i "*risikosamfunnet*", hvor oppmerksomheten blant folk er rettet mot "*miljøsikkerhet, matvaresikkerhet, samfunnssikkerhet, atomsikkerhet, global sikkerhet, helsesikkerhet* […] *kollektiv sikkerhet, personlig sikkerhet etc.*" Cybersikkerhet føyer seg inn denne rekken og stadig flere stater lanserer strategier for å takle denne utfordringen. I dette kapittelet defineres sikkerhet som forhold som har med "*den norske statens evne til å beskytte norske statsborgere mot eksistensielle eller alvorlige trusler, ivareta grunnlaget for velferd, og ivareta statens styreform og territorielle integritet.*"[23]

3.1 Sikkerhetsbegrepet og sentrale aktører

I Norge deles ovenfornevnte sikkerhetsbegrep inn i statssikkerhet, samfunnssikkerhet, menneskelig sikkerhet og økonomisk trygghet. Statssikkerhet innebærer først og fremst ivaretagelsen av suverenitet, territoriell integritet og politisk handlefrihet. Dette er oppgaver som tradisjonelt sett tilfaller forsvarsstrukturen i en stat. Cyberforsvaret ble opprettet i august 2012, og i tillegg finner vi Nasjonal Sikkerhetsmyndighet (NSM) under Forsvarsdepartementet med ansvar for forebyggende sikkerhet i både militær og sivil sektor i henhold til sikkerhetsloven. NSM rapporterer derfor også til Justis- og beredskapsdepartementet.[24] NSMs avdeling for håndtering av alvorlige IKT-hendelser, NorCERT, har røtter tilbake til årtusenskiftet og ble offisielt opprettet i 2006.[25],[26]

Samfunnssikkerhet er det som ikke truer statens eksistens direkte, men truer befolkningens trygghetsfølelse samt viktige samfunnsinstitusjoner og infrastruktur. Begrepet har vokst frem spesielt i lys av ikke-statlige trusler i tiden etter den kalde krigen, men er like fullt noe som tilfaller politimyndighetene innad i en stat. Forsvaret kan stille kompetanse til disposisjon i henhold til bistandsinstruksen dersom politimyndighetene skulle finne det nødvendig i sin håndhevelse av samfunnssikkerhet.

Menneskelig sikkerhet omhandler enda mykere verdier som menneskerettigheter, rett til liv og personlig trygghet samt et trygt miljø trekkes frem som sentrale komponenter av menneskelig sikkerhet. Dette er verdier som ikke beskyttes aktivt av en myndighet, slik det gjøres med de to første sikkerhetsaspektene, men som grovt sett faller inn under statlige- og internasjonale rettsapparater. Datatilsynet og NorSIS er eksempler på viktige aktører som virker inn på dette nivået. Til sist trekkes Norges interesse av en økonomisk trygghet som tillater oss å videreføre velferdssamfunnet og livsmiljø frem.[27] De aller fleste økonomiske hensyn dekkes i denne rapporten under seksjonen for økonomiske interesser.

[22] Lunde og Thune m.fl., 2008:75
[23] Lunde og Thune m.fl., 2008:75
[24] NSM (1)
[25] NSM (2)
[26] St.meld. nr. 17 (2006-2007)
[27] St.meld. nr. 15 (2008-2009):89

3.2 Kort historikk

Stater har i lengre tid vært klar over at cyberdomenet har et maktpotensiale. Begrepet «informasjonskrigføring», i konteksten cyber, oppstod i USA allerede i 1976, og har siden vært under utvikling ved Pentagon.[28] Til tross for dette arbeider fortsatt de aller fleste stater med å forstå konseptet fullt ut og utvikle nasjonale strategier og doktriner som reflekterer dette. Her har det skjedd spesielt mye de siste 10 årene sammenlignet med foregående år, og enda mer de siste 5 årene. Tjenestenektangrepene mot Estland i 2007, cyberelementene under konflikten i Georgia i 2008 og Stuxnet-ormen som ble avslørt i 2010 kan betraktes som katalyserende hendelser som åpnet øynene for cybermakt hos langt flere stater. Samtidig er det en stødig strøm med avsløringer av mer avanserte etterretningsoperasjoner som høyst sannsynlig kun kan gjennomføres av stater. I 2013 alene har vi hatt flere slike avsløringer, i tillegg til Mandiant-rapporten som hevder å ha avslørt omfattende kinesisk spionasje og nå til sist Edward Snowdens lekkasjer primært om amerikansk og britisk etterretning.

Verden rundt finner vi derfor i dag nye strategidokumenter (spesielt utkom mange i 2011), Computer Emergency Response Team (CERTer)[29] eller lignende strukturer for håndtering av IKT-hendelser, nye samarbeidsorganer mellom myndigheter for å sikre informasjonsdeling og en felles situasjonsforståelse, og ikke minst tydelig økt utenrikspolitisk press for å komme blant annet cyberkriminalitet til livs. Kanskje spesielt de siste årene har cyberkriminalitet og spionasje havnet høyt opp på agendaen i internasjonal politikk.

I Norge reflekteres det økte fokuset på sikkerhet i cyberdomenet gjennom en ny strategi for IKT-sikkerhet i regi av Fornyings-, adminstrasjons- og kirkedepartementet (FAD), opprettelsen av NSMs NorCERT og Cyberforsvaret. Det opprettes også sektorvise sentre, CSIRTer, i justis- og helsesektorene. I privat sektor har finansnæringen gått sammen i et eget samarbeid kalt FinansCERT. Store banker og selskaper som Statoil og Telenor har håndterer cybertrusler gjennom egen organisering, prosesser, rutiner og teknologi.

3.3 Statssikkerhet

De viktigste norske sikkerhetsinteressene er knyttet opp i ivaretagelsen av den internasjonale rettsordenen og det multilaterale systemet, samt det norske samfunnets sikkerhet og territorielle integritet.[30] I sin drøfting av norsk statssikkerhet skriver Lunde og Thune at "Norge står i dag ikke overfor sannsynlige eksistensielle trusler, men globaliseringen betyr allikevel ikke at alle klassiske territorielle sikkerhetsutfordringer forsvinner, eller at tradisjonelle forsvarspolitiske tiltak mister relevans. Heri inngår blant annet fremtidig ressurskonkurranse, økt strategisk betydning av Nordområdene og Norges asymmetriske forhold til Russland."[31]

[28] Langø, Hans-Inge, 2013
[29] Computer Emergency Response Team (CERT) er en vanlig benevnelse for slike sentre. CERT-begrepet lisensieres av Carnegie Mellon Universitet i USA, hvor den første CERT i verden ble opprettet. Ofte benyttes derfor begrepet Computer Incident Response Team (CSIRT).
[30] Lunde og Thune m.fl., 2008:75
[31] Lunde og Thune m.fl., 2008:75

Innen land-, luft-, sjø-, og romdomenene tar Forsvaret stadig i bruk ny informasjonsteknologi. I det nettverksbaserte forsvaret vil for eksempel informasjonsteknologi bidra til økt operasjonsevne ved å knytte sammen «sensorer, våpen og plattformer uavhengig av forsvarsgren og våpenart».[32] Stadig flere systemer skal knyttes sammen i nettverk, og snakke med hverandre for å gi Forsvaret økt operativ evne. Dette *gjør cyberdomenet til en tilrettelegger for maktutøvelse i de øvrige domenene*, og dermed er det spesielt viktig å kunne stole på at disse systemene. Forsvarets evne til å sikre integritet i egne systemer er i så måte høyst relevant for norsk statssikkerhet.

Samtlige land med grenser i nord har satt inn ressurser for å kunne nytte cyberdomenet militært. To stater som har kanskje spesielt gode forutsetninger for cybermakt er USA og Russland. Siden etableringen i 2009 har amerikanske US CYBERCOM økt bemanningen fra 900 til 5000. Det er og foretatt en tredeling hvor en gruppe har ansvar for kontraoffensiver og forstyrrelse av angrep mot kritisk infrastruktur i privat sektor (kraftstasjoner og strømnett), en andre planlegging av offensive cyberoperasjoner i utenlandsoperasjoner og en tredje beskyttelse av forsvarsdepartementets systemer.[33] Det vi i Norge omtaler som cyberkrigføring er i russiske og kinesiske øyne en del av informasjonskrigføring.[34] I august 2013 har imidlertid Russland også vedtatt å etablere en egen avdeling for *cyber*krigføring og anser Internett som et mulig stridsdomene.[35] Dette signaliserer et klart skifte fra tidligere ordelag fra russisk side.

Trusler mot norsk territoriell integritet kan ikke komme i eller igjennom cyberdomenet alene, men krever tilstedeværelse av konvensjonelle styrker. Cybermakt vil kunne benyttes i en slik kontekst, men motparten vil måtte ta inn over seg de øvrige sikkerhetspolitiske forholdene – slik som Norges Nato-medlemskap. Norges asymmetriske forhold til Russland består også i cyberdomenet da avanserte offensive cyberoperasjoner er svært krevende.

Som tidligere nevnt er de fleste stater i startgropen med å organisere cybersikkerhet internt og samhandle med andre stater for å fremme egne interesser i cyberdomenet. Dette betyr også at det er gode muligheter for å etablere nye samarbeider og utveksle erfaringer med likesinnede stater. Ifølge Stortingsmelding 15 (2008-2009) er de nordiske landene «Norges nærmeste partnere i internasjonal politikk, blant annet i FN og i nordområdene».[36]

Vi kommer tilbake til forsvarssamarbeidet i kapittelet om internasjonal organisering. Mer direkte relatert til norsk sikkerhet er det slik at Internett har en fysisk infrastruktur som kan bidra til å styrke vår evne til å avverge angrep og takle hendelser. For å avsløre ondsinnede handlinger i cyberdomenet er man blant annet avhengig av sensorer som overvåker og avslører unormal nettverkstrafikk. NSMs NorCERT, med sitt Varslingssystem for Digital Infrastruktur (VDI), skal håndtere alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.[37] Samtidig føres om lag 80 prosent av all Internettrafikk ut og inn av Norge igjennom Sverige og kan dermed

[32] Forsvaret (1)
[33] Atlanterhavsrådet (1)
[34] Atlanterhavsrådet (1)
[35] Atlanterhavsrådet (2)
[36] Stortingsmelding 15 (2008-2009):98
[37] NSM (3)

fanges opp av pakkeinspeksjonssystemet til Försvarets Radioanstalt (FRA). Sverige er og i ferd med å utvikle et mer omfattende pakkeinspeksjonssystem som skal overvåke all trafikk som krysser Sveriges grenser.[38] Det faller derfor naturlig å samarbeide med nabostaten for å oppdage ondsinnet programvare rettet også mot norske mål.

3.3.1 Nordområdene

Nordområdene har gått fra å være et militærstrategisk område i en verdensomspennende kald krig til et område med stor strategisk verdi i form av ressurser og nye transportruter. Befolkningsvekst og ressurskonkurranse i fremtiden gjør olje-, gass-, og fiskeressurser til enda mer tydelige norske interesser. Området er også viktig med tanke på forskning, blant annet på global oppvarming, noe som illustreres ved at kunnskap om, for og i nordområdene er det første av 15 nåværende overordnede strategiske prioriteringer.[39] Siden Stortingsmelding 15 (2008-2009) kom ut har norske og russiske myndigheter kommet til enighet om grenseoppgang i den såkalte delelinjeavtalen. Etterretnings- og sikkerhetstjenestene trekker frem i sine trusselvurderinger fra 2013 at det er sjøruter, og ikke ressurser, i Nordområdene som først og fremst innehar et potensiale for fremtidig konflikt.[40]

De nåværende grensedisputtene mellom andre aktører i Nordområdene omhandler først og fremst retten på det som per i dag er internasjonalt farvann i Arktis. Lemonosovryggen, en undersjøisk fjellkjede som strekker seg fra Canada og Grønland til Russland via Nordpolen. Dette er imidlertid en pågående prosess hvor Russland har levert sine krav allerede i 2001 og ventes å komme med utfyllende informasjon, Danmark ventes å gjøre krav på store områder i 2014 og Canada vil levere sine vurderinger i november 2013. Grønland er i tillegg rikt på såkalt "rare earth elements", stoffer som er viktige for blant annet forsvarsteknologi. Smeltingen av Grønlandsisen tiltrekker seg også oppmerksomhet med tanke på gruvedrift, også fra Kina som har tilnærmet monopol på utvinning av rare earth elements.[41]

FFIs sjømaktrapport viser for eksempel til at norsk sjømakt beskytter, ivaretar og fremmer norske interesser i Nordområdene blant annet gjennom å håndheve norsk jurisdiksjon og suverenitet og avskrekke potensielle motparter fra bruk av militærmakt.[42] Utførelsen av disse oppgavene i de store havområdene i årene fremover beror på teknologi en sofistikert motpart kan søke å manipulere gjennom cyberdomenet. Et eksempel på dette er satellitten AISSat-1, utviklet ved FFI, som bistår med å spore og organisere skipstrafikk i Nordområdene.[43] AISSat-1, og kommende AISSat-2, gir en oversikt over skipstrafikken ved hjelp av skipenes automatiske identifikasjonssystemer (AIS) som nå er påkrevet av den internasjonale skipsfartsorganisasjonen. Sikkerhetsselskapet Trend Micro har demonstrert hvordan dette systemet forholdsvis enkelt kan utnyttes gjennom cyberdomenet. Selskapet kunne flytte, lage eller modifisere båter i systemet.[44]

[38] Jørgenrud, 2013
[39] Utenriksdepartementet (1)
[40] Forsvarets Etterretningstjeneste, 2013
[41] Se for eksempel Matlock, 2013
[42] Børresen og Helseth, 2011:13-15
[43] FFI (1)
[44] Arnsdorf, 2013

3.3.2 Internasjonal rett

Lunde og Thune skriver blant annet at «Den viktigste fremtidige enkelttrusselen mot det norske samfunnets sikkerhet og territorielle integritet, er en erosjon av dagens internasjonale rettsorden og multilaterale system.»[45] Norge holder fast ved at folkeretten er tilstrekkelig dekkende også for hendelser i cyberdomenet[46], og her slås det fast at væpnet makt kan benyttes dersom Sikkerhetsrådet anser det som nødvendig for å bevare internasjonal fred og sikkerhet eller som forsvar mot et angrep fra et annet land.[47] Allikevel er det viktig å erkjenne at folkeretten så langt ikke er benyttet i forbindelse med en hendelse i cyberdomenet, og at det pågår utredninger, slik som Tallinn-manualen[48], som søker å forstå hvordan eksisterende lover og normer for konflikt passer sammen med det nye stridsdomenet.

Tallinn-manualen utkommer på bakgrunn av tjenestenektangrepene mot Estland i 2007, som ikke ble ansett som et angrep i henhold til folkeretten eller utløste Natos artikkel 5. Tjenestenektangrepet mot Estland ble aldri direkte attribuert[49] til russiske myndigheter, noe som enten antyder at de ikke stod bak eller illustrerer utfordringene knyttet til å fremskaffe ugjendrivelig bevis på at angrepet faktisk har et statlig opphav i cyberdomenet. Dersom Russland stod bak angrepet opplevde Estland i 2007 at det eksisterte et handlingsrom for å øve en form for politisk press mellom stater utenfor aksepterte kanaler hvor det var utfordrende å rettferdiggjøre respons. Både attribusjon, situasjon, konsekvenser og angrepsform og usikkerhet er eksempler på faktorer som kan ha bidratt til disse utfordringene. Antagelig vil denne typen handlingsrom, dersom flere eksisterer, lukkes gjennom internasjonal debatt om oppførsel i cyberdomenet og eventuelle nye erfaringer.

3.4 Trusler via ekstern ustabilitet

Refleksprosjektet introduserer begrepet trusler via ekstern ustabilitet, et begrep som innebærer at «trusler og forhold langt borte kan ha betydelig direkte og negativ innvirkning på den økonomiske, sosiale, politiske og økologiske situasjonen i Norge.»[50] Krig i Midtøsten vil øke den strategiske betydningen av norsk olje og gass samt Nordområdene dersom Hormuz-stredet stenges eller prisen på minne til datamaskiner vil gå opp ved uro i Taiwan og Korea. Oljeprisene og markeder reagerer på vestens vurderinger om militært svar på bruken av kjemiske våpen i den pågående borgerkrigen i Syria.[51] Forsvarssjef Harald Sunde og daværende landbruks- og matminister Trygve Slagsvold Vedum understreket i 2013 sårbarheten for ekstern ustabilitet.

[45] Lunde og Thune m.fl., 2008:75
[46] Utenriksdepartementet, 2013
[47] FN (5)
[48] Tilgjengelig på http://www.ccdcoe.org/
[49] Med attribusjon menes her å kunne fremstille ugjendrivelige bevis på at en spesifikk aktør står bak en handling. Attribusjon er en kjent problematikk i cyberdomenet. For eksempel er det både er tekniske utfordringer knyttet til å spore seg frem til opprinnelsen av en ondsinnet handling i cyberdomenet, og ytterligere utfordringer knyttet til å vite hvem som satt bak maskinen når angrepet ble utført og eventuelt hvem vedkommende handlet på vegne av.
[50] Lunde og Thune m.fl., 2008:81
[51] BBC, 2013a

Norge har gjennom å være helt avhengige av kornimport.[52] Disse punktene har alle til felles at forsyningskjeden strekker seg på tvers av landegrenser og kontinenter, et kjennetegn ved en globalisert verdensøkonomi. Dette gjelder også for andre land ovenfor Norge. I 2013 førte et strømbrudd til en reduksjon av gasseksporten ved Ormen Lange, slik at gassprisene doblet seg i Storbritannia.[53]

Cyberdomenet er en global forsyningskjede av informasjon som inngår i en rekke samfunnsstrukturer vi anser for å være kritiske. Chatham House' Dave Clemente visualiserer cyberdomenet som et 'tynt lag som trenger gjennom alle sektorer', eller som et slags nervesystem, som knytter sektorene sammen slik at de kan fungere hver for seg og sammen.[54] Denne logikken gjelder på tvers av landegrenser, og cyberdomenet er tilrettelegger på så mange ulike måter at listen over det som er kritisk blir stor og uhåndterlig. Clemente bemerker i denne sammenhengen at 'når alt er kritisk, er ingenting kritisk'.[55]

Viktige forsyningskjeder i cyberdomenet er dermed sårbare både rent fysisk i infrastrukturen og logisk. Sikringstiltak i systemene, kompetanse, nasjonalt lovverk samt evne og prioritering av cybersikkerhet er eksempler på faktorer som varierer fra land til land. Norge kan dermed befinne seg i en situasjon hvor deler av informasjonsinfrastrukturen vi er avhengige av ikke er underlagt sikkerhetsrutiner vi anser som tilstrekkelige. Vi har opplevd dette på nasjonalt nivå for eksempel gjennom bortfall av minibanktjenester som følge av tekniske feil hos tjenesteleverandøren Evry. Norske banktjenester ble driftet fra Ukraina en kort periode, før den ble flyttet tilbake til Norge etter bekymringsmeldinger fra Datatilsynet og Finanstilsynet.[56]

For Norges del kan en sentral utfordring være å identifisere de mest kritiske avhengighetene vi har i utlandet som kan påvirkes av ekstern ustabilitet. Dette gjelder både datasystemer og tjenester som er avhengige av cyberdomenet. Selv om det er en gjennomgående norsk interesse å fremme et trygt og åpent Internett generelt, vil en slik liste også kunne bidra til å prioritere ressursbruk og samarbeidspartnere i våre bi- og multilaterale samarbeid for å bedre cybersikkerhet.

3.5 Sub-nasjonale aktører

I Refleksprosjektets første bok skriver Lunde og Thune at "Svært mange steder i verden vil mange ikke se noen avgjørende forskjell mellom Norge som stat og norske selskaper og næringsinteresser. Det er derfor et toveis forhold mellom det offentlige og det sivile Norge i verden. I utenrikspolitikken vil det private og det offentlige Norge bli stående ansvarlig for hverandres opptreden."[57] Dette er bakgrunnen for trusler mot norske liv og interesser i utlandet, slik vi har sett i Karikaturstriden, brenningen av den norske ambassaden i Syria og nå senest terrorangrepet mot Statoil i In Amenas i Algerie.

[52] Sunde og Vedum, 2013
[53] Lie, 2013
[54] Clemente, 2013:1
[55] Clemente, 2013:V
[56] NTB, 2010 & Zachariassen, 2011
[57] Lunde og Thune m.fl., 2008:84

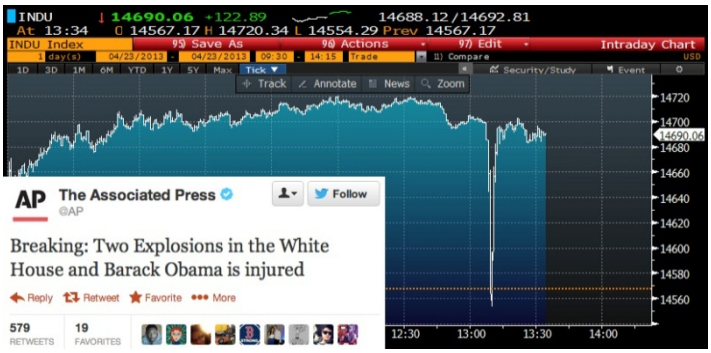
I 2013 er Lunde og Thune enda tydeligere, og beskriver bevegelser som oppstår direkte fra befolkningen og gjør seg gjeldene i politikken i en slik grad at de ikke kan ignoreres eller ventes å forsvinne. Al-Qaeda er det mest kjente eksempelet på den «statløse» politikken, men ett avsnitt spesielt understreker spekteret av interesser man nå må forholde seg til i utenrikspolitikken.:
«…sosiale bevegelser på gaten i Hviterussland og Libanon; YouTube opprør mot regimet i Teheran; nettstedet WikiLeaks massepubliseringer av fortrolige diplomatiske notater; hackernettverket Anonymous; opprørsgrupper og krigsherrer i statsløse områder av Afrika; og til slutt den spontane bølgen av opprør i den arabiske verden, okkupantene av Wall Street og Tea Party-bevegelsen, som alle er krysninger av gamle sosiale grasrotbevegelser og digitale nettsamfunn.»[58]

I vesten er Internett nå den primære informasjonsbæreren og dette vil være tilfelle for stadig større deler av verden i årene som kommer. Akkurat som stater søker å fremstille sin posisjon fordelaktig i medier, enten det er klandestint eller åpenlyst, i konflikt eller utenfor, har nå stadig flere ikke-statlige aktører langt bedre muligheter enn tidligere til å gjøre det samme. I foregående rapport konkluderte prosjektet blant annet med at sub-nasjonale aktører antagelig ikke evner å utføre avanserte cyberoperasjoner. Den britiske forskeren Thomas Rid ved Kings College hevder at det primært er terskelen for deltagelse som er senket for sub-nasjonale aktører i cyberdomenet, samtidig som mulighetene for å gjøre alvorlig skade fortsatt er forbeholdt langt mer sofistikerte aktører.[59] De hendelsene som har inntruffet så langt passer godt overens med dette.

I cyberdomenet har vi sett eksempler på at sub-nasjonale aktører aktivt responderer på hendelser, enten de er mellom stater eller innad i egen- eller andre stater, på både egne og andres vegne – og ikke nødvendigvis i henhold til statens interesse. Begrepet «patriothackere» benyttes om de som utfører ulovlige handlinger i cyberdomenet på vegne av eller for å støtte sin egen stat. Kinesiske patriothackere aksjonerte i etterkant av bombingen av den kinesiske ambassaden i Beograd i 1999 og etter en kollisjon mellom et amerikansk og kinesisk militærfly i 2001. [60] I 1999 hadde kinesiske og taiwanske hackere en egen «hacker-krig»[61]. Patriothackere er representert i en rekke konflikter og spente situasjoner, enten det er mellom Israel og Palestina, India og Pakistan, Russland og Estland/Georgia/Kazakhstan, Sør-Korea og Nord-Korea/USA.

[58] Lunde og Thune m.fl., 2013:91
[59] Rid, Thomas (2013) Cyber War Will Not Take Place.
[60] Rattray og Healey, 2011
[61] Jame, 1999

I konflikten i Syria er det hackere på både regime- og opprørssiden. Spesielt har gruppen Syrian Electronic Army (SEA) tiltrukket seg betydelig medieoppmerksomhet gjennom sine aksjoner rettet primært mot det de oppfatter som Assad-fiendtlige nyhetsmedier. I april 2013 meldte gruppen at President Barack Obama var blitt skadet i en eksplosjon i det hvite hus på Twitter-kontoen til nyhetsbyrået Associated Press. Meldingen forårsaket et *midlertidig* fall i New York børsen på 136 milliarder dollar.[62]



Kilde: The Washington Post

Figur 3.1 Twitter-melding og midlertidig børsfall

Fra et statsvitenskapelig synspunkt er SEA et ekstra interessant tilfelle som en borgerkrigsaktør som påtar seg ansvaret for åpenlys og tidvis kriminell spredning av regimefavoriserende informasjon også utenfor konfliktsonen i eller gjennom cyberdomenet. Borgerkrigen i seg selv er den første med utpregede cyberelementer. Regimet har ved flere anledninger kuttet Internettrafikken til og fra landet, SEA hacker primært vestlige medier og plasserer ut bilder og tekst til inntekt for Assads regime samtidig som de deler informasjonen de samler underveis inn med regimet, the Pirates of Aleppo går aktivt inn for å endre potensielt farlig informasjon[63] i sosiale medier for opprørere som er arrestert[64], og den kanskje sterkeste opprørsaktøren Harakat Ahrar al-Sham al-Islamiya (HASI) etablerte nylig en egen «teknisk divisjon» for å slå tilbake på nettsider affiliert med SEA.[65] Eksterne grupper tar del i konflikten gjennom cyberdomenet, slik som for eksempel Anonymous som søker å ramme både den syriske staten og Saudi-Arabia for å ha støttet opp under den.[66]

Siden mål kan rammes gjennom cyberdomenet uten at angriperen forflytter seg til målområdet fysisk, introduserer cyberdomenet nye kontaktflater mellom Norge, norske virksomheter og omverdenen. Et eksempel det siste året er gruppen Izz ad-Din Al-Qassam Cyber Fighters' «Operasjon Ababil». Operasjon Ababil er en serie omfattende tjenestenektangrep mot amerikanske banker som har pågått i 5 faser siden høsten 2012. Angrepene har hatt betydelige konsekvenser for amerikanske banker, selv om angrepene ikke har vært av katastrofalt omfang. Angrepene kommer som svar på filmen «Innocence of Muslims», en filmsnutt laget av en amerikansk privatperson som oppfattes som fornærmende mot Islam av gruppen. Amerikanske banker, og ikke privatpersonen, angripes som representant for den amerikanske staten. Gruppen krever at amerikanske myndigheter skal fjerne filmen fra videodelingsstedet YouTube, noe som strider i mot grunnleggende amerikanske verdier.

[62] Fisher, 2013
[63] Ifølge gruppen selv ville forhørene kun vare i noen timer dersom regimekritisk informasjon på Facebook og blogger ble erstattet med pornografi.
[64] Shelton, 2013
[65] Zelin og Lister, 2013
[66] Anonymous (1)

Sub-nasjonale aktører tilbyr naturligvis også et potensielt skalkeskjul for bakenforliggende aktører, slik at for eksempel stater kan benytte seg av dem som *proxy* for angrep de ikke ønsker å gjøre åpenlyst eller for å skjule seg i mengden. Ifølge seniorforsker James A. Lewis ved CSIS hersker det liten tvil om at Iran i realiteten står bak Operasjon Ababil.[67] Flere har trukket lignende konklusjoner om hendelsene i Georgia og Estland. Om man følger proxylogikken fullt ut, kan det tenkes at Anonymous utgjør det perfekte skalkeskjulet for slike operasjoner. Ikke-organisasjonen eksisterer allerede i en rekke ulike, og til dels motstridende, kapitler verden rundt. De har et renommé for å engasjere seg verden rundt i både kjente og obskure emner og har ikke behov for sentral organisering for å mobiliseres. I teorien kan en slik organisasjon også utnyttes av en statlig aktør, enten bare i navnet eller ved å motivere segmenter av gruppen til nye operasjoner.

Cyberdomenet muliggjør samarbeid på ad-hoc basis mellom grupper vi tidligere ville anse som usannsynlige. Ett slikt eksempel er OpBlackSummer, en aksjon planlagt mot amerikanske mål. Blant de påmeldte gruppene fant man for eksempel an gruppe fra Gaza-stripen (FoxySec), «Anons» fra Anonymous, Electronic Army of al-Qaeda, Tunisian Cyber Fighters og en gruppe kinesiske hackere uten kjent navn.[68]

Siden 2010 har Norge hatt et bilateralt forsvarssamarbeid med Georgia som inkluderer blant annet utveksling av offiserer, bistand til det georgiske heimevernet og øvelsessamarbeid.[69],[70] Konflikten mellom georgiske myndigheter og de to gjenværende utbryterregionene Sør-Ossetia og Abkhasia, og de sterke russiske interessene i området, har sine røtter tilbake til sent 1700-tall.[71] Påtroppende president Georgy Margvelashvili legger opp til å ha et godt forhold til både Russland og vesten, og fortsette det georgiske arbeidet mot Nato og EU-medlemskap.[72],[73] Gjenopprettelsen av georgisk territoriell integritet er imidlertid også et mål, og dermed er det liten endring i den underliggende frosne konflikten i regionen.[74] Dette er ett av de nåværende norske engasjementene som potensielt kan bringe Norge i kontakt med patriothackere i fremtiden. Da konflikten sist blusset opp i 2008 var det cyberelementer i kombinasjon med konvensjonelle militæroperasjoner. En av diskusjonene i etterkant har gått på i hvilken grad et sjikte av patriothackerne handlet selvstendig, på vegne av russiske myndigheter – eller i realiteten var russiske myndigheter.[75] Hendelsene illustrerer hvordan statlig aktivitet i cyberdomenet kan være vanskelig å skille fra ikke-statlig aktivitet, og hvordan stater kan tenkes å skape eller benytte seg av et eksisterende ikke-statlig cyberelement i en konflikt.

[67] Perlroth og Hardy, 2013
[68] RT, 2013
[69] Forsvarsdepartementet (1)
[70] Georgia er et lappeteppe av etniske minoriteter, og det gjenstår å se om uroligheter vil oppstå i andre regioner av landet dersom det settes en presedens for å la utbryterregioner gå sin egen vei. Russisk støtte til regionene er sannsynligvis avgjørende for dette. Adjar-provinsen, som ligger nede ved grensen mot Tyrkia, ble tatt inn under Georgisk kontroll igjen kort tid etter Roserevolusjonen i 2004 uten lignende problemer.
[71] Se Ronald Grigor Suny (1994) *The Making of the Georgian Nation*. Indiana University Press, 2nd ed.
[72] AFP, 2013
[73] Antidze og Heritage, 2013
[74] Caucasus Elections Watch, 2013
[75] Se for eksempel Leyden, 2009

Sub-nasjonale aktører er altså i høyeste grad aktive i cyberdomenet, og domenet senker listen for deltagelse samt muliggjør nye samarbeids- og aksjonsformer med hurtig dynamikk. Forsvaret, men også næringsliv og offentlig sektor for øvrig, bør påregne å støte på slike aktører i årene som kommer, kanskje spesielt når vi involverer oss i konflikter hvor slike cyberelementer allerede eksisterer.

Siden både trusselbildet og aktørenes rekkevidde er globale kan opphavet for slike angrep se ut til å være i konfliktsonen, men i realiteten komme utenfra og vice versa. I tillegg kan opphavet være en motpart som ikke er direkte involvert i konflikten, eller eventuelt en ikke-statlig aktør. Dersom det skulle være behov for, eller ønskelig, å «hacke tilbake» når man blir angrepet i cyberdomenet er dette kompliserende faktorer. Det kan være vanskelig å vite om motparten er en gruppe eller en stat. I tillegg kommer utfordringene med å vite hva slags konsekvenser et eventuelt motangrep kan ha, spesielt når man rammer sivil infrastruktur. Den amerikanske tenketanken CNAS tar for eksempel til orde for et «aktivt forsvar».[76] Ifølge Martin Libicki er et sentralt problem med denne typen tenkning at motparten vil forvente dette, og skjule seg i mål det ikke er akseptabelt å ramme.[77] Dette kan for eksempel være sykehus, religiøse bygg eller barnehjem.

3.6 Overvåkning i cyberdomenet

For å forsøke å skille spionasje med kommersielle formål fra spionasje i sikkerhetshenseende, omtales industrispionasje i økonomikapittelet. Disse overlapper når det kommer til spionasje rettet mot forsvarsindustri med både det formål å stjele teknologi og skaffe seg kunnskap om motpartens systemer. Det understrekes derfor her at tyveri av intellektuell eiendom rettet mot både Forsvaret og forsvarets leverandører, som for eksempel kildekoden til systemer i Forsvarets nye kampfly, kan ha alvorlige sikkerhetsimplikasjoner.

Krigen mot terror stiller store krav til innhenting av informasjon om både vårt eget samfunn og omverdenen. Siden 9/11 har bare informasjon om individer og grupper blitt langt mer viktig samtidig som cyberdomenet vokst og utviklet seg til å bli et komplekst og viktig medium for kommunikasjon og organisering av terroraktivitet. I Stortingsmelding 15 (2008-2009) vises det til at… *«Verken Norge eller andre land har noen garanti mot å bli rammet av alvorlige terroraksjoner. Høy kvalitet på nasjonal etterretning er essensielt i lys av dette. Det samme gjelder betydningen av effektiv informasjons- og erfaringsutveksling internasjonalt. Samtidig innebærer anti-terrorarbeidet viktige avveininger og mulige dilemmaer som vi deler med andre land. Blant annet handler det om hvor grensene går mellom legitime overvåkingsbehov og enkeltmenneskets rettssikkerhet.»*[78]

Om ikke sitatet er en direkte henvisning til cyberdomenet, er det høyst relevant. Utviklingen av alt fra nye tjenester og brukermønstre til krypteringsalgoritmer og anonymiseringsverktøy presenterer nye utfordringer med å nå frem til informasjonen man har behov for også mot ikke-statlige trusler. Både mengde og detaljnivå på informasjonen vi legger ut på Internett øker stadig.

[76] Center for a New American Security, 2013
[77] Libicki, 2009
[78] St.meld. nr. 15 (2008-2009):24

Etterhvert som cyberdomenet i økende grad blir en arena for flere aspekter av menneskelivet, fra sosialliv til handel og eGovernance, endres implikasjonene av overvåking. Dette presenterer nye dilemmaer mellom legitime overvåkingsbehov og enkeltmenneskets rettssikkerhet, slik sitatet over viser til.

Noen av disse avveiningene og mulige dilemmaene har vi fått langt mer kjennskap til etter at tidligere Booz Allen Hamilton-ansatt Edward Snowden tok med seg tusenvis av graderte dokumenter, primært fra amerikanske NSA og britiske GCHQ, og rømte landet. Nye dokumenter kommer i skrivende stund ut med noen ukers mellomrom, og noen av avsløringene benyttes her til å belyse utfordringene stortingsmeldingen påpeker. Det understrekes i denne sammenheng at man kan stille spørsmål til dokumentenes rettskaffenhet, journalistenes tolkning av innholdet og ikke minst den bredere konteksten de passer inn. FFI tar ikke til Snowden eller USAs handlinger, eller nøyaktig hvor balansen mellom «legitime overvåkingsbehov og enkeltmenneskets rettssikkerhet» bør ligge. Snarere understreker vi her at avsløringene antagelig burde tas som eksempler på hvordan avanserte stater, da spesielt de med det fortrinnet å ha flere store globale tjenestetilbydere og knutepunkter for kommunikasjon på egen jord, kan søke å øke og utøve egen cybermakt i verden.

3.6.1 Forsyningskjeder

En stor del av avsløringene omhandler programmer som siler nettverkstrafikk på Internett i knutepunkter verden rundt for informasjon med potensiell etterretningsverdi, da primært i kampen mot terrorisme. Automatiserte systemer går gjennom en ukjent andel av den totale trafikken, samler inn interessant informasjon basert på selektorer[79] gitt av NSA/GCHQ, prosesserer dataene videre og lagrer de i en database. Databasene sees først av mennesker idet analytikere rettferdiggjør et behov for innsyn i denne. Et helt sentralt spørsmål er hvilke juridiske rammer det er for innsyn og bruk av opplysninger.

For det første er programmene realisert til dels gjennom samarbeider med private aktører. Microsoft, Yahoo!, Facebook og Apple er eksempler på noen av vår tids største aktører innen teknologiutvikling og tjenester med global kundebase, som alle har blitt tvunget til stilltiende aksept av samarbeid med NSA gjennom amerikansk lovgivning. Dette er et godt eksempel på hvordan nasjonal lovgivning kan benyttes til å fremme egen cybermakt ovenfor resten av verden. Ett annet mulig eksempel på kraften nasjonal lovgivning kan ha her er videochat-tjenesten Skype. Tjenesten ble kjøpt opp av Microsoft, men har fortsatt hovedkontor i Luxembourg. Luxembourg har nå iverksatt etterforskning av tjenesten som øyensynlig har inngått lignende samarbeidsavtaler med NSA som øvrige amerikanske virksomheter.[80] Andre dokumenter viser til at NSA bruker 250 millioner dollar i året på enten åpenlyst eller klandestint å påvirke både nasjonal og utenlandske kommersielle IT-produkter for å gjøre det mulig å utnytte disse.

[79] For eksempel nøkkelord eller trafikk til personer av interesse
[80] Gallagher, 2013

Dette inkluderer påvirkning av kommersielle krypteringsverktøy for å gjøre dem *enklere*[81] å knekke for de med kjennskap til sårbarheten.[82]

Selv om vi vanskelig kan vente å erstatte flertallet av tjenester vi er avhengige av i cyberdomenet, er det områder Norge allerede er godt etablerte på som kan være satsningsområder. Ifølge sjef for Forsvarsdepartementets avdeling for sikkerhetspolitikk og langtidsplanlegging, kontreadmiral Elisabeth Natvig, er den nasjonale kryptoindustrien ett område hvor Norge ligger i front av utviklingen.[83] Slik kunnskap kan i tillegg vise seg å være verdifull for norske borgere og næringslivet som i økende grad oppbevarer sensitiv informasjon i cyberdomenet. Forsvaret benytter i økende grad kommersielle teknologier[84], og disse avsløringene understreker viktigheten i å sørge for sikkerhet så vel som anvendbarhet i anskaffelsene.

Overvåkingen innebærer potensielt at norske personopplysninger lagres i databaser i andre land. Dette er ikke nødvendigvis noe nytt, dog både detaljnivå og omfang *kan* være større enn tidligere fordi vi frivillig deler mer og mer informasjon om oss selv på Internett. NSMs Roar Thon skrev kort tid etter PRISM-avsløringene at noen av reaksjonene i Norge var «et godt eksempel på vår kollektive nasjonale naivitet».[85] Datatilsynet ønsket blant annet informasjon om hva slags informasjon som faktisk var samlet inn, hvor sikkert de ble oppbevart og hvem som hadde tilgang.[86] Justisminister Grete Faremo møtte den amerikanske ambassadøren, og en norsk delegasjon møtte myndighetene i USA og fikk forsikringer om at norske borgere ikke ble urettmessig overvåket gjennom PRISM-programmet, og at USA forholdt seg til Wien-konvensjonen som blant annet skal sikre norske diplomatiske stasjoner fra overvåking.[87] Ifølge Roar Thon er det viktig at brukerne forstår at det er utenlandske tjenester vi benytter oss av, og at disse ikke er gratis selv om de ikke koster penger. Avslutningsvis i sin bloggpost om PRISM skriver han «Informasjon som er på nett er allerede på avvei. Oppfør deg deretter!».[88] Et mulig spørsmål for fremtiden er hvordan stater Norge har et mindre godt forhold til vil forvalte informasjonen i lignende systemer, kanskje med andre lagringskriterier og sikkerhetsrutiner?

Innføringen av Datalagringsdirektivet vil føre til noen av de samme sikkerhetsutfordringene for metadata[89] om norske personer. Direktivet er ikke implementert, men ifølge Datatilsynet vil det være vanskelig å unngå at norske personopplysninger fritt vil bevege seg i EØS-området.

---

[81] Kryptering bygger på generering av tilfeldige tallrekker. Tallgeneratorene er igjen avhengige av startverdier å generere tilfeldige tall fra, derav tilnavnet pseudo-generatorer. Ved å påvirke disse tallrekkene kan man redusere kompleksiteten i en krypteringsalgoritme og gjøre den enklere å knekke.
[82] Menn, 2013
[83] Natvig, Elisabeth (2013) Cybermaktseminar ved FFI 09.10.2013
[84] Eggen, Anders (2013) Foredrag i Oslo Militære Samfund oktober 2013.
[85] Thon, 2013
[86] Datatilsynet (BREV)
[87] Færås, 2013
[88] Thon, 2013
[89] Store Norske Leksikon definerer metadata som "data om data, informasjon som beskriver annen informasjon". I denne konteksten viser metadata først og fremst til de data som lages ved bruk av cyberdomenet. Eksempler på dette er lokasjonsdata fra mobiltelefoners GPS, lister over hvilke nummer som ringes med telefonen og hvor lenge samtalen varer, hvilke sider som besøkes med en datamaskin, IP-adresse og lignende.

I den anledning uttrykker tilsynet en bekymring over at mottakerlandet, selv med tilfredsstillende regelverk, ikke vil gi tilfredsstillende norsk kontroll med opplysningene.[90] Sentrale utfordringer her er både fremmede etterretningstjenester, politiske endringer eller nye eiere av virksomheter som lagrer opplysningene. Til forskjell fra PRISM-programmet vil Datalagringsdirektivet innebære 6 måneders lagring av utvalgte metadata.

3.6.2 Større utfordringer for telekomselskaper

En av presentasjonene lekket av Snowden viser til at GCHQ har gjennomført en etterretningsoperasjon mot det delvis statlig eide belgiske selskapet Belgacom. Operasjonen ble gjennomført for å nå frem til en sentral ruter for internasjonal mobiltrafikk i Belgia for på den måten å kunne overvåke, og eventuelt manipulere kommunikasjon mellom personer.[91] At knutepunkter for kommunikasjon er interessante for etterretningstjenester er ikke nytt, men GCHQ kunne her nå målet gjennom cyberdomenet uten å være fysisk tilstede i Belgia. Hva slags muligheter har Belgia til å svare politisk på en annen stats handling igjennom cyberdomenet? Og hva vil et proporsjonalt svar være? Det som står mellom Belgacom og GCHQ er i all hovedsak selskapets egne sikkerhetsrutiner samt den nasjonale CERTen. Operasjonen åpner for to andre spørsmål; siden Belgia er en alliert stat innebar formodentlig overvåkningen en inngripen i belgisk mobiltrafikk belgiske myndigheter selv ikke ville kunne utføre på forespørsel britiske myndigheter? Behovet for å overvåke innhold i trafikken for å oppdage nye ikke-statlige trusler fremhever utfordringene knyttet til det juridiske skillet mellom egne og andres borgere i cyberdomenet, og samarbeid om informasjonsdeling.

Etterretningsoperasjonen var rettet mot en helt sentral ruter i den belgiske kommunikasjonsinfrastrukturen. Et annet viktig spørsmål i den sammenheng er i hvilken grad man risikerer å påvirke stabiliteten i kritisk infrastruktur hos en annen stat ved slike operasjoner? Hva slags utfordringer innebærer dette for sentrale knutepunkter for kommunikasjon i fremtiden hvor flere stater kan søke å gjøre det samme?

3.6.3 Ringvirkninger av avsløringene

Ambisjonsnivået amerikanerne har satt seg i cyberdomenet kan vise seg å gå ut over et bredere spekter av interesser enn sikkerhet og mellomstatlige forhold. Lekkasjene har antagelig i stort skadet statens kredibilitet i internasjonale diskusjoner som har med overvåking, regulering av Internett og spionasje å gjøre. Første halvdel av 2013 var preget av relativt krasse ordelag mellom Kina og USA i etterkant av den såkalte Mandiant-rapporten, hvor den kinesiske hæren langt på vei ble anklaget for omfattende industrispionasje i cyberdomenet av et privat sikkerhetsselskap. I løpet av våren ble det sågar etablert en dedikert arbeidsgruppe for å diskutere cybersikkerhet.[92] Avsløringene kan nå brukes som bevis på at amerikanerne selv driver med offensive cyberoperasjoner mot andre nasjoner.[93]

[90] Direktiv 2006/24EF, 2011
[91] Spiegel Online International, 2013a
[92] Gruppens første møte ble overskygget av Edward Snowdens lekkasjer som begynte på samme tid. Se BBC (2013b)
[93] Sanger, 2013

I flere stater har både politikere og befolkning reagert tydelig på overvåkingen. Spesielt Brasil har tatt til orde for økt statlig kontroll over Internett, blant annet gjennom e-posttjenester som bedre sikrer brasilianske borgere og bedre kontroll med trafikkflyten for å forhindre overvåkning.[94] ICANN[95] har blitt enige om at det er nødvendig å bevege seg hurtigere mot et globalt multi-stakeholder forum.[96] I debattene i ITU, som vi kommer tilbake til i kapittelet om internasjonal organisering, er internasjonal kontroll med funksjonene som nå ligger hos slike ikke-statlige organisasjoner og fora et sentralt mål for flere stater som ønsker mer statlig kontroll over Internett.

Silent Circle og Lavabit, to tilbydere av sikker kommunikasjon på Internett NSA antagelig hadde store utfordringer med å avlytte, har nå lansert et samarbeid for en mer sikker e-post tjeneste. Tjenesten vil ha åpen kildekode og sørge for ikke bare kryptering av innhold, men angivelig også metadata.[97] Dersom reaksjoner som dette lykkes i å tilby enkle løsninger for sikker kommunikasjon som ikke kan overvåkes fra sentrale knutepunkter i Internetts infrastruktur vil utfordringene for etterretningsorganisasjoner bli større i fremtiden. Når informasjonen ikke lenger kan fanges opp ved hjelp av overvåking ved knutepunkter vil antagelig etterretningstjenestene måtte fokusere på brukerens datamaskin isteden – eller rette oppmerksomheten mot brukerens informasjon i kommersielle skytjenester. Den massive filtreringen av internettrafikk vil kunne erstattes med mer en mer målrettet innsats.

3.7 Kriminalitet

Det foregår utstrakt kriminell virksomhet i cyberdomenet. Kriminaliteten berører både næringsliv gjennom tyveri av intellektuell eiendom, noe rapporten omtaler nærmere i kapittelet om økonomiske interesser, og enkeltindivider. Det foreligger ingen gode tall på hverken omfanget eller kostnadene av cyberkriminalitet i Norge, blant annet fordi slik kriminalitet sjeldent anmeldes i utgangspunktet.[98] INTERPOL estimerte kostnadene på verdensbasis i 2007 og 2008 til 8 milliarder dollar.[99]

Politidirektoratets rapport «Politiet i det digitale samfunn» viser til at kriminelle benytter seg av krypterings- og anonymiseringstjenester og omsetter ulovlige varer på svarte markeder ved hjelp

[94] Brooks og Bajak, 2013
[95] Internet Corporation for Assigned Names and Numbers (ICANN) er et non-profit partnerskap opprettet i 1998 for å koordinere arbeidet med unike navn og nummer på Internett. Kort fortalt er det de grunnleggende tildelingene av domenenavn og blokker med IP-adresser, og vedlikeholdet av adressebøkene for disse, som gjøres av ICANN. Internet Assigned Numbers Authority (IANA) er en underseksjon av ICANN med ansvar for blant annet tildelingen av IP-blokker til regionale registre som igjen deler disse ut til internettilbydere som for eksempel Telenor. ICANN sørger altså for at maskiner finner hverandre, eller sagt på en annen måte at Internett fungerer overhode. Disse oppgavene befant seg opprinnelig i det amerikanske handelsdepartementet, men er nå utskilt til ICANN. Se http://www.icann.org/ for mer informasjon.
[96] ICANN (1)
[97] SilentCircle (1)
[98] Politidirektoratet, 2012:6
[9999] INTERPOL (1)

av blant annet et digitalt uregulert betalingsmiddel kalt «Bitcoins».[100] I tillegg til bruken av Internett til ren kommunikasjon og organisering, oppstår det unike muligheter etter hvert som et stadig bredere spekter av menneskelig aktivitet foregår i cyberdomenet. Fordelene knyttet til å overføre tjenester til Internett, slik som nettbank, Altinn eller lignende er at brukeren har tilgang til tjenesten hjemmefra. Dette innebærer at brukeren kan bli det svakeste ledd, og skaper nye utfordringer for sikkerhetsløsninger som ikke kompromitteres dersom brukeren svindles på Internett. Vinningskriminalitet i cyberdomenet omfatter alt fra innbrudd i banktjenester til identitetstyveri eller å kryptere innholdet på datamaskinen for så å kreve løsepenger for å dekryptere.

Siden domenet er globalt kan kriminalsaker i cyberdomenet få trekk vi ellers kjenner igjen i større kriminelle nettverk. I mai 2013 ble det rapportert om et bankran hvor 45 millioner dollar var blitt stjålet. Bankranerne hacket først firmaer som behandler kredittkortopplysninger i India og USA, og hevet grensen for maksuttak. Deretter slo ranerne til mot bankene ved å forfalske bankkortene og ta ut penger i 27 forskjellige land verden rundt.[101] Hendelsen er et godt eksempel på at kriminelle tilpasser seg den globaliserte verdensøkonomien ved å angripe tjenester outsourcet til et annet kontinent gjennom cyberdomenet og spre denne informasjonen til deltagere i flere land for å gjennomføre selve tyveriet.

En studie av 19 globale organisasjoner, gjennomført av Verizon, tar for seg 47 000 hendelser og 621 bekreftede datainnbrudd. Ifølge rapporten kommer de fleste økonomisk motiverte angrepene fra USA eller øst-europeiske land som Romania, Bulgaria samt Russland. I en rapport fra sikkerhetsselskapet Trustwave har de analysert 100 millioner angrep, og finner at 37, 8 prosent stammer fra USA med Russland på andre plass med 12,3 prosent og Taiwan på tredje med 8,8 prosent.[102] En analyse av 450 enkeltsaker viste at 40 ulike typer ondsinnet programvare ble benyttet, og at denne kunne spores tilbake til 6 ulike grupper mennesker.[103].

Av disse grunnene ansees cyberkriminalitet som et globalt problem. Dette stiller store krav til samarbeid mellom stater, både i polititjenestene og politisk, noe rapporten kommer tilbake til i kapittelet om internasjonal organisering. I 2012 understreket en rapport fra Politidirektoratet blant annet at «etterspørselen etter datatekniske undersøkelser er økende» samtidig som at «Mørketallsundersøkelser viser at IKT-kriminalitet i liten grad anmeldes». Videre understreket Politidirektoratet at de anså «Nasjonalt og internasjonalt samarbeid er avgjørende for forebygging og bekjempelse av IKT-kriminalitet».[104]

En annen interessant observasjon hva gjelder myndighetsutøvelse i cyberdomenet er at de store programvareselskapene på sett og vis tar del i den. Tetting av sikkerhetshull og beskyttelse mot ondsinnet programvare er ett aspekt av dette som kanskje er analogt til vakt- og sikringsselskaper

[100] Politidirektoratet, 2012:10
[101] Long og Mendoza, 2013
[102] Trustwave , 2013:27
[103] Trustwave, 2013:20
[104] Politidirektoratet, 2012:6

i den fysiske virkeligheten. Men flere former for ondsinnet aktivitet gjennomføres ved at kriminelle røver til seg kontroll over et stort antall maskiner *spredt verden rundt* i såkalte *botnet*. 5 juni 2013 tok Microsoft ned 1 400 slike botnet som inngikk i kommando og kontrollstrukturen til banktrojaneren Citadel. Microsoft gjorde dette i samarbeid med amerikanske Federal Bureau of Investigation samt andre industripartnere.[105]

Teoretisk sett har de kriminelle her hele verdens lovverk å spille på. Ved for eksempel å drive kriminalitet fra stater med mangelfullt lovverk, som det er vanskelig for Norge å samarbeide med eller skjule egen trafikk ved å rute den gjennom slike stater blir utfordringene for etterforskningen desto større. Spørsmålet er da om ikke kampen mot cyberkriminalitet blir som å klemme på en ballong? Idet man slår ned på den ett sted finner den rom og eser ut der forholdene ligger best til rette for det. Her kan det være et sammenfall mellom de statene det er vanskelig å samarbeide med og de statene hvor omstendighetene ligger best til rette for kriminalitet. Ikke minst må man forvente en dynamikk siden cyberdomenet fortsatt bygges ut i store deler av verden.

4 Økonomi

Lunde og Thune skriver at den økende sammenknytningen med omverdenen gjør «norske økonomiske og velferdsorienterte interesser i større grad må ivaretas utenfor landets grenser».[106] Man ser dette blant annet gjennom norske virksomheter som etablerer seg utenlands, og at utenlandske virksomheter etablerer seg her i Norge. Telenor og Statoil er to giganter som har utvidet sin virksomhet til en rekke andre steder i verden, og dermed også flyttet norsk interessesfære og prioriteringer. Noen virksomheter er globale av natur (f.eks. Opera, Norman, REC[107]), noe som kanskje spesielt gjelder tjenester og programvare i cyberdomenet. Andre, slik som Telenor eller Statoil, har valgt å ta steget ut i verden for å konkurrere også i andre land. I tillegg foregår det en betydelig handel med varer og tjenester på tvers av landegrensene. Ifølge Victor Normann vil Norges inntekter i fremtiden primært komme fra tre kilder: «(1) Produksjon og salg av petroleum og varer og tjenester med tilknytning til petroleumsproduksjon, (2) salg av varer og tjenester fra norskeid virksomhet med base i andre land (med Telenors virksomhet i Asia og Russland som et eksempel), og (3) avkastning på Statens pensjonsfond utland (SPU). Alle disse er allerede i dag mer globale enn regionale.» [108] Norske økonomiske interesser har dermed en omfattende og økende grenseflate med utenrikspolitikken.

Et bredt spekter av økonomisk aktivitet foregår i og gjennom cyberdomenet, og i tillegg til at mye av denne er direkte relatert til Norge og norske interesser er det og et overordnet mål at flere stater får ta del i globaliseringsprosessen.[109] Stadig flere mennesker får ta del i både personlige og samfunnsmessige goder som følger med cyberdomenet og det som kalles internettøkonomien.

[105] Boscovich, Richard Domingues, 2013
[106] Lunde og Thune m.fl., 2008:96
[107] Opera er et norsk selskap som har hatt internasjonal suksess med en egen nettleser. Norman er et kjent norsk antivirusselskap. REC er et norsk solenergiselskap. Alle tre er avhengige av en global kundebase.
[108] Norman, 2013:132
[109] Lunde og Thune m.fl., 2008:110-111

Internettøkonomien er et begrep som ifølge OECD innbefatter «det fulle spekter av økonomiske, sosiale og kulturelle aktiviteter støttet opp av Internett og relaterte informasjons- og kommunikasjonsteknologier.» Norge var ett av de 40 landene som underskrev Seouldeklarasjonen for internettøkonomiens fremtid i 2008. Deklarasjonen understreker blant annet viktigheten av mellomstatlig samarbeid for å legge til rette for innovasjon, investeringer og konkurranse i informasjons- og kommunikasjonsteknologi.[110] Visjonen som legges frem i dokumentet viser til en rekke mekanismer, alt fra å gjøre sysselsetting og gründervirksomhet enklere til demokratiserende effekter, som springer ut av internettøkonomien og bidrar til høyere livskvalitet. Slike effekter stemmer godt overens med dem vi forsøker å oppnå gjennom engasjementspolitikken. De viktigste utfordringene for å nå visjonen er blant annet spredningen av Internett, sikring av kritisk infrastruktur, sikre personvern på Internett og svare på nye trusler.[111] For å få et bedre grep på den konkrete betydningen Internett har for økonomi og vekst, valgte konsulentselskapet McKinsey & Company å sammenligne den med andre sektorer. Deres undersøkelse, basert på 13 land[112] verden rundt, fant at Internett i gjennomsnitt stod for 3,4 prosent av bruttonasjonalproduktet. Om man hadde regnet internettøkonomien som en egen sektor ville den være større enn landbruks- og energisektorene. Det totale bidraget fra internettøkonomien i disse statene er større enn bruttonasjonalproduktet i Spania eller Canada, og vokser hurtigere enn Brasil.[113] Norge er «midt på treet når det kommer til salg av varer og tjenester på nett».[114]

Enkelte steder i verden er det en tendens til «leap-frogging», hvor man hopper over teknologiske utviklingstrinn slik som fasttelefon og går rett på mobiltelefoni. FNs bredbåndskommisjon hevder at siden mobiltelefonen nå har Internettaksess betyr at flere økonomier rett og slett vil hoppe over datamaskinen.[115] Google-sjef Eric Schmidt hevder at hele verdens befolkning vil være på Internett i løpet av de neste sju årene.[116] Ett viktig spørsmål i forbindelse med utviklingen av internettøkonomien i disse områdene avhenger blant annet av hvilken grad tilgang og innhold reguleres, slik Seoul-deklarasjonen påpeker. Reguleringsspørsmålene er relevante både for norske virksomheters vilkår utenlands og internettøkonomien men for mykere verdier som ytringsfrihet og organisasjonsfrihet. En sentral arena for debatt her er WCITs konferansene i regi av ITU, noe som drøftes nærmere i kapittelet om internasjonal organisering.

4.1 Cyberdomenets våpenindustri og sårbarhetsøkonomi

Statens Pensjonsfond Utland (SPU) gjør Norge til en «betydelig finansiell aktør» i verden.[117] I 2004 ble det opprettet et eget Etikkråd for SPU som kunne komme med anbefalinger for investeringene. Etikkrådet har mulighet til å anbefale utestengelse av enkeltselskaper fra SPUs

[110] OECD, 2008
[111] OECD, 2008
[112] Canada, Frankrike, Tyskland, Italia, Japan, Russland, Storbritannia, USA, Sør-Korea, Sverige, Brasil, India og Kina.
[113] McKinsey & Company Global Institute, 2013
[114] NOU 2013:2, Innledning.
[115] ITU Broadband Commission, 2013:16
[116] Gross, 2013
[117] Stortingsmelding 15 (2008-2009) S 87

investeringsunivers ved enkelte graverende tilfeller, slik som produksjon av «våpen som ved normal anvendelse bryter med grunnleggende humanitære prinsipper», «selger våpen eller militært materiell til stater som er omfattet av ordninger for statsobligasjonsunntak…» samt «alvorlige krenkelser av individers rettigheter i krig elle konfliktsituasjoner» og «alvorlig miljøskade».[118]

En ekvivalent til våpenindustrien i cyberdomenet er i ferd med å vokse frem, og kan by på lignende problemstillinger i fremtiden. For å kunne bryte seg inn i datasystemer er det nødvendig med kjennskap til sårbarheter i programvaren hos målet. Sårbarheter som er offentlig kjente kan bli tettet i en programvareoppdatering og en motpart med gode rutiner for oppdateringer vil være sikret mot denne. Sårbarheter som ikke er offentlig kjente er dermed av stor verdi for en angriper da sannsynligheten for et vellykket innbrudd blir større. Ukjente sårbarheter kalles ofte nulldagssårbarheter, eller zero-days. Markedet som har oppstått for kjøp og salg av sårbarheter kalles gjerne sårbarhetsøkonomien.

Tradisjonelt har sårbarheter blitt rapportert direkte til produsenten uten kompensasjon. Større virksomheter har i dag begynt å utlove dusør til de som gjør dem oppmerksomme på et sikkerhetshull slik at det kan tettes i en oppdatering. Samtidig jobber både privatpersoner og profesjonelle selskaper med å finne sikkerhetshull, forsøke å gjøre disse utnyttbare og selge dem til andre enn programvareutvikleren selv. Industrien ansees som kontroversiell fordi salg av ukjente sårbarheter til andre enn programvareutvikleren innebærer at sårbarheten forblir utettet for alle – og potensielt utnyttbar for eieren av sårbarheten. Et sentralt spørsmål i den anledning er hvem får lov å kjøpe? Foreløpig er det spesielt nasjonalstater som er villige til både å betale og utnytte den til sitt fulle. To kjente slike selskaper, VUPEN og REVULN, holder til henholdsvis i Frankrike og Malta. VUPEN hevder at de kun selger til Nato-stater[119], mens kundelisten for REVULNs sårbarheter for industrielle kontrollsystemer forblir ukjent. Under et intervju med Forbes Magazine viste sårbarhetsmegleren «the Grugq» til at nasjonalstater ikke bare betalte bedre, men også betalte gjentatte ganger dersom sårbarheten forble ukjent. Å selge til den russiske mafiaen var en mulighet, men rett og slett ikke lønnsomt.[120]

Et relatert dilemma kan oppstå når det gjelder programvare for eksempel til overvåking av enkeltpersoner eller filtrering av internettinnhold. To kjente eksempler på dette er amerikanske Blue Coat systemer eller britiske FinFisher. Disse kan benyttes i legitimt sikkerhetsøyemed, men og til indre makt på en måte som er lite forenelig med både internasjonal lov og norske verdier. Slike systemer er for eksempel blitt benyttet av Gadafi i Libya[121] og Assad i den pågående borgerkrigen i Syria.[122]

[118] Finansdepartementet (1)
[119] Hofmann og Timm, 2012
[120] Greenberg, 2012
[121] Sonne og Coker, 2011
[122] Valentino-Devries, Sonne og Malas, 2011

4.2 Outsourcing

Avslutningsvis i sikkerhetskapittelet ble det vist til et bankran hvor to kredittkortselskaper i henholdsvis India og USA hadde blitt hacket av ranerne, før penger ble tatt ut i et tyvetalls land. Bankene som ble ranet var hverken indiske eller amerikanske. Det var Bank of Muscat of Oman og National Bank of Ras Al Khaimah PSC i de Forende Arabiske Emirater. Kredittkorttjenestene deres var altså outsourcet til India og USA. Outsourcing er et annet kjennetegn på en globalisert verdensøkonomi hvor fornuftige handlinger rent økonomisk sett også kan ha sikkerhetsimplikasjoner igjennom cyberdomenet.

Outsourcing innebærer ikke bare at enkelte oppgaver i norsk næringsliv settes bort til andre land, men og at norsk næringsliv kjøper enkelte oppgaver fra utenlandske aktører snarere enn å gjøre de selv. "Kinesiske Huawei leverer for eksempel enkelte komponenter til radiodelen av 4G-nettet. Huawei er en global gigant som her bidrar til radiodelen i den største oppgraderingen av mobilnettet i Norge noensinne, og har sine egne nettverksoperasjonssentre lokalisert i Romania, Spania, Sveits og Italia.[123]

Deler av fremtidens norske mobilnett leveres altså av et selskap med tette bånd til kinesiske myndigheter og en driftsinfrastruktur spredt ut over andre land i Europa. Ansvaret for å sørge for et tilstrekkelig sikkerhetsnivå i anskaffelsene tilfaller Telenor og NetCom, med mindre disse vurderer det dithen at anskaffelsen er sikkerhetsgradert og krever evaluering fra NSM. I vurderingen av leverandører til fornyelsen av mobilnettet hadde Telenor en dialog med NSM, og mottok ikke innspill som skulle tilsi at Huawei av sikkerhetsmessige årsaker burde ekskluderes i leverandørprosessen.124

Norske sikkerhetsinteresser kan her også komme i konflikt med økonomiske interesser. Siden Liu Xiaobo fikk nobels fredspris har Norge hatt et forholdsvis kjølig forhold til Kina, og en gransking av en stor kinesisk bedrift kan virke negativt inn på dette forholdet. En slik gransking kan ha negative konsekvenser for øvrige økonomiske interesser i Kina. Som følge av en amerikansk granskning skvises nå Huawei ut av det amerikanske markedet. Selskapet satser nå sterkere i Europa, og EU-kommisjonen vurderte å innlede en etterforskning av selskapet, og ett annet kinesisk selskap ved navn ZTE, for prisdumping og sikkerhet. Svenske Sony Ericsson var tydelig motstander av en slik granskning da den kunne slå negativt ut på deres konkurranseevne i Kina.[125]

Selv om Huawei her har vært hovedtema for drøftingen antyder Edward Snowdens avsløringer at også Norges allierte stater produserer maskin- og programvare med bakdører som kan utnyttes logisk på et senere tidspunkt. Det er i så måte ikke gitt at de samme utfordringene ikke gjelder også andre utenlandske leverandører av telekomutstyr.

[123] Huaweis hjemmesider (1)
[124] Bruaset og Dahl, 2012; Dahl og Bruaset, 2012
[125] Rossen, Eirik, 2013

4.3 Vilkår for virksomheter og investeringer i utlandet

En stadig større andel av norske inntekter fremover vil komme fra utlandet, da primært gjennom kapitalinvesteringer. «Derfor er det viktig at myndighetene gjennom utenrikspolitikken arbeider aktivt for å sikre at disse investeringene får trygge og rettferdige vilkår i så mange land som mulig.»[126] I tillegg kommer og de norske virksomhetene som etablerer seg også i andre land. Norske økonomiske interesser i andre land i verden gjør at innenriksforholdene i disse landene også blir viktigere for Norge. Lunde og Thune nevner eksempelvis viktigheten av innenrikspolitikk i Algerie grunnet Statoils virksomhet i landet. Disse hensynene flettes sammen med andre utenrikspolitiske interesser, både statlige så vel som norske innbyggeres, som ikke nødvendigvis passer godt overens med ren profittmaksimering.[127] Menneskerettigheter, kriminalitet og korrupsjon i cyberdomenet er dermed noe Norge må evaluere opp mot våre økonomiske interesser.

4.3.1 Cybersikkerhet for norske virksomheter i utlandet

Norske virksomheter i utlandet, og utenlandske virksomheter i Norge, vil nødvendigvis måtte forholde seg til gjeldende nasjonalt lovverk i de lokasjonene de har verden rundt. Som konkurrerende aktør, representant for den norske stat eller sågar representant for det noen oppfatter som et onde i verden (for eksempel Statoil og miljøvernaktivister) står disse virksomhetene allikevel overfor et globalt trusselbilde i cyberdomenet. Hvorvidt de statene de opererer i vier oppmerksomhet til cybersikkerhet og har evner, interesse og kompetanse til å takle og etterforske hendelser vil variere verden rundt. Dette kan fungere til angriperens fordel da det er mulig å foreta en målutvelgelse i de statene hvor muligheten for å bli tatt er lavest. Dette kan gjøre virksomhetene ekstra avhengige av både egne og den norske stats ressurser for påvirkning av lokale cybersikkerhetsforhold.

Akkurat som Norge arbeider for å bedre vilkårene for norske økonomiske interesser i utlandet, vil andre stater gjøre det samme i Norge. Innenrikspolitikken som skal sikre oss et godt cybersikkerhetsregime her til lands vil kunne være med på å gjøre oss attraktive for utenlandske virksomheter.[128] I likhet med det fysiske domenet, er det umulig å tilby perfekt sikkerhet, men det kan være mulig å oppnå komparative fortrinn som trekker oppmerksomhet til Norge. Her kan mellomstatlige rettssamarbeid, informasjonsutvekslingsregimer og samarbeid mellom dataovervåkningssentre bidra til å fronte Norge som en trygg nasjon å etablere seg i.

I februar 2013 meldte Business Insider at flere store bedrifter, slik som Apple Inc, General Electric Co, Caterpillar, DSM, General Motors og kinesiske Lenovo nå satset tyngre i USA. Dette innebærer ikke nødvendigvis en reversering av den lengre trend hvor arbeidsplasser flyttes utenlands hvor arbeidskraften er billigere. Det er imidlertid interessant å merke seg at *en av grunnene* for denne endringen er problemer med rettssikkerhet rundt intellektuell eiendom i Kina.[129] Selv om virksomheter ikke nødvendigvis kan flytte bort fra en trussel i cyberdomenet

[126] Lunde og Thune m.fl., 2008:97
[127] Lunde og Thune m.fl., 2008:99
[128] Stortingsmelding 15 (2008-2009) S 115
[129] Welsh, 2013

kan de flytte til områder hvor forutsetningene for å sikre seg er bedre. Å profilere Norge som et trygt miljø å etablere virksomhet i også når det gjelder cybersikkerhet kan bidra til å trekke næringsliv til Norge.
Lunde og Thune skriver at man må «vurdere justeringer av lokalisering og funksjoner for ambassader og konsulater i lys av globaliseringen» for å sikre forståelse av at norsk utenrikspolitikk også har konsekvenser for norske virksomheter i landet. [130]
Cybersikkerhetsspørsmål er her noe norske representanter i utlandet må være forberedt på å arbeide med for å bedre forhold for norske virksomheter i utlandet.

4.3.2 Nasjonal lovgivning for å fremme norske økonomiske interesser i cyberdomenet?

I foregående kapittel ble det nevnt hvordan nasjonal lovgivning var benyttet mot selskaper med globale kundebaser til å fremme amerikanernes evne til å utøve cybermakt. Den krypterte e-posttjenesten Silent Circle opplevde en inntektsøkning på 400 prosent i månedene etter de første Snowden-lekkasjene, før den stengte ned i frykt for å måtte utlevere informasjon til amerikanske myndigheter. Dette ville være i strid med de garantiene som var blitt gitt til brukerne av tjenesten.[131] Sikkerhetseksperten Bruce Schneier understrekte at dette var forskjellen mellom mulighetsrommet for en virksomhet eid og driftet av en person, og en med ansvar ovenfor aksjonærene.[132] Artmotion, et sveitisk datalagringsfirma, opplevde også en tydelig økt popularitet for sine tjenester, som blant annet er beskyttet av Sveits' lovgivning og nøytralitet.[133] Norske Jottacloud opplevde en tidobling over natten i sine skytjenester som følge av en ny personverngaranti rett etter avsløringene. Ett av salgspunktene var nettopp det at dataene ble lagret her i Norge, og ikke hos Apple eller Google i USA.[134] Flere høyerestående politikere i europeiske land, og EU, har og tatt til orde for å gå over mot egne skytjenester for å sørge for bedre kontroll med dataene. Ifølge en rapport fra en amerikansk tenketank vil en slik trend føre til et tap på mellom 21,5 og 35 milliarder dollar innen 2016, eller mellom 10 og 20 prosent av inntjeningen for amerikanske skytjenester.[135], [136]

En rekke tyske virksomheter har gått over til å benytte vanlig postgang istedenfor elektroniske løsninger for informasjon de ikke ønsker ut i det offentlige rom eller til sine konkurrenter. Hovedårsaken er ikke nødvendigvis at de motsetter seg overvåkningen fra amerikansk etterretning, men at de frykter industrispionasje gjennom det tette samarbeidet mellom etterretnings- og sikkerhetstjenestene i USA og private kontraktører.[137]

Den grunnleggende lærdommen her er egentlig at det nasjonale lovverket var avgjørende for hvor dataene havnet, selv om man har med en global tjenestetilbyder å gjøre. Dette innebærer

[130] Lunde og Thune m.fl., 2008:99
[131] Olson, 2013
[132] Schneier, 2013
[133] Tsukayama, 2013
[134] Jottacloud (1)
[135] Whittaker, 2013
[136] Rossen, 2013
[137] Spiegel Online International, 2013b

nødvendigvis også at nasjonalt lovverk kan benyttes til å tiltrekke seg kunder, om det så handler om et *komparativt fortrinn* i verden. Nasjonal lovgivning kan benyttes til å tilby tjenester beskyttet av norsk lov til en global kundebase. Viktige punkter her er under hvilke omstendigheter data kan utleveres fra tjenesten, og hvem dette kan deles med. Det er kanskje mer enn økonomiske interesser som kan underbygges med norsk lov, for eksempel ved å gi kommunikasjonsmuligheter for mennesker som opplever undertrykkelse og overvåking i cyberdomenet?[138]

4.4 Internasjonal konkurranse om arbeidskraft innen cybersikkerhet

Eldrebølgen vil gjøre Norge mer avhengig av å importere arbeidskraft og etterspørselen etter UDs tjenester vil derfor i følge Lunde og Thune blir større. I årene fremover vil fagkompetanse innen cybersikkerhet være høyt etterspurt ikke bare i Norge, men etter alt å dømme også andre land. Lunde og Thune viser til at den norske inntektsfordelingen gjør det vanskelig å trekke spesialister til Norge, og at de fremtidige utenrikspolitiske utfordringene her vil være knyttet til aktivt promoterings- og rekrutteringsarbeid.[139] Den vedvarende finanskrisen har kanskje gjort det lettere å tiltrekke arbeidskraft siden norsk økonomi går relativt godt, spesielt sammenlignet med land sør i Europa. Det er imidlertid ikke en utvikling vi kan regne med, eller ønske at fortsetter på sikt.

Rent politisk har det skjedd et brått skifte i interessen for cybersikkerhet rundt om i verden, samtidig som det er mangel på ferdigutdannet kompetanse. Det blir derfor desto viktigere å sørge for et godt utdanningssystem som holder god kvalitet internasjonalt sett slik at vi kan sikre rekruttering og holde på kompetansen etter endt utdanning. Satsning på å etablere utdanningsløp og kunnskapssentre sees nå i flere stater. I Storbritannia har non-profit selskapet Cyber Challenge UK, et fristilt selskap sponset av britiske myndigheter, starter opp et pilotprosjekt med 2 000 skolebarn for å fremme cybersikkerhet som et karrierevalg i fremtiden.[140] Det er i tillegg bevilget 7.5 millioner pund til utdanning av cybersikkerhetseksperter ved to universiteter.[141] Satsning på utdanning, arbeidsplasser og produktutvikling innen cybersikkerhet er og ett tema som trekkes frem i den finske cybersikkerhetstrategien.[142]

Det er allerede en mangel på kompetent personell, og dette kan også veie inn i beslutningsprosessen for virksomheter som vurderer å etablere seg her. I tillegg etableres det nå flere CERTer, blant annet i justisdepartementet, helsesektoren og finanssektoren. Etterspørselen etter kompetanse ventes altså å gå opp i årene som kommer. Problemet forsterkes ytterligere for staten, som må konkurrere mot lønn i privat sektor samt leve med behov for sikkerhetsklarering. Eksperter innen cybersikkerhet vil være viktige for både politimyndighetene og forsvarssektoren så vel som tilbydere av kritisk infrastruktur i offentlig og privat sektor fremover. Samtidig som disse vil spille en viktig rolle overfor virksomhetene i samfunnet for øvrig.

[138] Sammenlignet med andre stater kan for eksempel en e-posttjeneste underlagt norsk jurisdiksjon fremstå som attraktiv for dissidenter i autoritære regimer.
[139] Lunde og Thune m.fl., 2008:97
[140] Hopkins, 2013
[141] Coughland, 2013
[142] Finland's Cyber security Strategy

Opprettelsen av et senter for cyber- og informasjonssikkerhet ved Høgskolen i Gjøvik kan være et viktig tiltak for å øke tilgangen på kompetanse i fremtiden. Senteret har ifølge dekan Morten Irgens potensiale til å tilby en unik kompetanseprofil i Europa.[143] I tillegg til Politidirektoratet har FFI, NSM og Cyberforsvaret vært viktige støttespillere for å sikre finansiering til ti nye professorater på Gjøvik.[144]

4.5 Spionasje med kommersielle formål

I en verden av stater uten noen overordnet myndighet med voldsmonopol vil det nødvendigvis foregå etterretningsaktivitet for at stater skal kunne holde et øye med potensielle sikkerhetstrusler. I tillegg til den etterretningsaktivitet stater bedriver for å ivareta egen nasjonal sikkerhet foregår det spionasje for å fremme kommersielle mål, både i statlig og ikke-statlig regi. Denne typen spionasje kan omtales som kriminalitet, men skiller seg fra øvrig kriminalitet i cyberdomenet ved å være både målrettet og langt mer avansert. Vinningskriminaliteten er ofte basert på at millioner av e-poster sendes ut og et fåtall lar seg lure (*phishing*). Spionasje med kommersielle formål gjøres ofte ved hjelp av sosial manipulering av nøkkelpersoner, og tar for eksempel form som skreddersydde meldinger det er langt vanskeligere å gjennomskue (*spear-phishing*). De mest avanserte aktørene kalles ofte «*Advanced Persistant Threats*», eller APTer.

De hemmelige tjenestenes åpne trusselvurderinger viser alle til industrispionasje rettet mot norske mål. Cyberdomenet, også i kombinasjon med personer på innsiden, benyttes ifølge PST for å «understøtte virksomhet som kan øke den nasjonale evnen til utvikling, innovasjon og produksjon av forsvarsmateriell.» Dette gjelder også for sivil sektor, for eksempel «nano- og biovitenskap, medisin, IT og romforskning, arktisk petroleumsteknologi og skips- og verftsteknologi, samt til enkelte nisjeområder som fysikk og ingeniørfag» som i tillegg også kan være viktig i forsvarsteknologi. [145] NorCERT trekker fram olje- og gassektoren som en av de sektorene som er særskilt utsatt for målrettet spionasje.[146]

Estimater på kostnadene knyttet til kriminalitet i cyberdomenet i verden varierer voldsomt og ofte gjennomføres undersøkelsene av anti-virus og sikkerhetsselskaper, som kan ha en interesse av å overdrive problemet. Definisjonene av cyberkriminalitet spriker, slik at tallene også blir ekstra utfordrende å sammenligne. I en rapport basert fra 2012 meldte selskapet Symantec at det var 556 millioner ofre for cyberkriminalitet hvert år med en prislapp globalt på 110 milliarder dollar.[147] Dette inkluderer altså både vinningskriminalitet og spionasje. En rapport i regi av McAfee og CSIS estimerte kostnadene til mellom 300 milliarder og 1 trillion dollar, tilsvarende 0,4 til 1,4 prosent av verdens samlede bruttonasjonalprodukt.[148] Til sammenligning var for eksempel FNs estimat på den globale narkotikaøkonomien 320 milliarder dollar i året.[149] NSA/US CYBERCOMs sjef Alexander hevder cyberkriminalitet er «the greatest transfer of wealth in

[143] Børresen, Gregersen og Sørenes, 2013
[144] Nilsen, 2013
[145] Politiets Sikkerhetstjeneste, 2013:8-9
[146] Nasjonal Sikkerhetsmyndighet, 2012
[147] Norton, 2012
[148] Center for Strategic and International Studies og McAfee, 2013
[149] FNs nyhetssenter, 2012

history».[150] Ifølge INTERPOL var de økonomiske tapene knyttet til cyberkriminalitet i 2007 og 2008 på om lag 8 milliarder dollar, mot 1 trillion knyttet til industrispionasje i cyberdomenet.[151]

Det er flere verdier som er vanskelige å tallfeste, spesielt med tanke på spionasje. Hvordan kalkulerer man tap fra mangeårige forskningsprosjekt, fremtidige inntekter og tap av markedsfortrinn? Skal man regne med nedetiden for tjenester og ressursene brukt på å gjenopprette integritet eller samfunnskostnadene ved etterforskning osv? Kommer disse tallene i sin helhet i tillegg til all annen kriminalitet og spionasje, eller er det et overlapp? En rapport fra 1992, før the World Wide Web, estimerte kostnadene av spionasje i USA til 597 milliarder dollar i produktutvikling alene. En annen rapport fra 1996 estimerte 100 milliarder dollar årlig til fremmed spionasje.[152]

Det er heller ikke slik at spionasje resulterer i et direkte tap ekvivalent til den informasjonen som er stjålet. For avansert teknologi er det nødvendig med en teknologibase og kompetanse for forståelse, store mengder data stiller krav til analyseevne. Det kan sies å være en forskjell mellom å stjele informasjon og faktisk evne å nytte seg av den. Det er en forskjell på eksplisitt kunnskap og erfaring. Thomas Rid sammenlikner det med forskjellen mellom å stjele en oppskrift på brød og det å lære å bake det av den beste bakeren.[153] I det minste for enkelte typer intellektuell eiendom er det krav til for eksempel kompetanse og fasiliteter før man kan nytte seg av den.

Det er altså vanskelig å tallfeste kostnadene knyttet til både cyberkriminalitet og spionasje, men slike tall får kanskje heller ikke frem hvorvidt dette er et kritisk problem eller ikke. Sett opp mot det norske bruttonasjonalproduktet i 2011 utgjør de 20 milliardene snaue 1 prosent. Samtidig er det ikke bare intellektuell eiendom som stjeles, men og for eksempel øvrig bedriftsinformasjon som kan få store konsekvenser for selskapene på sikt. Informasjonen som stjeles av APTer er ikke nødvendigvis noe som merkes umiddelbart, men først får konsekvenser flere år frem i tid. Ifølge tidl. avdelingsdirektør i NSM Eliv Ofigsbø har det vært flere angrep i Norge med tap i hundre millioners-klassen i kontrakter i etterkant. Det kan derfor være vanskelig å estimere det reelle tapet et angrep har forårsaket før etter lengre tid. Den kanadiske telegiganten Nortel er et godt eksempel på skaden en APT kan gjøre over tid. Nortel ble uforvarende tappet for informasjon over en tiårsperiode, og begjærte seg konkurs i 2009 etter 114 års virksomhet.[154] Selskapet mistet rett og slett sitt konkurransemessige fortrinn i telemarkedet.[155]

I mars 2013 anmeldte Telenor for første gang avansert industrispionasje gjennom cyberdomenet begått av en annen organisasjon.[156] En rapport fra cybersikkerhetsselskapet Norman Shark konkluderte med at Telenor kun var ett av flere mål. Gruppen som stod bak var basert i India og hadde tidligere spionert mot mål i Pakistan. Ifølge rapporten hadde gruppen i løpet av 2012-2013

[150] Protalinsky, 2012
[151] INTERPOL (1)
[152] Bellocchi, 2001:368
[153] Rid, 2013:82-84
[154] Se The Huffington Post, 2012 & Naraine, 2012
[155] Berkow, 2012
[156] Johansen, 2013

gått over i industrispionasje mot et bredt spekter av mål innen gruvedrift og naturressurser, transport, rettsvesen, ingeniørvitenskap, matindustri, militæret, finans og en aktivist som skulle delta på Oslo Frihetsforum.[157] I likhet med stadig flere innbrudd ble målene i Telenor, her utvalgte personer i sjefsstillinger, lurt ved hjelp av et e-postvedlegg med ondsinnet kode. Antagelig var dette angrepet gjennomført av en ikke-statlig aktør, men det lyktes i å tappe ofrenes datamaskiner for e-post, alle typer filer og passord samt personlige data.[158]

Med Nortels konkurs mister ikke bare Canada en viktig arbeidsgiver, men også hovedaktøren for en hel sektor. Dette er et skrekkeksempel hvor det er forholdsvis enkelt å forstå at konsekvensene er store. Ringvirkningene kjennes også samfunnsøkonomisk i form av for eksempel tapte arbeidsplasser. Selv dersom de økonomiske tapene på nasjonalt nivå ikke skulle synes å være en direkte trussel er det verdt å spørre seg om summen av flere hendelser på sikt kan gir alvorlige utslag? Hva slags langsiktige implikasjoner vil for eksempel målrettet og systematisk industrispionasje mot norsk petroleumsteknologi kunne ha?

Den internasjonale debatten vedrørende spionasje med kommersielle hensikter har så langt vært preget av nokså generelle referanser til ondsinnede aktører. En av årsakene er antagelig ikke bare at metodene for å gjennomføre industrispionasje ligner på metodene for annen spionasje, men også fordi attribusjon gjennom cyberdomenet alene er vanskelig. Å gå konkret ut med informasjon om nøyaktig hvem som står bak, og hva som er blitt gjort, innebærer nødvendigvis også å avsløre egne metoder for etterforskning utenfor egne grenser. De mest frittalende aktørene så langt har vært antivirusselskaper, sikkerhetsselskaper og tenke-tanker som ikke har de samme sikkerhets- og utenrikspolitiske hensynene å ivareta. Spesielt en slik rapport har fått et betydelig statlig etterspill er sikkerhetsselskapet Mandiants rapport om APT1. Rapporten kom i februar 2013 og har et pågående etterspill mellom USA og Kina. Mandiants rapport er spesiell fordi den langt på vei hevder at APT1 i realiteten er en avdeling av den kinesiske frigjøringshæren (PLA). Samtidig som at slike rapporter kan være utfordrende for mellomstatlige forhold er de en måte å få ut informasjon som stater selv ikke kan frigi.

4.6 Beskyttelse av økonomiske interesser

Norsk næringsliv står altså ansikt til ansikt med et globalt trusselbilde muliggjort av cyberdomenet. De aller fleste norske virksomheter er små[159] og kan vanskelig ventes å investere tungt i cybersikkerhet, da spesielt egne CERTer. Det kan være billigere å bære kostnadene av et angrep enn å investere i sikkerhet eller å holde angrepet skjult fra offentligheten og egen kundebase.[160] I mørketallsundersøkelsen 2012 hevder Datakrimutvalget at økt oppmerksomhet på sikkerhetskompetanse, holdninger og informasjonsinnhenting om sikkerhetshendelser er de viktigste tiltakene for å bedre sikkerhetstilstanden i næringslivet.[161]

[157] Fagerland, 2013
[158] TV2, 2013
[159] NOU (2013:2):30
[160] NOU (2007:2):Kap 3.3
[161] Næringslivets Sikkerhetsråd, 2013:9

I møtet med nye trusler og utviskede grenser implementerer stater nå flere ulike nye, og til dels unike, tiltak. I den nederlandske nasjonale cybersikkerhetsstrategien ble det vedtatt å etablere et nasjonalt cybersikkerhetssenter med representanter fra både offentlig og privat sektor med ansvar for å implementere strategien. Den statlige CERT-funksjonen, GOVCERT, ble også underlagt dette senteret.[162] Den britiske cybersikkerhetsstrategien viser blant annet til etableringen av et nytt partnerskap for informasjonsdeling om trusler mellom offentlig og privat sektor[163] samt opprettelsen av en ny nasjonal CERT hvor eksperter fra både privat og offentlig sektor koordinerer sitt arbeid mot cyberkriminalitet og cyberangrep. [164] Det er angivelig 160 selskaper involvert i dette prosjektet.[165]

I handlingsplanen for den norske strategien for informasjonssikkerhet slås det fast at et nett av sektor-CIRT'er, under koordinering fra NorCERT, skal gjøre Norge i stand til å takle fremtidens nettbaserte trusler.[166] I strategidokumentet understrekes det og at myndighetene må ha et «tett samarbeid med alle relevante aktører i offentlig og privat sektor» for å ivareta ansvaret for informasjonssikkerhet i Norge.[167] Arbeidet mot kriminalitet og spionasje i Norge faller først og fremst en oppgave for politimyndighetene. I handlingsplanen for den norske strategien for informasjonssikkerhet legges det opp til en styrking av disse kapasitetene. Da strategien ble publisert var PST ferdig med første del i et prosjekt for å undersøke ansvar og egen rolle ved nettverksangrep. Deres rapport viste til et behov for å øke bemanningen innen etterretningsinnsamling og ledelse, teknisk håndtering, strategisk analyse og etterforskning. I tillegg var ett mulig tiltak deltagelse i NorCERT på permanent basis for å øke egen kompetanse til håndtering av slike trusler.[168]

Det virker å være få områder hvor Forsvaret kan bidra til å fremme økonomiske interesser i cyberdomenet. Forsvaret kan ikke patruljere cyberdomenet for å beskytte, ivareta og fremme norske økonomiske interesser på en måte analogt til den som gjøres for eksempel til sjøs. I den grad det eksisterer noen analogi til en slik rolle i cyberdomenet ligger denne nå hos NorCERT, sektorvise CERTer og hos den enkelte virksomhet. Grenseflaten mot Forsvaret ligger først og fremst der hvor etterretningstjenester i fremmede stater søker å fremme egne økonomiske interesser gjennom spionasje mot norske mål.

Cyberforsvaret er en slik sektorvis CERT med ansvar for Forsvarets egne nett, i inn- og utland. Forsvarets nåværende rolle i å beskytte, ivareta og fremme norske økonomiske interesser er derfor primært knyttet til den informasjons- og kunnskapsutvekslingen det legges opp til mellom disse CERTene. Forsvaret forsker, utvikler og benytter imidlertid teknologi som kan være av interesse for både statlige og ikke-statlige aktører, akkurat som næringslivet for øvrig. Forsvarsindustrien fremstår som interessante mål for en motpart både for å få kjennskap til

[162] Ministry of Security and Justice, 2010:9
[163] Det britiske kabinettkontoret, 2011:9
[164] Ring, 2013
[165] Hutton, 2013
[166] Fornyings-, administrasjons- og kirkedepartementet, 2013b:19-20
[167] Fornyings-, administrasjons-, og kirkedepartementet, 2013a:10
[168] Fornyings-, administrasjons- og kirkedepartementet, 2013b:21

teknologien og dermed mulige svakheter, men også for å stjele teknologien for å kopiere den. I de omstendigheter det lar seg gjøre er utveksling av informasjon om de delene av trusselbildet Forsvaret har til felles med andre av gjensidig nytte. Forsvaret kan fremstå som en foregangsaktør innen sikkerhet og delta i samfunnsdebatten, enten gjennom trusselvurderingene eller øvrige debattinnlegg, for på den måten å bidra til økt bevissthet rundt trusler i cyberdomenet, noe blant annet Mørketallsundersøkelsen viser til at det er et behov for.

5 Energi, klima, miljø og naturressurser

Lunde og Thune skriver «Energi – i vår sammenheng olje og gass – er Norges viktigste økonomiske ressurs […] og det synligste norske fotavtrykket utenfor egne grenser.»[169] Norske Statoil driver per 2013 forretningsvirksomhet i 35 land verden rundt.[170] Norge var per 2011 verdens femte største oljeeksportør og tredje største gasseksportør. I 2012 utgjorde råolje og naturgass alene henholdsvis 307 og 252 milliarder kroner av den totale norske eksporten på 936 milliarder kroner, eller om lag 60 prosent.[171] I tillegg til Statoil er en rekke utenlandske operatører representert i norske farvann, også i den pågående letingen i Barentshavet.[172] Norge huser og en rekke foregangsmiljøer for utvikling av petroleumsteknologi. Den norske petroleumssektoren er altså internasjonal på en rekke måter, og helt sentral i norsk økonomi.

Lunde og Thune beskriver klare endringer i hvordan Norge må forholde seg til energi i utenrikspolitikken. «Inntil nylig har mye av fokuset og tyngdepunktet vært på økonomiske og rent energipolitiske/forvaltningsmessige sider ved Norge som ressursnasjon». Økende geopolitisk spenning og klimaendringer gjør nå at Norge i langt større grad må vurdere også den politiske betydningen av vår rolle som energinasjon.[173] Norge må for eksempel balansere interessene for profittmaksimering med normer ovenfor investeringsområdene våre og klimaendringer samtidig som vi fremstår som en «pålitelig, ansvarlig og forutsigbar leverandør» av energi.[174]

5.1 Petroleumsteknologi

Petroleumsindustrien er både et mål for kritikk i miljøhenseende og samtidig en kritisk avhengighet på globalt nivå. Lunde og Thune viser til at Norge har høye miljøstandarder som gjør at vi blant annet kan vise til verdens mest miljøvennlige oljesektor. Disse kravene har og vært kimen til utenrikspolitiske utfordringer i forbindelse med for eksempel utenlandske operatører på norsk sokkel, transport av olje og gass fra eller gjennom norske områder.[175]

Norge ligger langt fremme i utviklingen av petroleumsteknologi, da spesielt den godt egnet til drift under vanskelige forhold til havs. Vanskeligere forhold, kostnadseffektivisering og ønske om

[169] Lunde og Thune m.fl., 2008:121
[170] Statoils nettsider (1)
[171] Statistisk sentralbyrå, 2013
[172] Stangeland, 2013
[173] Lunde og Thune m.fl., 2008:113
[174] Lunde og Thune m.fl., 2008:113-114
[175] Lunde og Thune m.fl., 2008:127

økt sikkerhet både for utvinningsprosessen og personell gjør også at driften blir mer teknologiintensiv. Bedrifter som West Drilling Products og Robotic Drilling Systems i Stavanger utvikler for tiden robotiske borerigger som ifølge enkelte vil revolusjonere oljebransjen, ikke ulikt hva horisontalboringen gjorde på 1990-tallet.[176] Teknologiutviklingen som dette støtter både norske økonomiske interesser og energiinteresser ved å forbli en ledende aktør på markedet, og effektivisere egen produksjon. Utviklingen av petroleumsteknologi bringer en stadig større del av næringen tettere opp mot cyberdomenet, og stiller skjerpede krav til sikre systemer og evne til å håndtere uønskede hendelser. Som teknologidriver innen petroleumsnæringen har Norge også gode forutsetninger for å bidra til å implementere sikre og stabile systemer i fremtidens energiinfrastruktur.

Refleksprosjektet viser til at store deler av de gjenværende petroleumsressursene befinner seg i «land og regioner med utstrakt grad av konflikt, menneskerettighetsbrudd, korrupsjon og manglende demokratisk utvikling.» [177] Når norske energiinteresser skal fremmes i slike klima kan de komme i konflikt med andre norske verdier. Økt ressursnasjonalisering forsterker og politiserer denne typen problematikk.[178] Hovedhypotesen fra Leiv Lunde og Iselin Stensdal ved Fridtjof Nansens Institutt er at kommersielle, og ikke maktpolitiske, strategier vil benyttes av de kommende asiatiske energigantene for å sikre tilgangen til energi.[179] I foregående kapittel var ett av hovedtemaene spionasje med kommersielle formål, blant annet mot petroleumsteknologi. I mørketallsundersøkelsen 2012 skriver Statoil at det «Innenfor forretningsutvikling, hvor en arbeider med internasjonale prosjekter med stor strategisk og finansiell betydning, ser vi at eksterne aktører i økende grad forsøker å tilegne seg informasjon».[180]

Terrorangrep mot olje- og gassinstallasjoner er ett av de scenarioene Forsvarets spesialstyrker trenes til å håndtere. Et lignende konsept kan vanskelig overføres til cyberdomenet. Kjennskap både til hvordan oljeriggen fungerer, systemene og konsekvensene av ulike tiltak for gjenoppretting av systemintegriteten besittes av selskapene selv. Forsvaret kan i første rekke bidra med kunnskap om trusselbildet og analyse av ondsinnet programvare.

5.2 Alvorlig skade, produksjonsstans og miljøutslipp forårsaket gjennom cyberdomenet

Den norske rollen som «pålitelig, ansvarlig og forutsigbar leverandør» av energi kan påvirkes gjennom cyberdomenet på flere ulike måter. Selv dersom anleggene opererer i lukkede nett er det flere eksempler på at ondsinnet programvare finner veien inn, noe som har ført til at oljebransjen også tenker på cybersikkerhet. Spesielt ett såkalt «cyberangrep» har fått vid omtale i pressen verden rundt. I 2012 ble oljeselskapet Saudi Aramco rammet av det en ondsinnet programvare kalt Shamoon. Programvaren slettet innholdet på om lag 30 000 datamaskiner, men påvirket ikke selve produksjonen. I 2010 brukte ingeniører 19 dager på å rense ondsinnet programvare med

[176] Helgesen, 2013
[177] Lunde og Thune m.fl., 2008:124
[178] Lunde og Thune m.fl., 2008:115
[179] Lunde, Leiv og Iselin Stensdal, 2013:90-91
[180] Næringslivets sikkerhetsråd, 2012:6

ukjent opphav fra systemene på en oljerigg. I dette tilfellet var ikke riggen satt i drift, dog den samme programvaren hadde rammet andre fartøyer fra oljebransjen i samme tidsrom.[181] Faktisk er flere tilfeller av produksjonsstans på grunn av ondsinnet programvare i petroleumssektoren forårsaket av de ansatte selv. Produksjonsstans har funnet sted på oljerigger som resultat av at ansatte uforvarende laster ned ondsinnet programvare i forbindelse med egen bruk av Internett, og overfører denne til riggens interne systemer.[182] Det er her viktig å understreke at det er en vesentlig forskjell mellom produksjonsstans forårsaket av et rettet angrep i regi av en ondsinnet aktør, og egenvalgt produksjonsstans, som i ovenfornevnte eksempler. Cybermaktprosjektet holder fast ved at det er svært krevende å gjennomføre et rettet angrep, også for å forårsake produksjonsstans eller miljøutslipp i petroleumsnæringen. Produksjonsstans kan imidlertid være både kostbart og ødeleggende for selskapet og Norge som leverandør.

En mulig utfordring for norske energi-, og miljøinteresser i fremtiden kan være å sørge for at etterslepet med sikkerhetshull i viktige systemer er så lite som mulig. I industrialiserte stater eksisterer det flere generasjoner med industrikontrollsystemer som aldri var tiltenkt å kobles opp mot et åpent nett med et globalt trusselbilde som dagens Internett. Mange slike systemer, både av eldre og nyere art, kobles imidlertid til Internett av praktiske grunner eller i uten at brukeren selv er klar over det – og kan teoretisk spenne seg fra en kaffeautomat til et kjernekraftverk. I forbindelse med Nasjonal Sikkerhetsmåned 2013 publiserte Dagbladet en egen spalte om IKT-sikkerhet i Norge. Her benyttet de blant annet søkemotoren Shodan, som søker opp alle typer enheter koblet på Internett, til å lete opp kontrollsystemer koblet opp mot Internett i Norge. Over en nokså kort tidsperiode fant de om lag 2500 slike systemer.[183]

Flere punkter taler for at dette er meget alvorlig. Mange av systemene oppdateres sjeldent og kan inneholde kjente sikkerhetshull som gjør de enklere å bryte seg inn. Andre er uten passordbeskyttelse, og dermed åpne for hvem som helst. Samtidig er det svært få av disse som styrer prosesser som kan gjøre skade på anlegget selv eller omgivelsene, ei heller at kontrollsystemet evner å påføre anlegget den skaden. I 2003 krasjet Slammer-ormen *ved en tilfeldighet* kontrollsystemet som overvåket kjølingssystemer, kjernetemperaturer og eksterne strålingssensorer ved et kjernekraftverk i Ohio. Analoge backupsystemer sørget her for at driften kunne fortsette som normalt, dog under noe økt arbeidsbelastning. [184] Personellet med ansvar for ivaretagelsen av cybersikkerheten ved anlegget var ikke klare over at systemet var tilgjengelig fra Internett, og at sårbarheten ormen brukte var tettet av Microsoft seks måneder tidligere.

En ofte sitert hendelse med konsekvenser for miljøet er utslippet av flere millioner liter kloakk i Maroochy Shire, Australia i 2001. Gjerningsmannen, Vitek Boden, arbeidet for et selskap som hadde installert industrielle kontrollsystemer for vannverket, og forårsaket utslippet fordi han hadde fått avslag på en jobbsøknad i kommunen. Han hadde derfor ikke bare gode kunnskaper

[181] Shauk, 2013a
[182] Shauk, 2013b
[183] Hillestad, Kongsli og Strømman, 2013
[184] Poulsen, 2003

om systemene, men også maskinvare tilgjengelig i tillegg til en spesialkabel han laget selv.[185] Flere millioner liter råkloakk forurenset parker, elver og landområder i det som best kan beskrives som et angrep fra en utro tjener med meget gode forkunnskaper om infrastrukturen.
I en kommentar til Dagbladets artikkel om åpent tilgjengelige kontrollsystemer sa NSMs Marie Moe at de for første gang ble varslet om slike av amerikanske myndigheter i 2011.[186] Siden har de mottatt en håndfull varsler, og håndtert disse. Det foreligger dermed ingen tall på hvor mange åpent tilgjengelige sårbare systemer som både har et skadepotensiale som det samtidig finnes en aktør med interesse og evne til å utnytte. Det er her viktig å understreke at varslene, som gjerne kommer fra andre lands myndigheter, omhandler systemer som ikke inngår i nasjonal kritisk infrastruktur og dermed faller utenfor NSMs primære ansvarsområde.

5.3 Smarte strømnett

Energieffektivisering ansees som ett viktig ledd for å oppnå en mer klimavennlig elektrisitetsforsyning.[187] Såkalte smarte strømnett ruller nå ut i Norge og EU og vil i fremtiden bidra til betydelige gevinster i form av energieffektivisering, men samtidig nye grenseflater opp mot sikkerhet ved å koble nasjonal kritisk infrastruktur sammen på Internett – og kanskje til en viss grad også med andre land.

Ifølge det norske smartgrid-senteret er smarte strømnett fremtidas kraftsystem som tar i bruk informasjons- og kommunikasjonsteknologi og nye måle- og styresystemer.[188] Hos kunden installeres det et automatisk målesystem (AMS) i sikringsskapet som kommuniserer med driftskontrollsystemene hos energiselskapene, og gjør det mulig å holde oversikt over strømforbruket for mer effektiv allokering. Norge er ett av lederlandene i de om lag 60 multinasjonale smart-grid prosjektene i Europa i dag.[189] Det langsiktige målet for en gruppe kraftselskaper er å knytte sammen strømnettene i hele Europa til et «supernett» slik at strøm leveres på den mest effektive måten. Norsk vannkraft kan spille en nøkkelrolle i å sikre stabilitet i strømtilførselen på supernettet, som er en nøkkelbrikke i EUs større plan om et 80-95 prosents kutt i klimagassutslipp innen 2050.[190]

Full innføring av AMS i Norge, og det mulige europeiske supernettet, ligger fortsatt flere år fremover i tid, og det er derfor knyttet stor usikkerhet til hva slags løsninger som vil tas i bruk. Det kan for eksempel følge nye utfordringer for personvernet med nye databaser over når vedkommende bruker strøm eller hva slags apparater som er i hjemmet. NVE har bedt Olje- og energidepartementet vurdere muligheten for å benytte en felles infrastruktur med Danmark og lagre norske kundeopplysninger der.[191] Dersom enhetene i hjemmet skal få lov å kommunisere tilbake til strømnettet åpnes og muligheten for å bruke dette som angrepsvektor, hvorpå koblinger

[185] Abrams og Weiss, 2008 & Crawford, 2006
[186] Hillestad, Sandli og Strømman, 2013
[187] St. Meld. 15 (2008-2009) S 63
[188] For mer informasjon, se http://smartgrids.no/
[189] Europakommisjonens Institutt for Energi og Transport (IET), 2012
[190] Eikeseth, 2013
[191] Zachariassen, 2013

opp mot både personvern og driftskontrollsystemer er viktige spørsmål.[192] Statnett finansierer ett professorat i fem år ved det nye nasjonale senteret for cyber- og informasjonssikkerhet ved Høgskolen i Gjøvik nettopp for å kunne møte slike utfordringer.[193]
Et annet sentralt spørsmål er i hvilken grad smarte strømnett er mer, eller mindre, motstandsdyktige mot cyberangrep? Hva slags ringvirkninger kan et angrep få, og hvordan håndterer man dette i en delt infrastruktur? Vil sikkerhetsnivået i andre land ha implikasjoner for norsk sikkerhet?

6 Internasjonal organisering

Stortingsmelding nr. 15 (2008-2009) *Interesser, ansvar og muligheter: Hovedlinjer i norsk utenrikspolitikk* skriver i klartekst at «den sentrale målsetningen i norsk utenrikspolitikk er å ivareta norske interesser.» Disse interessene blir i stor grad ivaretatt og promotert internasjonalt gjennom ulike organisasjoner som Norge enten er medlem av eller har et samarbeidsforhold med. Disse samarbeidsordningene er i all hovedsak globale (som FN), regionale (som Nato, EU, og NORDEFCO) eller bilaterale mellom Norge og andre stater. Med hensyn til cyberdomenet kan Norges kjerneinteresse beskrives som det å fritt kunne anvende domenet til egne formål. Dette vil innebære det å inneha en viss cybermakt: evnen til å i ytterste konsekvens kunne projisere makt i eller gjennom cyberdomenet.[194]

6.1 En «avgjørende interesse» for Norge

Norge «er et lite land, har en åpen økonomi, en økonomisk viktig og miljømessig sårbar kystlinje, strategisk sentrale nordområder og utfordrende naboskap med Russland»[195]. Gitt disse forutsetningene har det lenge vært en kjerneinteresse å opprettholde «en robust regional og internasjonal rettsorden og et sett av effektive globale institusjoner til å opprettholde og videreutvikle en slik orden.»[196] Lunde m.fl. går så langt som å hevde at Norge har en «ekstra dyp samfunnsmessig, økonomisk og sikkerhetsmessig avhengighet av en robust internasjonal orden» i forhold til andre land, og at det derfor er å regne som en «avgjørende interesse».[197] Mens det i dag kan synes selvsagt at Norge er en storforvalter av ressurser i både petroleums- og fiskerinæringen, er faktum at disse ressursene i stor grad har tilfalt staten som et resultat av at det eksister en internasjonal rettsorden som de fleste land respekterer. Lunde m.fl. peker på FNs Havrettskonvensjon av 1982 som avgjørende da den etablerer Norges rettigheter som kyststat. Norges promotering av den internasjonale rettsordenen kan ved første øyekast virke som et idealistisk rettet prosjekt, men kan altså like gjerne tolkes som klassisk realpolitikk.[198]

[192] Kirkenes, 2011
[193] Statnetts hjemmesider (1)
[194] Windvik m.fl., 2013
[195] Stortingsmelding nr. 15 (2008-2009) 17 Bidra til global organisering innrettet mot nåtidens og framtidens utfordringer
[196] Stortingsmelding nr. 15 (2008-2009) 11.4 *Norges utvidede interesser*
[197] Lunde m.fl., 2008:64
[198] Lunde m.fl., 2008:69-70

Windvik m.fl. hevder at cyberdomenet i langt større grad enn de fysiske domener er folkerettslig uregulert, og at nasjonalstater og koalisjoner av stater i mindre grad har monopol på cyberdomenets maktmidler. Cyberdomenet fremstår som et domene *sui generis*, da det på noen områder hverken er under nasjonal eller global suverenitet (som de globale allmenninger). Den internasjonale rettsordens grunnleggende prinsipp er den westfalske statlige suverenitet, et prinsipp det er et uttalt mål å opprettholde. Ettersom det er vanskeligere å markere yttergrensene for statssuvereniteten i cyberdomenet, vil eksisterende internasjonale lovverk bli utfordret. Det finnes ikke internasjonalt konsensus for hvordan man skal svare på denne utfordringen, og man kan si at det foregår en maktkamp i internasjonale fora mellom to relativt steile fronter. De fleste vestlige land arbeider for å fremme ytringsfrihet, demokratiske verdier og fri flyt av informasjon på Internett, og mener at dagens folkerettslige prinsipper også er dekkende for cyberdomenet. Dette synet deles nødvendigvis ikke av stater som Russland og Kina, som ønsker økt regulering av cyberdomenet og arbeider for mer nasjonal kontroll over domenet innenfor egne grenser (også i form av ytringsbegrensninger).[199]

I dette grunnleggende internasjonale spørsmålet om cyberdomenet og folkeretten sammenfaller Norges utstrakte arbeid for demokrati og ytringsfrihet med statens realpolitiske interesse av å støtte oppunder dagens internasjonale rettsorden. Det gjør det på mange måter til en enkel beslutning å fremme norske interesser internasjonalt. Dette vil derimot ikke alltid være tilfelle. Det kan tenkes at cyberdomenet vil bidra til å øke denne tendensen, gitt sin globale karakter, heller enn å minske den. Dilemmaer som dette kan skape blir diskutert videre i Kapittel 7 - Engasjement.[200]

Ettersom verden gjennom globalisering blir stadig mer «kompleks og uforutsigbar, konfliktnivået større, trusselbildet mer sammensatt, stormaktene flere, alliansene mer skiftende og norsk økonomi og velferd enda tettere innvevd i globale prosesser» blir det stadig viktigere å bli bedre til å fremme norske interesser gjennom aktiv bruk av det globale rettsordensapparatet.[201] For å opprettholde det internasjonale rettssystemets relevans, må nye utfordringer også integreres og løses innenfor systemet. Derfor er det en overgripende norsk interesse at cyber integreres i systemet og organisasjonene Norge ønsker skal styrkes i fremtiden. Norge deltar i en rekke ulike flernasjonale samarbeid, som i ulik grad og på ulike måter behandler cyberdomenet. De følgende seksjonene av dette kapittelet vil beskrive noen av de mest sentrale av disse, og fremhever norske interesser innenfor de ulike organisasjonene.

6.2 FN

Stortingsmelding nr. 15 (2008-2009) beskriver FN som selve fundamentet i dagens internasjonale organisering og for Norges globale politikk, og fremhever at det stadig blir viktigere at FN samler alle land til globalt samarbeid. «Samtidig er det viktig med fornyet fokus på hvordan og hvor

[199] Windvik m.fl., 2013
[200] Lunde m.fl., 2008:15-18
[201] Stortingsmelding nr. 15 (2008-2009) 11.4 *Norges utvidede interesser*

effektivt dagens internasjonale organisasjoner og konvensjoner tjener norske interesser, og hvordan Norge kan arbeide enda mer målrettet for å fremme interessene våre.»[202]

FN-pakten er en av de mest sentrale delene av det internasjonale lovverket, og Norge promoterer dens viktighet ved enhver anledning. En fundamental debatt, som ble presentert i Cybermakt-prosjektets første rapport, er hvorvidt anslag i cyberdomenet bryter med FNs maktforbud. Maktforbudet inngår i FN-paktens artikkel 2(4), som erklærer at alle medlemslandene skal avstå fra trusler eller brukt av makt mot andre staters territorielle integritet. Sjef Cyberforsvaret, Generalmajor Roar Sundseth, tolker dette som også gjeldende for offensive cyberoperasjoner: bruk av cybermakt mot andre nasjoner er med andre ord forbudt etter FN-pakten. Dette grunngis med at maktforbudet også dekker ikke-kinetiske virkemidler, og at en vurdering av intensjon og konsekvenser også her vil være sentralt for å vurdere om maktforbudet er brutt.[203]

Når cyberdomenet og FN nevnes i samme setning, er det ofte i forbindelse med den Internasjonale Telekommunikasjonsunionen (ITU). ITU er et spesialorgan under FN som er ansvarlig for koordinering av internasjonal telekommunikasjon, og ITU har i stor grad tatt ledelsen i å koordinere cybersikkerhet internasjonalt. Unionen leverer også trusselvurderinger til FNs generalsekretær hvert kvartal. ITU holder med jevne mellomrom internasjonale konferanser og toppmøter der verdens stater kommer sammen for å diskutere og forsøksvis bli enige om hvordan cyberdomenet skal reguleres, sikres og forvaltes. ITUs generalsekretær har uttalt at cyberkriminalitet er en av hans tre viktigste prioriteter. Som resultat av hans lansering av en global cybersikkerhetsagenda i 2007, ble en *Global Strategic Report* utgitt i 2008 som fokuserte på cybersikkerhet fra ulike perspektiver: lovverk, tekniske og prosessmekanismer, organisasjonsstrukturer, kapasitetsbygging og internasjonalt samarbeid. Fokus var i all hovedsak på beskyttelse av kritisk infrastruktur og cyberkriminalitet. Generalsekretæren har ved flere anledninger uttalt at han oppfordrer stater til å ikke benytte seg av cyberangrep, begrunnet med muligheten for eskalering til krise og krig som følge.[204]

Det økonomiske og sosiale rådet (ECOSOC) har også til en viss grad vært på banen, hovedsakelig i samarbeid med ITU, for å gi FN-landene større innsikt i de utfordringene som økt avhengighet av cyberdomenet skaper, identifisere *best practices* for cybersikkerhet, og for å utforske muligheter for globale aktiviteter i kampen mot økende cyberkriminalitet. ECOSOCs president, H.E. Lazarous Kapambwe, har uttalt at cybersikkerhet er en global utfordring som trenger en global løsning, og at FN gjennom sin unike globale posisjon kan stille med strategiske og analytiske kapabiliteter for å finne løsninger på utfordringene knyttet til cyberdomenet.[205]

Norge har vært en forkjemper for at internasjonale operasjoner må forankres med mandat fra FNs Sikkerhetsråd, og ønsker ikke å delta i operasjoner som ikke er legitimert i FN. Regjeringen har

[202] Stortingsmelding nr. 15 (2008-2009) 17.3 Norske hovedprioriteringer i reform av global organisering
[203] Windvik m.fl., 2013;
Sjef Cyberforsvaret, Oslo Militære Samfunn
[204] FNs nettsider (3);
Maurer, 2011
[205] FNs nettsider (3)

også uttalt at deltagelse i FNs fredsbevarende operasjoner er en prioritet, og at målet er å øke bidraget til disse operasjonene. Per 31. januar 2013 var de ti største bidragsyterne til FNs fredsbevarende styrker målt i personell Bangladesh, Pakistan, India, Ethiopia , Nigeria, Rwanda, Nepal, Jordan, Egypt og Ghana.[206] Hvor cyberresiliente er disse styrkene? Hvor stor fokus har cybersikkerhet i disse statenes respektive militære organisasjoner? Om Norge har som mål å øke samvirke med stater hvis cybersikkerhet er svak, bør man kanskje operere på en annen måte enn om man samvirker med likemenn, enten ved å ta ekstra forhåndsregler eller ved å støtte samarbeidspartnere med mål om å øke deres cybersikkerhet.

6.3 Nato

Stortingsmelding 15 (2008-2009) beskriver Nato som «Norges tyngste sikkerhetspolitiske forankring», «hjørnesteinen i norsk sikkerhetspolitikk» og en «bærebjelke i det internasjonale sikkerhetssystemet». Det presiseres at det fra norsk side ikke er noe motsetningsforhold mellom globalt multilateralt samarbeid i FN og medlemskap i Nato, og at arbeidet i de to organisasjonene kan sees som gjensidig forsterkende.[207] Stortingsmeldingen trekker frem Natos evne til omstilling som en viktig årsak til at organisasjonen fremdeles er relevant i dag. For at dette skal opprettholdes, må Nato fortsette å være omstillingsdyktig. En avgjørende karakteristikk i så måte er evnen til å ta innover seg dagens og fremtidens utfordringer, der cyberdomenet vil spille en viktig rolle. Nato har i de seneste årene lagt vekt på cyberdomenet i stadig økende grad. For Nato er det hovedsakelig cyberforsvar og økt resiliens mot cyberangrep som har vært i fokus, heller enn offensive cyberkapabiliteter. Det er et uttalt mål at cyberforsvar skal være en kjernekapabilitet for alliansen ettersom cyberangrep stadig er en reell trussel mot Nato.

Allied Command Transformation (ACT) har ansvar for Natos transformasjonsprosesser, herunder konseptutvikling og definering av kapabilitetskrav for fremtidens flernasjonale fellesoperasjoner, samt utdanning og trening for å gjøre alliansen og dens medlemmer i stand til å implementere disse konseptene og kapabilitetene. ACT har fokus på den teknologiske utviklingen, og hvordan denne påvirker Nato i fremtiden. ACTs *Futures*-arbeid fremhever at Nato-landene hittil har hatt det teknologiske overtaket i cyberdomenet, men at dette kan endre seg ettersom andre land vektlegger cyberteknologi i stadig økende grad. Nato har i de siste årene vært preget at av en høy grad av omstillingsaktivitet, for å gjøre alliansen relevant også i fremtiden. Nato lanserte på Lisboa-toppmøtet i 2010 et nytt strategisk konsept, der det fremheves at alliansens sikkerhet avhenger av at man klarer å beskytte Natos IKT-systemer på best mulig måte, så raskt som mulig. Nato vedtok året etter en revidert *policy* for cyberforsvar sammen med en såkalt handlingsplan. Disse beskriver nye krav til cyberforsvar, og definerer de politiske og operasjonelle mekanismene som utgjør Natos svar på cyberangrep. Med denne *policyen* ble cyberforsvar integrert i forsvarsplanleggingsprossessen på lik linje med andre kapabiliteter (under ledelse av *Defence Policy and Planning Comittee*). Det beskrives også hvordan Nato kan støtte allierte som ønsker

[206] FNs nettsider (4)
[207] Stortingsmelding nr. 15 (2008-2009) 17 Bidra til global organisering innrettet mot nåtidens og framtidens utfordringer

det i nasjonalt cyberforsvar, for å optimere informasjonsdeling og situasjonsforståelse, samarbeid og interoperabilitet.[208]

Natos internasjonale stab er fordelt på syv avdelinger (*divisions*), hvorav alle på en eller annen måte må ta hensyn til cyberdomenet, enten med tanke på forsvarsplanlegging, media og kommunikasjon, eller i Natos operasjoner. Størst fokus på dette domenet ligger dog i den nyeste avdelingen, Emerging Security Challenges Division (ESC), som ble opprettet i 2010. Cyberforsvar er ett av områdene som avdelingen legger særlig vekt på, sammen med terrorisme, masseødeleggesvåpen og energisikkerhet. ESC tar i all hovedsak for seg politisk-militære spørsmål, og mye av arbeidet fokuseres rundt strategiske analyser.[209] Det har også nylig blitt etablert ulike organer med ansvar for de tekniske aspektene ved Natos cyberressurser. Etter at Nato reformerte strukturen for de ulike byråene og deres ansvarsområder, ble Natos kommunikasjons- og informasjonsbyrå (NCIA) etablert. Byrået skal sørge for IT-tjenester for Nato generelt, samt støtte alliansen i anskaffelser av kommando- og kontrollsystemer, taktisk og strategisk kommunikasjons- og cyberforsvarssystemer.[210] Nato Computer Incident Response Capability (NCIRC) ble etablert i begynnelsen av 2012, med mål om å nå full operasjonell kapabilitet innen året var omme. Det har også blitt satt opp en Cyber Threat Awareness Cell som skal sørge for etterretningsdeling og forbedret situasjonsforståelse. NCIRC har ansvaret for å overvåke og beskytte Natos egne nettverk, en omfattende oppgave.[211]

Det har vært tunge debatter innad i Nato om hvorvidt et cyberangrep skal utløse artikkel 5, artikkelen i Atlanterhavspakten som omhandler retten til kollektivt selvforsvar. Daværende forsvarsminister Espen Barth Eide har uttalt at Norges offisielle innspill til Nato er at dataangrepet må gå over i den fysiske verden for at Artikkel 5 skal utløses, «[a]t inntrengningen skjer via dataanlegget, men at konsekvensene påvirker liv og helse, eller skaper store ødeleggelser i det fysiske rom.» Han fremhever dog at Nato kan involveres med alminnelig hjemmel i folkeretten.[212] FN-paktens artikkel 2(4) erklærer at medlemslandene skal avstå fra trusler eller bruk av makt mot andre staters territorielle integritet, og Atlanterhavspaktens artikkel 4 gir anledning til at en truet stat kan rådslå med sine allierte.[213]

Stortingsmelding 15 (2008-2009) predikerer at Nato sannsynligvis vil fortsette å utvikle seg mot å (for)bli en «kollektiv sikkerhetsorganisasjon med ansvar både for å bidra til stabilitet, sikkerhet og forsvar av menneskerettigheter i områder langt fra medlemslandenes territorium, og for forsvaret av medlemslandenes territorium», og påpeker at dette vil stille større krav til medlemslandene «ikke minst når det gjelder aktiv deltakelse og byrdefordeling i forbindelse med Nato-operasjoner i konfliktområder rundt om i verden.»[214] Den økonomiske krisen i Europa har

[208] Natos nettsider (2)
[209] Natos nettsider (3)
[210] Natos nettsider (4)
Natos nettsider (5)
[211] Natos nettsider (2)
[212] Espen Barth Eide i Teknisk Ukeblad
[213] Windvik m.fl., 2013:46
[214] Stortingsmeldig 15 (2008-2009) 17.6 *Sikkerhet*

skapt et enda større press på europeiske forsvarsbudsjetter, og Norge har vært det eneste landet med økning i budsjettet. Teorier om kollektive goder så vel som historisk praksis viser at såkalt «*freeloading*» er et utbredt fenomen, og at det er naturlig at små land bidrar relativt mindre enn store land til alliansens forsvarsutgifter.[215] Når det kommet til cyberdomenet kan det tenkes å være en mulighet for Norge som småstat til å få økt innflytelse gjennom å bære en større del av byrden enn forventet. Sjef Cyberforsvaret, Generalmajor Sundseth, sa i Oslo Militære Samfunn 18. februar 2013 at Norge er «en nasjon som har alle forutsetninger for å være god på dette nye området. Vi er en teknologisk avansert nasjon, og vi har teknologi, kompetanse og kunnskap nok til å trygge oss for fremtiden – såfremt vi er villige til å prioritere og forplikte ressurser til det.»[216]

Det levner liten tvil om at Natos lederskap er opptatt av cyberdomenet, og at det kommer til å forbli et fokusområde i årene som kommer. Generalsekretær Anders Fogh Rasmussen fremhever jevnlig at cyberdomenet blir stadig viktigere for alliansens sikkerhet, og at medlemslandene må satse på å bedre sine cyberforsvarskapabiliteter. Daværende Supreme Allied Commander (SACEUR) og leder for US European Command, Admiral Stavridis, skrev i april 2013 at cybersikkerhet bør være ett av tre satsningsområder for Nato i de kommende årene. Han karakteriserer cyberdomenet som et domene der trusselen er høy og beredskapsnivået lavt sammenlignet med alliansens andre virksomhetsområder. Han viser til en rekke mer eller mindre konkrete tiltak han ser som nødvendige for de neste årene, som økt informasjonsdeling mellom allierte med hensyn til både etterretning, teknikker og prosedyrer for cyberforsvar; utvikling av Natos evne til å motstå cyberangrep både på alliansenivå og nedover i kommandostrukturen; og styrking av det Nato-akkrediterte Cooperative Cyber Defence Centre of Excellence (CCD COE) i Tallinn, Estland. Han tar også til orde for å definere «cyberangrep» i konteksten av Nato-traktatens artikkel 5, som setter rammene for hvilke angrep som kan regnes som et angrep på alliansen og utløse selvforsvarsretten.[217]

Selv om mye som gjøres i Nato er på politisk og militærstrategisk nivå må man ikke glemme operasjonsaspektet. Norge kommer til å delta i Nato-operasjoner også i fremtiden, og cyberforsvar vil bli et stadig viktigere operasjonelt aspekt. I 2008 ble for eksempel norske styrkers lukkede militære nett angrepet i Afghanistan, sannsynligvis av utenlandsk etterretning. Daværende Sjef for Forsvarets Ingeniørhøgskole, Oberstløytnant Roger Johnsen, sa til NRK at «Vi antar at formålet var kartlegging, innsamling av etterretning og om mulig ødelegge systemene i en kritisk situasjon.» For at man skal kunne utføre operasjoner på effektivt og suksessfullt vis, må man inneha resiliente og forsvarbare cyberressurser. I alliansesammenheng vil det være i Norges interesse å vise seg som en stat som tar cyberdomenet på alvor og kan vise til sikre og forsvarbare systemer.[218]

For at en koalisjons- eller alliansestyrke skal kunne operere effektivt og sikkert sammen i cyberdomenet, vil en høy grad av interoperabilitet være en fordel, om ikke en forutsetning. Nato

[215] Kvalvik m.fl., 2013 (kommende)
[216] Sjef Cyberforsvaret i Oslo Militære Samfunn
[217] Nato ACOs nettsider
[218] NRKs nettsider

beskriver interoperabilitet som bestemmelser som muliggjør og sørger for samarbeid, og Natos STANAG AAP-6 definerer det i mer detalj som «systemer, enheter og styrkers evne til å tilby tjenester til og akseptere tjenester fra andre systemer, enheter og styrker, og til å bruke disse utvekslede tjenestene til å muliggjøre det å operere effektivt sammen» [forfatterens oversettelse]. For å oppnå interoperabilitet i operasjoner, må man arbeide for felles utvikling og tilpasning sammen med sine allierte, innenfor organisasjoner man er en del av. For Norge betyr dette at om man ønsker å delta i Nato-operasjoner, bør hovedvekten av interoperabilitetsbyggingen gjøres innenfor denne rammen.[219] CCD COE i Tallinn, Estland støtter opp under Natos arbeid for økt interoperabilitet i cyberdomenet, og har som en av sine hovedmålsetninger å arbeide for en økning i sikker interoperabilitet i NNEC-miljøet (*Nato Network Enabled Capability*). Norge er på nåværende tidspunkt ikke medlem av senteret, som har 11 Nato-land som sponsorer.[220] Det er imidlertid ikke til å stikke under en stol at mens interoperabilitet som regel blir fremhevet som et gode, kan det også innebære høye kostnader, en viktig faktor i usikre økonomiske tider. [221]

For å kunne gjennomføre operasjoner med suksess må man i tillegg øve og trene sammen med dem man skal operere sammen med, også på cyberforsvar. Fjorårets Nato Crisis Management Exercise ble arrangert i parallell med en egen cyberøvelse, Cyber Coalition. Målet var å øve Natos prosedyrer for å håndtere cyberangrep mot kritisk infrastruktur. Norge deltok i denne, og fikk blant annet øvet på samarbeidet mellom Forsvaret, Nasjonal Sikkerhetsmyndighet, departementer og andre sivile virksomheter. Dette er et eksempel på øving med allierte som samtidig utfordrer våre egne nasjonale samhandlingsprosedyrer i cyberdomenet.[222]

6.4 EU

EU har siden opprettelsen av Den europeiske kull- og stålunionen av 1952 vokst til å bli en politisk og økonomisk union som får en stadig større global sikkerhetspolitisk rolle. Unionen har posisjonert seg som en sentral forkjemper for flernasjonale løsninger og en robust global rettsorden, en interesse som i all hovedsak overlapper med Norges egne interesser. En mer utfordrende faktor hva gjelder EUs globale rolle er at unionen i økende grad fremstår som Europas talsmann på globale og regionale spørsmål. [223] Her er det rom for at Norges særegne interesser, kanskje spesielt med tanke på kystnæringer og nordområdene, ikke vil få det globale fokus som man kunne ønske eller at fullstendig motstridende interesser blir promotert.

På grunn av dette vil det være å regne som en sentral norsk interesse «å ha en velfungerende tilknytningsform som sikrer et godt samarbeid med de europeiske institusjonene og medlemslandene» for å være i inngrep med EUs prosesser. Selv om Norge ikke er medlem av EU, samarbeides det med EU på stadig nye områder, både innenfor og utenfor det rent

[219] Norheim-Martinsen, 2009:9;
For mer om interoperabilitet i Nato, se NATO Backgrounder for Interoperability in Joint Operations, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120116_interoperability-en.pdf
[220] CCD COEs nettsider
[221] Aabakken, 2002
[222] NSMs kvartalsrapport for 4. kvartal, 2012:5
[223] Stortingsmelding 15 (2008-2009);
Regjeringens nettsider (1)

forsvarsrelaterte. Mye av samarbeidet blir gjort gjennom EØS-avtalen og Schengen-avtalen, men også ved økt deltagelse i EUs utenriks- og forsvarspolitiske samarbeid. Dette er viktig på generelt grunnlag, men også spesielt med tanke på cyberdomenet. EUs medlemsland er blant våre nærmeste allierte og geografiske naboer, og politikk som utvikles i EU vil i høy grad påvirke Norge og norske interesser på en eller annen måte. Cyberdomenet er et ungt militært domene, og et nytt satsingsfelt for utvikling av militære kapabiliteter. Med dette i tankene kan cyber tenkes å være et felt der det er enda viktigere å være i inngripen med de ulike EU-prosessene, ettersom mye av definisjonsmakten for militære krav, kapasiteter og konsepter sannsynligvis vil ligge i det EU-medlemmene blir enige om gjennom deltagelse i nettopp disse prosessene.

Norge underskrev en samarbeidsavtale med European Defence Agency (EDA) i 2006, som første ikke-medlemsland, og benytter seg aktivt av mulighetene for deltagelse denne avtalen gir.[224] Cyberforsvar er beskrevet som en av ti hovedprioriteringer i EDAs plan for kapabilitetsutvikling, det overordnede strategiske verktøyet for EDA og driveren for alle EDAs arbeidsområder. Høsten 2011 etablerte EDA en ny prosjektgruppe for cyberforsvar kalt EDA Project Team Cyber Defence (PT CD). På nåværende tidspunkt deltar 23 av EUs medlemsland i gruppen, og Norge og Sveits er også inviterte på tross av manglende EU-medlemskap. PT CDs portefølje er omfattende, og innebærer kartlegging av kapabiliteter for cyberforsvar og cyberetterretning, trening og øvelsesrelaterte aktiviteter, samt en rekke konseptuelle arbeid og studier. EUs kapabilitetsdirektør beskriver denne gruppen som en viktig støtte til EDA, og hevder at fremgangen på feltet i EU-sammenheng har vært stor allerede.[225]

Europakommisjonen og EUs høyrepresentant for utenrikssaker og sikkerhetspolitikk lanserte i februar 2013 en felles strategi for cybersikkerhet. Strategien promoterer et åpent og fritt internett, og fremhever verdier som demokrati og frihet. Dette sammenfaller med politikken som er fremmet av Norge og de fleste andre vestlige land i ITU. Strategien er også tydelig på at ambisjonen er å utforme en felles cyberpolitikk for EUs medlemsland, og det vies mye plass til sikkerhets- og forsvarspolitiske spørsmål. Et positivt aspekt fra norsk perspektiv er at koordinering med Nato står sterkt, spesielt innenfor cyberforsvar. Dette er absolutt i Norges interesse, som Nato-medlem som står utenfor EU.[226]

Norges deltakelse i EUs sivile og militære krisehåndteringsoperasjoner ble beskrevet av regjeringen Stoltenberg som et viktig element i det praktiske samarbeidet med EU. Forutsatt mandat fra FN vil Norge bidra aktivt til EU-ledede operasjoner «innenfor rammen av ikke-medlemskapet og den brede enigheten på Stortinget».[227] EUs militære operasjoner vil i all hovedsak være flernasjonale, og EUs militære stab (EUMS) har identifisert dette som en faktor som kan gjøre en EU-styrke mer sårbar for cybertrusler. For å redusere denne sårbarheten vektlegger EUMS økt koordinasjon mellom deltagende staters nasjonale cyberforsvarskapabiliteter. Dette fokuset søkes å effektiviseres gjennom EDAs arbeid med

[224] Regjeringens nettsider (2)
[225] EDAs nettsider (1), (2)
[226] EUs cyberstrategi
[227] Stortingsmelding 15 (2008-2009) 17.6 *Sikkerhet*

kartlegging og utvikling av cyberforsvarskapabiliteter i og på tvers av EUs medlemsland. EU prøver med andre ord å redusere en flernasjonal EU-styrkes cybersårbarheter ved å øke interoperabiliteten mellom deltagerstatene. Dette arbeidet følger i stor grad modellen EU har benyttet for å søke interoperabilitet i de andre militære domenene. EU har i stor grad unngått å identifisere egne standarder for interoperabilitet, og har heller tilpasset sine definisjoner til Natos allerede eksisterende STANAG på området. Det er i Norges interesse at EU opprettholder sin intensjon om å «dekonflikte» med Nato, ettersom man har uttalt at det er ønskelig at Norge deltar i EU-ledede operasjoner. Skal man delta i operasjoner bør det gjøres på mest mulig effektivt vis, og da er interoperabilitet viktig.[228]

Det er også viktig at man øver sammen med de statene man skal operere sammen med. Det foreligger for øyeblikket planer om et flernasjonalt samarbeidsprosjekt for trening og øvelser som Nederland, Estland og Østerrike har tatt initiativ til. Tanken bak dette prosjektet er å muliggjøre nødvendig cybertrening, -utdanning og –øving ved at man samarbeider og dermed får økt utbytte og reduserte kostnader (kalt «pooling and sharing» i EU-terminologi). Dette arbeidet vil utvikles gjennom EDA. Det europeiske byrå for nett- og informasjonssikkerhet (ENISA) har de siste årene arrangert øvelser for krisehåndtering i cyberdomenet, der Norge har vært involvert. ENISA har i EU ansvar for å øke resiliensen og motstandskraften til Europas kritiske infrastruktur og nettverk. De utvikler også råd og anbefalinger for informasjonssikkerhet for EU-institusjonene, medlemsstatene, samt Europas private sektor og innbyggere, og støtter medlemslandenes arbeid med å implementere EUs lovverk på området.[229] NorCERT deltok for eksempel i øvelsen Cyber Europe, der 300 fagfolk i 25 europeiske land jobbet sammen for å bekjempe et massivs simulert tjenestenektangrep. Dette er en positiv utvikling for Norges del, at man er en del av EUs krisehåndteringsøvelser, all den tid cyberdomenet ikke er et domene som tar hensyn til hvilke organisasjoner man har medlemsskap i. På denne måten får vi tilgang til ekspertise på området fra våre allierte og naboer, samt får delta i utvikling av prosedyrer og prosesser som vi vil bli påvirket av på senere tidspunkt.[230]

6.5 OSSE

Organisasjonen for sikkerhet og samarbeid i Europa (OSSE) har en bred tilnærming til sikkerhet, og arbeider for politisk dialog og samarbeid for å forebygge og håndtere konflikter i regionen. Stortingsmelding nr. 15 (2008-2009) beskriver OSSE som et «naturlig forum for drøftelser av de felles sikkerhetspolitiske utfordringene deltakerlandene står overfor,» og fremhever det som viktig at arbeidet videreføres.[231]

Når det kommer til cyberdomenet er OSSEs fokus hovedsakelig på å bekjempe cyberkriminalitet og bruk av Internett til terrorformål. OSSEs Action Against Terrorism Unit og Strategic Police Matters Unit driver opplysningsarbeid og trening i kampen mot ulike former for cyberrelatert

[228] Norheim-Martinsen, 2009:11-10
[229] ENISAs nettsider
[230] NSMs kvartalsrapport for 4. kvartal 2012:5.
[231] Stortingsmelding 15 (2008-2009) 6.7 *Europarådet og OSSE*;
Regjeringens nettsider (3)

kriminalitet, med hovedfokus på opplæring i øst-europeiske land. En viktig målsetning for OSSE, som er på linje med Norges politikk på området, er at arbeidet som gjøres for å sikre cyberdomenet ikke går på akkord med fundamentale prinsipper som ytringsfrihet og møtefrihet på Internett.[232]

6.6 Europarådet

Cyberkriminalitet er også å finne høyt på agendaen til Europarådet, som i følge regjeringen har «en sentral rolle i arbeidet for å sikre respekt for menneskerettigheter, demokrati og rettsstatsprinsipper i vår del av verden og er det fremste forumet for regelverks- og standardutvikling på disse områdene i Europa.»[233]

Europarådets konvensjon om cyberkriminalitet, også kjent som Budapest-konvensjonen, er hittil den eneste internasjonale lovlig bindende traktaten om cyberkriminalitet. Konvensjonen ble åpnet for signering i 2001, og trådte i kraft i juli 2004. Hensikten til Budapest-konvensjonen er i følge Europarådet å beskytte frihet, sikkerhet og menneskerettigheter på nettet. Konvensjonen tilbyr blant annet et rammeverk for hvordan myndighetene kan utvikle nasjonal cyberlovgivning, og er åpen for signering også for stater utenfor Europa. Hittil har 40 stater ratifisert avtalen. I 2013 ble en tilleggsprotokoll som regulerer handlinger av rasistisk og xenofobisk[234] art gjennom datasystemer lagt til konvensjonen, som et ledd i Europarådets menneskerettighetsarbeid.[235]

6.7 NORDEFCO

Nordisk forsvarssamarbeid skjer gjennom NORDEFCO, et rammeverk for samarbeid som ble etablert i 2009. Forsvarsdepartementet skriver på sine nettsider at «[e]t hovedmål for NORDEFCO er å bevare og videreutvikle landenes militære kapabiliteter og operative evne gjennom kostnadseffektivt samarbeid.»[236] Nordisk samarbeid og politisk dialog er viktig for Norge, og NORDEFCO sees også på som en mulighet til å utvikle løsninger sett i sammenheng med europeiske samarbeidsspørsmål.[237]

Cyberforsvar er valgt som ett av tolv fokusområder for det nordiske forsvarssamarbeidet, innenfor «Samarbeidsområde Kapabiliteter» (COPA CAPA). Disse fokusområdene er valgt ut på bakgrunn av at man mener at det innenfor disse er mest å tjene på å samarbeide med de andre nordiske landene. Hovedmålet for samarbeidet på dette området er å undersøke hvilke økonomiske og operasjonelle fordeler man kan få ved økt nordisk informasjonsdeling i cyberdomenet. Fokus ligger på økt situasjonsforståelse og varsling av trusler gjennom militære CERT-samarbeid, og cyberøvelser i nordisk setting. Det vil absolutt være i Norges interesse å oppnå økonomiske og operasjonelle fordeler ved nordisk samarbeid, spesielt siden det allerede er en politisk målsetning.

---

[232] OSSEs nettsider
[233] Regjeringens nettsider (5)
[234] Xenofobi er termen som benyttes for fremmedfrykt. (xenos (fremmed) og phobos (frykt))
[235] Europarådets nettsider (1), (2), (3)
[236] Regjeringens nettsider (4);
NORDEFCOs nettsider
[237] Stortingsmelding 15 (2008-2009)

Da dette prosjektet er i en relativt tidlig fase er det vanskelig å si hvor lønnsomt og effektivt det vil være.

6.8 Så hvem bør man samarbeide med?

Norge samarbeider som vist med ulike stater, på ulike måter, i ulike fora. Men hvordan velger man partnere og samarbeidsformer? Når det kommer til cyberdomenet er et dilemma hvorvidt man bør fokusere på å samarbeide med stater som er fysisk nære, med stater som er fysisk fjerne, eller begge deler. Med stater som er fysisk nære deler man ofte felles kultur og historie, som kan gjøre selve samarbeidet enklere å gjennomføre. Selv om cyberdomenet hovedsakelig er virtuelt, og man med enkelhet kan kommunisere med mennesker på den andre siden av kloden, finnes også den fysiske delen av domenet, som blant annet består av infrastrukturen som datatrafikken beveger seg gjennom. Denne krysser grenser, og i vår egen region er for eksempel Sverige et land der mye av datatrafikken fra området passerer, inkludert trafikk til og fra Russland. Denne typen kontroll og innsyn i trafikken i regionen kan være av strategisk betydning, og kan gjøre det attraktivt for USA så vel som Norge å samarbeide med Sverige. Norge er Nato-medlem, og ser på USA som den viktigste allierte, mens Sverige av historiske grunner er nøytralt. Sverige er derimot med i EU, der Norge står utenfor. Selv om de to organisasjonene har de aller fleste medlemmene til felles, og har som målsetning å samarbeide og «dekonflikte» der det er mulig, finnes det fremdeles punkter som skaper gnisninger. Mens Nato er en forsvarsallianse, har EU et langt bredere politisk mandat, noe som gjør at EU også behandler de sivile aspektene ved cyberdomenet. Det kan tenker at EU vil nå konsensus rundt cyberrelaterte løsninger i det sivile samfunnet som siden får konsekvenser for forsvarssektoren, noe som tydeliggjør viktigheten ved å også være i inngripen med EUs politiske prosesser. Man kan ikke forvente at det i fremtiden alltid vil være Nato som setter standarden, og EU som deretter «dekonflikter» sine handlinger.

En sentral utfordring knyttet til flernasjonalt samarbeid er informasjonsdeling, et felt der cyberdomenet er i sentrum. Det blir på mange møter et motsetningsforhold mellom ønsket om å dele informasjon om trusler og sårbarheter for å gjøre «fellesskapet» sikrere, og ønsket om å holde egne kapasiteter, kapabiliteter og sårbarheter hemmelige. Informasjonsdeling, spesielt om et så sensitivt felt som cyberdomenet, er vanskelig selv innad i en organisasjon – når man samarbeider med partnere utenfor de etablerte fellesskapene vil dette blir stadig mer utfordrende. Norge har lang tradisjon med å promotere internasjonalt samarbeid, og det er sannsynlig at dette vil fortsette også i fremtiden. Derfor er det viktig at Norge tar innover seg både muligheter og utfordringer som cyberdomenet bringer med seg, med tanke på fremtidens internasjonale og regionale samarbeid i cyberdomenet.

7 Engasjement

Norsk engasjementspolitikk inkluderer i stort bistand, humanitær politikk, fred og forsoning, og arbeid for menneskerettigheter og demokrati, i følge Stortingsmelding nr. 15 (2008-2009) *Interesser, ansvar og muligheter: Hovedlinjer i norsk utenrikspolitikk*. Begrepet «engasjementspolitikk» ble lansert av historikeren Rolf Tamnes, og han poengterer at selv om engasjementspolitikk bærer i seg en uegennyttig karakter er ingen utenrikspolitikk «genuint

uegennyttig». For en småstat som Norge er det naturlig å søke å tjene både idealer og interesser gjennom engasjementspolitikken.[238] Den norske engasjementspolitikken har historisk vært basert på «ønsket om å bidra til et bedre liv for mennesker rundt om i verden», men på grunn av globalisering og geopolitiske endringer bidrar også politikken til å realisere mål som er i norsk interesse.[239] Statsviter Lene Kristoffersen skriver at den offisielle bruken av begrepet «engasjementspolitikk» gradvis har endret dets meningsinnhold, og viser til daværende utenriksminister Jonas Gahr Støres beskrivelse av engasjementspolitikk i forbindelse med nordområdestrategien av 2007. Han uttaler at Norge søker å bygge nære bånd til og felles interesser med Russland, Nato og EU for å unngå at konflikter utvikles. «Det er dette som er engasjementspolitikk,» slår han fast. Kristoffersen peker på at engasjementspolitikk med dette trekkes i en mer egennyttig retning enn det som før har vært tradisjon i Norge.[240] Lunde m.fl. legger til at engasjementspolitikken er «noe *mer* enn et mål om å bidra til å redusere fattigdom, skape fred og bygge demokratier i andre land. Det handler også om å skape det nødvendige grunnlaget for effektiv global styring.»[241]

Globalisering er definert som prosessen der selskaper eller andre organisasjoner utvikler internasjonal påvirkning eller begynner å operere på internasjonal skala.[242] Sosialantropologen Thomas Hylland Eriksen peker på tre dimensjoner som har drevet globaliseringen fremover de siste par-tre tiårene: økt handel og transnasjonal økonomisk aktivitet, økte spenninger mellom (og innen) adskilte kulturelle eller etniske grupper på grunn av intensivert gjensidig eksponering, og fremveksten av raskere og tettere kommunikasjonsnettverk, hovedsakelig ved fremveksten av Internett. Disse tre dimensjonene påvirker Norges utenrikspolitiske interesser på ulike, men sammenvevde måter, og får konsekvenser for norsk engasjementspolitikk.[243]

Med globaliseringen kommer nye utfordringer, og en av disse er en global maktforskyvning. Utenriksminister Espen Barth Eide skriver i 2013 at vi må «tegne våre mentale kart på nytt», siden sikkerhetspolitikk ikke lenger bare dreier seg om forholdet mellom øst og vest, og utviklingspolitikk ikke lenger bare skjer fra nord til sør. Leira og Sending fremhever to viktige trender for nær fremtid: regionalisering og bilateralisering, mens utenriksminister Barth Eide spør seg om fremtiden vil bringe en multipolar eller non-polar verden. Med andre ord må partene i fremtiden prioritere hvilke saker og hvilke geografiske regioner man velger å fokusere engasjementet sitt i større grad enn det Norge har gjort hittil, et poeng Lunde m.fl. fremhever som en av sine hovedkonklusjoner. Denne maktforskyvningen og behovet for prioriteringer bringer opp spørsmål rundt en av engasjementspolitikkens viktigste aktører, nemlig FN. FN gjenspeiler med sitt Sikkerhetsråd med permanente medlemmer med vetorett det «gamle verdenskartet», og mange hevder at FN må reformeres for å gi organisasjonen ny relevans. Som nevnt i Kapittel 6 – Internasjonal organisering, er Norge avhengig av internasjonal orden og at FN-systemet

[238] Kristoffersen, 2009
[239] Stortingsmelding 15 (2008-2009), 11.4 *Norges utvidede interesser*
[240] Kristoffersen, 2009: 10
[241] Lunde og Thune, 2008: 154-155
[242] Oxford dictionaries, *globalization*
[243] Eriksen, 2008

respekteres. Lunde og Thune hevder derfor at Norge har «mye å tjene på reformer av FN», nettopp for å gjøre FN relevant også for fremtiden.

Norge er verdens femte største leverandør av økonomiske ressurser til FN-systemet, med totalt 5 milliarder hvert år, og har derfor større innflytelse enn man kunne forvente av et lite land på utkanten av Europa. Dette tolkes av Leira og Sending som et forsøk på «å bruke norsk økonomisk makt for å styrke global styring innen former som Norge er komfortabel med.»[244] Thune m.fl. beskriver i tillegg Norge som en av verdens mest sentrale leverandører av fredsdiplomati, og hevder at norske aktører har vært involvert i forsøk på å finne fredelige løsninger i «de fleste av verdens viktigste konflikter etter år 2000». Dette såkalte fredsdiplomatiet tar mange ulike former, fra rollen som megler i en offisiell fredsprosess til roller fullstendig utenfor det internasjonale rampelyset. Mens noen stater har som praksis å annonsere sin deltagelse og sine roller i ulike prosesser til det internasjonale samfunnet, har Norge i stor grad operert uten å flagge konkret deltagelse. Lunde m.fl. hevder videre at Norges største merkevare i fredspolitikken er nettopp *fortrolighet*. Mens cyberdomenet kanskje ikke er det man intuitivt forbinder med freds- og forsoningsarbeid kommer det i denne sammenheng frem som en viktig forutsetning for suksess, i form av godt utviklet cybersikkerhet. Skal Norge fortsette å være en fortrolig partner i sårbare fredsprosesser, må partene kunne stole på at Norge har god nok cybersikkerhet til at sensitiv informasjon om både partene selv og prosessen vil forbli fortrolig – man må vise at man klarer å holde på andres hemmeligheter. Det at man deltar aktivt i ulike fredsprosesser er nok også en faktor som vil gjøre Norge til et mer attraktivt etterretningsmål, spesielt blant de som har interesser i de til enhver tid pågående prosesser. Skulle norske systemer bli offer for informasjonsuthenting og lekkasjer om pågående fredsforhandlinger vil det sitte langt inne å la Norge få nye, viktige roller i fremtidige prosesser, og det vil være vanskeligere å få parter i en konflikt til å stole på at Norge vil kunne beskytte deres informasjon. Med andre ord kan dårlig cybersikkerhet skade Norges merkevare og dermed Norges posisjon som en sentral aktør innen internasjonalt fredsdiplomati. Cybermakt i denne sammenheng vil derfor være å demonstrere at man tar Internetts sårbarheter og utfordringer på alvor, og på den måten få større betydning innen internasjonalt fredsdiplomati enn landets størrelse skulle tilsi. I ytterste konsekvens kan man tenke seg at Norge ikke bare sørger for egen cybersikkerhet til bruk i fredsdiplomatiet, men også støtter andre nasjoner som ønsker det samme, kanskje ved å fasilitere beskyttede arenaer i på Internett?

Siden Norge er en småstat i FN-systemet, har man valgt å bruke sin innflytelse i FNs underorganer, der man i større grad har innflytelse på bakgrunn av økonomiske bidrag heller enn makt i verden. Norsk engasjementspolitikk er i stor grad fokusert på arbeid for menneskerettigheter, og Norge søkte derfor i 2009 å bli valgt inn i FNs Menneskerettighetsråd for perioden 2009-2012.[245] Her har Norge promotert ytringsfrihet på Internett, og argumentert for at de samme rettighetene til ytring som mennesker har «*offline*», inkludert retten til å søke informasjon, og til å møtes og samles, skal beskyttes også på Internett. Videre har Norge argumentert for så få restriksjoner som mulig på informasjonsflyten på nettet, og at alle slike

[244] Leira og Sending, 2013:31
[245] Lunde m.fl., 2008

restriksjoner må være i overensstemmelse med internasjonale menneskerettigheter. Ytringsfrihet anses som å gå hånd i hånd med personvern på Internett. Datatilsynet beskriver personvern som «retten til et privatliv og retten til å bestemme over egne personopplysninger», og brudd på retten til privatliv ved bruk av cyberdomenet står stikk i strid med prinsippene om ytrings- og forsamlingsfrihet. Denne debatten har fått fornyet oppmerksomhet i forbindelse med nylige lekkasjer om det amerikanske NSAs overvåkning på nett.[246] Norge har også ved flere anledninger uttalt at det er viktig å sikre et velfungerende og åpent Internett, og arbeider i den Internasjonale Teleunionen for ytringsfrihet og mot sensur av såkalt «innhold» på Internett. Interessene Norge fronter i FN-systemet stemmer overens med arbeidet Norge gjør gjennom engasjementspolitikken for menneskerettigheter og demokrati på områder som ikke berører cyberdomenet direkte.[247]

Stortingsmelding 15 (2008-2009) påpeker at «[d]en globale kommunikasjonsrevolusjonen bringer verden inn i norske stuer og øker nordmenns behov for å være respektable globale borgere, bidra til å begrense menneskelig lidelse og til å arbeide i bedrifter som realiserer viktige verdier (og ikke bryter dem ned). Den driver menneskerettigheter og ytringsfrihet stadig nærmere kjernen av norske interesser, i betydningen politiske verdier som konstituerer Norge som sivilisert samfunn.»[248] Mens man tidligere kunne skjule menneskerettighetsbrudd internt i en stat i mye større grad, har fremveksten av informasjonsteknologi, og spesielt Internett, ikke bare gjort verden «mindre» men også stater mer gjennomsiktige. Det er i dag mye vanskeligere å holde brudd på menneskerettighetene «innenriks», og man ser for eksempel fra den arabiske våren at overgrep blir filmet med smarttelefoner og publisert på Youtube umiddelbart. Internett muliggjør sivilsamfunnet og andre staters påtaling av menneskerettighetsbrudd på tvers av landegrenser, nærmest i sanntid. Lunde og Thune beskriver den norske tradisjonen for at myndighetene samarbeider med ikke-statlige organisasjoner, kommersielle selskaper og aktivistgrupper, en tradisjon som synes å være nyttig å bygge videre på i cyberdomenet. På denne måten kan man i engasjementspolitikken på mest effektivt vis arbeide for ytringsfrihet og andre menneskerettigheter både *i* cyberdomenet, og *ved hjelp av* cyberdomenet.

Stortingsmelding 15 (2008-2009) fremhever videre at «[e]t omfattende engasjement i FNs og Verdensbankens utviklingsagenda fremmer uegennyttige mål, men bidrar også til å videreutvikle globale styringsorganer av betydning for Norge, og styrker Norges omdømme blant mange land som etter hvert får større tyngde i internasjonal politikk.»[249] I følge Verdensbanken er teknologisk fremgang en viktig driver for økonomisk utvikling, og den arbeider gjennom en rekke prosjekter i utviklingsland for å «stimulere bærekraftig økonomisk vekst, forbedre tjenestelevering og fremme godt styresett og sosial ansvarlighet» [forfatterens oversettelse]. Verdensbanken har vært involvert i over 100 prosjekter for å støtte utviklingen av IKT i land som Afghanistan, Ghana og Rwanda, for å oppnå klassiske engasjementspolitiske mål som utbedring av helsesektoren, skole- og utdanningssystemer og befolkningens mulighet for politisk deltagelse.[250]

---

[246] Norges delegasjon til FNs nettsider;
Datatilsynets nettsider
[247] Port- og teletilsynets nettsider
[248] Stortingsmelding 15 (2008-2009), 11.4 *Norges utvidede interesser*
[249] Stortingsmelding 15 (2008-2009), 11.4 *Norges utvidede interesser*
[250] Verdensbankens nettsider

Thune og Lunde peker på at fokus i engasjementspolitikken på mange måter har blitt flyttet fra penger til kompetanse, og for å prioritere og konsentrere sin innsats vil det derfor lønne seg for Norge å satse på felt i engasjementspolitikken der vi har høy kompetanse. Selv om det ikke er sannsynlig at Norge vil bli en fremtidig supermakt i cyberdomenet, er Norge er teknologisk høyt utviklet og har betydelig kompetanse på området. En mulig logisk slutning vil derfor være å fokusere vår innsats ved å kombinere to ting Norge er gode på – engasjement og cyberdomenet – og hjelpe stater som trenger det med å bygge opp sikker og effektiv cyberinfrastruktur. I Kapittel 4 – Økonomi beskrives det hvordan Norge ved å vise seg som et land med høy grad av cybersikkerhet kan tiltrekke seg investeringer og gjøre seg til et attraktivt land å drive forretninger i, sammenlignet med land som legger mindre vekt på cybersikkerhet. Dette kan på et vis sees som analogt med engasjementspolitikken – man kan kombinere det med å bli gode på utvikling av cyberinfrastruktur med et område der Norge allerede stiller sterkt, og dermed bli en foretrukket samarbeidspartner for stater som trenger hjelp med cyberinfrastruktur. Kanskje kan dette i fremtiden gjøres til et såkalt komparativt fortrinn, som dermed kan gi Norge større innflytelse internasjonalt.

Støtte til utvikling av andre staters cyberinfrastruktur er dog ikke uten etiske dilemmaer: hva brukes denne infrastrukturen til etter at norsk støtte er avsluttet? Respekt for menneskerettighetene og demokrati er verdier som ligger til grunn for norsk politisk identitet, og arbeidet med å sikre menneskerettigheter også på Internett har vært et viktig fokusområde for Norge i internasjonale fora. Det er også i Norges interesse at flest mulig land er stabile demokratier og respekterer menneskerettigheter av den grunn at dette er parallelt med støtte til den internasjonale rettsordenen som landet er avhengig av. Det er derimot ikke gitt at et land som har fått støtte av Norge vil bruke sin nye infrastruktur på en måte som vil gå overens med Norges arbeid for ytringsfrihet. Kanskje vil regimet overvåke alt deres borgere gjør på Internett? Kanskje vil de sensurere informasjonsflyten, for å hindre kritikk av det sittende regimet? Her kan man tenke seg paralleller med tradisjonell engasjementspolitikk, der man for eksempel gjennom forsvarsrettet sikkerhetssektorreform bygger opp et sikkerhetsapparat som senere kan bli brukt til å undertrykke folkegrupper, eller at man bygger opp valgsystemer der man enten driver utstrakt valgfusk, eller rett og slett på demokratisk vis velger ledere som vil ta landet i en autokratisk retning. Hva gjør Norge om stater bruker cyberinfrastruktur man har hjulpet til med å sette opp for å utøve intern cybermakt mot sine borgere, stikk i strid med norske verdier og universelle menneskerettigheter? Om vestlige stater sanksjonerer stater for denne typen oppførsel, kan det tenkes at andre aktører blir mer attraktive bistandsytere. Kina har allerede etablert seg som en viktig bygger av infrastruktur i afrikanske land, da de har færre krav og regler knyttet til blant annet gjennomsiktighet og korrupsjon hos mottagerlandet enn mange vestlige aktører. Landet har heller ingen motforestillinger mot å investere i stater av strategisk nytte og interesse.[251] Med tanke på cyberdomenet kan dette bli særlig urovekkende, ettersom Kina har både teknologien, kompetansen og få reservasjoner med hensyn til sensur og overvåkning.

Denne rapporten har ikke som mål å komme frem til et entydig svar på dette dilemmaet, men søker heller å belyse hvilke problemstillinger som kan bli stadig viktigere i fremtidens

[251] Kelley, Jeremy (2012)

engasjementspolitikk. Om en stat bruker norsk-sponsede cyberressurser til å utøve intern cybermakt, kan man i alle fall se for seg at Internett vil gjøre det lettere for Norge og likesinnede stater å påtale eventuelle menneskerettighetsbrudd, som nevnt ovenfor. Det kan også tenkes at Norge gjennom strategiske valg i engasjementspolitikken kan få økt internasjonal tyngde, og at eventuell fordømmelse fra norsk hold vil kunne påvirke stater i retning av mer demokratisk praksis. Det levner uansett liten tvil om at cyberdomenet vil fortsette å spille en stadig større rolle også i engasjementspolitikken.

8 Identitet

I Refleksprosjektets bok om norske interesser er det et eget kapittel om *identitet*. Identitet er det som handler om «tilhørighet og hvordan personer og grupper forstår seg selv og blir sett på utenfra.»[252] Utenrikspolitiske aspekter ved identitet som trekkes frem her er kulturelt mangfold som gjør Norge mer attraktivt for utenlandsk næringsvirksomhet, spenningen mellom sekularisme og religiøs fundamentalisme som har preget 2000 tallet spesielt, migrasjonsspørsmål og utfordringer knyttet til å fremstå som et «kulturelt ensartet og enhetlig» Norge utad.[253]

Økt kontakt mellom mennesker på tvers av landegrenser og vår interesse for nyheter verden rundt bringer kulturelle uttrykk nærmere hverandre. Etter hvert som verden blir mindre og interaksjonen mellom stater øker ytterligere oppstår det splittelser og krasse debatter i samfunnet. Lunde og Thune trekker spesielt frem konflikten «mellom en religiøst fundamentalistisk og en utpreget sekulær verdiorientering og identitet» som viktig i internasjonal politikk de senere år. Det understrekes i denne sammenheng at dette ikke innebærer en «Clash of Civilizations»[254] slik forespeilet av Samuel S Huntington i 1993. «Det er en norsk interesse både å støtte opp om mangfoldet, og å bidra til å dempe identitetskonflikter som globaliseringen fører med seg og som gjør det vanskeligere å leve sammen i sammensatte samfunn lokalt og globalt.» [255]

8.1.1 Norsk identitet på Internett

Før kommersialiseringen av Internett var det kun radio og fjernsynsmediene som hadde muligheten til å dekke hele områder med kommunikasjonssignaler. Massekommunikasjon var derfor primært forbeholdt organisasjoner, og ikke enkeltpersoner. Kommersialiseringen av Internett har endret dette i kraft av seg selv, den grunnleggende «hjemmesiden», og i kraft av tjenester som sosiale medier. *Alle* med Internettilgang kan nå være avsendere av massekommunikasjon, anonymt om man vil, men har ikke lenger de samme begrensningene som radio og fjernsyn hadde med geografisk dekning. Domenet er globalt, og alle med Internettilgang

[252] Lunde og Thune m.fl., 2008:186
[253] Lunde og Thune m.fl., 2008:187
[254] Sammen med Francis Fukuyamas "The End of History and the Last Man" var Huntington's "The Clash of Civilizations?" innflytelsesrike verk som forsøkte å forstå hvordan fremtidens konflikter ville se ut rett etter den kalde krigen tok slutt. Huntington forespeilet, grovt forenklet, at konfliktene ville oppstå i grenselandene mellom de store verdenssivilisasjonene. Han delte verden inn i sju (evt. åtte) sivilisasjoner; den vestlige, den konfusianske, den japanske, den islamske, den hinduistiske, den slavisk-ortodokse, den latin-amerikanske og muligens den afrikanske.
[255] Lunde og Thune m.fl., 2008:187

har muligheten til å lese det andre har skrevet, oversatt til et annet språk av Google dersom det skulle være nødvendig. Selv med streng innholdsregulering vil en stat oppleve at borgere evner å omgå mekanismene, og får fatt i den informasjonen de ønsker. Det er en samfunnsmessig kommunikasjonsrevolusjon uten sidestykke.

Over Internett vil brukeren på godt og vondt komme over det fulle spekter av meninger. Der fant Anders Behring Breivik sine meningsfeller og der blogget 14 år gamle Malala Yousafzai om livet under Taliban før hun ble forsøkt henrettet. En anbefaling Lunde og Thune gir er å «bidra med kunnskap og nyanser i norsk offentlig debatt for å motvirke stereotypier og tabloid virkelighet, konfliktfiksering og radikaliseringsspiral».[256] En vesentlig del av identitetsdebattene utspiller seg i avisenes debattspalter, åpne og lukkede nettfora og sosiale medier. En rapport fra Politihøgskolen viser til at det med tanke på nettradikalisering er utfordringer knyttet til «hvor omfattende ytringsvernet for internettbaserte aktiviteter bør være» i tillegg til at «Internett har kortet ned avstanden mellom tanke og handling».[257]

I del to av Lunde og Thunes siste bok, *Hva Norge kan være i verden*, tar forfatterne for seg nettopp *hva Norge er i verden*. Kapittelet innledes med en fortelling om en barnevernssak i Stavanger 2012 som involverte et indisk foreldrepar. Saken viste seg å vekke enorm oppmerksomhet i India, og saksbehandleren i Stavanger var med ett blitt et bilde på Norge utad.[258] Cyberdomenet har gjort oss alle til avsendere av massekommunikasjon med et potensielt globalt publikum og dermed har alle norske borgere potensielt en rolle å spille i utenrikspolitikken. Hva om saksbehandleren fra Stavanger hadde en blogg hvor hun skrev egne meninger basert på sitt arbeid? Hva om hun hadde lest seg opp om India, og skrevet krass kritikk i bloggen? Denne typen spørsmål kan like gjerne stilles ovenfor privatpersoner eller ansatte i privat sektor. Den spenningen Lunde og Thune refererer til mellom det sekulære og fundamentalistiske kan få altså utløp på Internett - til skue for resten av verden. Det behøver ikke å være en offentlig ansatt for å fremprovosere reaksjoner rettet mot Norge. Slagkraften private aktører potensielt har i cyberdomenet kom tydelig frem i forbindelse med amatørfilmen «Innocence of Muslims»[259], nevnt tidligere under sikkerhet. Hva slags systemer for informasjonsdeling vi vil finne i fremtidens sosiale medier er umulig å forutsi, men trenden så langt tilsier kort og godt at avstanden mellom mennesker verden rundt vil bli mindre og mindre. Hvordan Norge oppfattes ute i verden påvirkes altså i større grad av handlingene til enkeltpersoner, både privat så vel som i regi av arbeidsgiver. Dette gir Forsvaret både nye muligheter og nye utfordringer.

I internasjonale operasjoner kommer forsvarspersonell i tett kontakt med fremmede kulturer. Forsvaret har derfor gode forutsetninger for å bidra med kunnskap som fremmer en nyansert debatt, både med tanke på kunnskaper om samfunnene vi opererer i og operasjonene i seg selv. Opp gjennom historien har historier, fotografier og video fra konfliktsoner bidratt til å fortelle

[256] Lunde og Thune m.fl., 2008:200
[257] Politihøgskolen Forskning, 2013:64
[258] Lunde og Thune (2013) Kapittel 8
[259] Amatørfilmen som ble oppfattet som blasfemisk av deler av den muslimske befolkningen i verden, og førte til omfattende tjenestenektangrep mot amerikanske banker.

verden om alt fra heltedåd og dagligliv til krigsforbrytelser og tragedier til verden, men aldri før har enkeltpersoner hatt de samme mulighetene til å gjøre slike opptak selv og spre dem globalt. For at Forsvaret skal fremstå som en profesjonell aktør i internasjonale operasjoner blir det desto viktigere at informasjon som ikke er sannferdig eller er tatt ut av kontekst ikke bidrar til unødig splittelse mellom samfunnsgrupper. Hastigheten informasjon sprer seg med er en ytterligere utfordring. Hvordan skal man beholde initiativet ovenfor nettaviser, blogger eller nettfora og samtidig levere informasjon av høy kvalitet?

Forsvarsansatte kan og igjennom privat bruk av cyberdomenet undergrave det norske Forsvarets innsats i internasjonale operasjoner. I 2003 dukket det opp en video på Internett som viste soldater fra Norbataljonen synge og danse til Beach Boys «Kokomo», for anledningen med ny tekst tilpasset deres oppdrag i Kosovo. Videoen var aldri ment for allmenheten, men ble ifølge NRK sendt til en privatperson som deretter la den ut på Internett.[260] Det som var ment som intern humor i bataljonen var med ett internasjonalt skue, ble blant annet sendt på serbisk fjernsyn, og satte det norske bidraget i negativt lys. I dag, ti år senere, er denne videoen den første som dukker opp på YouTube dersom man søker på «Norwegian Soldiers Kosovo». To hendelser som vakte oppsikt i 2011 kom i form av video og bilder som viser amerikanske tropper som urinerer på døde Taliban-soldater samt bilder av brente utgaver av Koranen fra 2011.[261]

8.1.2 Diasporagrupper i norsk utenrikspolitikk

Diasporagrupper[262] gjør den norske identiteten mer heterogen enn tidligere og det er et større press på å representere ulike gruppers identitet utad gjennom utenrikspolitikken. Det er kort og godt et «behov for å representere et «nytt Norge»».[263] De nye kommunikasjonsmulighetene legger til rette for at diasporagruppene kan følge med på venner, familie og hendelser i sitt gamle land langt bedre enn tidligere. Hvordan Norge forholder seg til disse landene i utenrikspolitikken er viktig for de som har bånd dit, og vi kan derfor vente stadig mer oppmerksomhet rettet mot norsk utenrikspolitikk fra egne borgere. Lunde og Thune kaller dette båndet for et «virtuelt fellesskap», og ett som da kan preges av diasporagruppen er uenig med begge lands politikk.

Norge har diasporagrupper fra en rekke land, og enkelte av disse landene har en tradisjon for sensur og overvåkning som ikke er forenelig med norske verdier, også i cyberdomenet. Det er varierende hvor langt landene har kommet i utbyggingen av infrastruktur, dermed gjenstår det å se hvordan myndighetene velger å forholde seg til de nye kommunikasjonsmulighetene befolkningen får gjennom cyberdomenet. Bruken av indre cybermakt for sosial kontroll kan derfor bli et aktuelt tema for diasporagrupper i Norge i årene som kommer. De kan også bli mål for flyktningespionasje igjennom cyberdomenet. Denne debatten kan og kompliseres av bidrag til utbygging av infrastruktur gjennom den norske stat eller næringslivsaktører som Telenor, slik nevnt under kapittelet om norsk engasjementspolitikk.

[260] Prohi og Alstadsæter, 2005
[261] Stewart og Alexander, 2006
[262] Diaspora-begrepet benyttes om befolkningsgrupper i et land med røtter i et annet, som for eksempel pakistanere bosatt i Norge.
[263] Lunde og Thune m.fl., 2008:197

8.1.3 Nettidentitet

Lunde og Thune bemerker at «det som føles som utvisking av økonomiske, sosiale og kulturelle grenser har de siste tiårene vist seg å fremprovosere identitetsbaserte motreaksjoner».[264] En interessant parallell til dette i cyberdomenet er reaksjonene som snarere kommer mot statsmaktenes inntog i cyberdomenet. Nettentusiaster viser stor interesse for et fritt og åpent Internett med fri flyt av informasjon, og danner en slags global interessegruppe hvis kamp utspiller seg både nasjonalt og transnasjonalt. I flere stater, inkludert Norge, ser vi denne kulturen komme til uttrykk gjennom etableringen av «Piratpartier» - internasjonalt organisert i paraplyorganisasjonen Pirate Parties International (PPI).[265] Den mer ekstreme varianten av nettidentiteten kjenner de fleste i dag, gjemt bak Anonymous-masken.[266] Dette er en av måtene «Internett og global media kanaliserer, forsterker og skaper koblinger. Innenrikspolitiske og utenrikspolitiske arenaer smelter sammen».[267] For slike grupper er Internett i seg selv en interesse.

Disse bevegelsene representerer ingen identitetskonflikt sammenlignbar med den mellom det sekulære og fundamentalistiske i verden. Segmenter av denne typen bevegelser har imidlertid vist seg å være kapable til å gjennomføre angrep i cyberdomenet som påfører ofre både økonomiske kostnader og skade på omdømme. Hvordan denne «identiteten» utvikler seg i takt med Internett i årene som kommer, gjenstår å se.

[264] Lunde og Thune m.fl., 2008
[265] For oversikt over piratpartier i verden, se hjemmesidene for den internasjonale piratpartiorganisasjonen, http://www.pp-international.net/
[266] "Ikke bekymr deg, vi kommer fra Internett" er et eksempel på utsagn som brukes i "nettkulturen", inkludert Anonymous.
[267] Lunde og Thune m.fl., 2008:195

Litteraturliste

8.2 Artikler, bøker og rapporter

Aabakken, Ola (2002). INTEROPERABILITET: Kostnadsdriver og styrkemultiplikator. FFI-rapport 2002/02320

Abrams, Marshall og Joe Weiss (2008). *Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia*. Sist besøkt 30.10.2013 http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

Bellocchi, Luke P (2001) «Assessing the Effectiveness of the Economic Espionage Act of 1996». *International Journal of Intelligence and Counterintelligence*, 14(3):366-387.

Caucasus Elections Watch (2013) Margvelashvili launches programme ahead of Presidential election in Georgia *Caucasus Elections Watch Inter Press News*, 20. September 2013. Sist besøkt 30.10.2013 http://electionswatch.org/2013/09/20/margvelashvili-launches-programme-ahead-of-presidential-election-in-georgia/

Center for a New American Security (2013). *Active Cyber Defense. A Framework for Policymakers*. Sist besøkt 30.10.2013 http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf

Center for Strategic and International Studies (CSIS) og McAfee (2013). *The Economic Impact of Cybercrime and Cyber Espionage*. Sist besøkt 30.10.2013 http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

Clemente, Dave (2013). Cyber Security and Global Interdependence: What is Critical? London: Chatham House.

Det britiske kabinettkontoret (2011) *The UK Cyber Security Strategy. Protecting and Promoting the UK in a digital world*. Sist besøkt 30.10.2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Direktiv 2006/24 EF (2011). *Plan om regelverk, konsesjonsplikt, sikkerhetstiltak og tilsyn*, Datatilsynet. Sist besøkt 30.10.2013 http://www.datatilsynet.no/Global/04_analyser_utredninger/2011/2011-11-15-Direktiv2006-24-EF.pdf

Eriksen, Thomas Hylland (2008). *Globalisering: Åtte nøkkelbegreper*, Universitetsforlaget, Oslo

Europakommisjonens Institutt for Energi og Transport (IET) (2012). *JRC Scientific and policy report. Smart Grid projects in Europe: Lessons learned and current developments (2012 update)*. Sist besøkt 30.10.2013 http://ses.jrc.ec.europa.eu/jrc-scientific-and-policy-report

Fagerland, Snorre (2013) .The Hangover Report. Rapport publisert på *Norman*s hjemmesider. Sist besøkt 30.10.2013 http://blogs.norman.com/2013/security-research/the-hangover-report

Finland's Cyber security Strategy (2013). Sist besøkt 30.10.2013 http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Fornyings-, administrasjons- og kirkedepartementet (2013a) *Nasjonal strategi for informasjonssikkerhet*. Sist besøkt 29.10.2013 http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf

Fornyings-, administrasjons- og kirkedepartementet (2013b), *Nasjonal Strategi for informasjonssikkerhet. Handlingsplan*. Sist besøkt 29.10.2013 http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Handlingsplan_nasjonal_strategi_informasjonssikkerhet.pdf

Forsvarets Etterretningstjeneste (2013) *Fokus 2013 Etterretningstjenestens vurdering*. Sist besøkt 29.10.2013 http://forsvaret.no/om-forsvaret/organisasjon/felles/etjenesten/Documents/FOKUS-2013.pdf

ITU Broadband Commission (2013) The State of Broadband 2013: Universalizing Broadband. Sist besøkt 29.10.2013 http://www.broadbandcommission.org/Documents/bb-annualreport2013.pdf
Jacob Børresen og Hans Christian Helseth (2011) *Norske interesser og Sjømakt*. FFI-rapport 2011/00759.
Kelley, Jeremy (2012) "China in Africa: Curing the Resource Curse with Infrastructure and Modernization", *Sustainable Development Law & Policy* 12(3):35-41, 57-60.
Kristoffersen, Lene (2009) *Interesser i norsk utenrikspolitikk*, Oslo Files on Defence and Security nr. 4, Institutt for Forsvarsstudier, Oslo.
Kvalvik, Sverre og Tore Nyhamar, (ventes i 2013) Consequences of the financial crisis for NATO, FFI-rapport.
Langø, Hans-Inge (2013) «Slaying Cyber Dragons: Competing Approaches to Cyber Security». *NUPI Working Paper 820*.
Leira, Halvard og Ole Jacob Sending (2013). «Maktforskyvning, global organisering og norsk utenrikspolitikk». I Mølster, Odd og Åsmund Weltzien (red.) (2013) *Norge og det nye verdenskartet. Debattbok fra Utenriksdepartementets Refleksprosjekt.* 1. utg. Oslo: Cappellen Damm.
Libicki, Martin C (2009). «Cyberdeterrence and Cyberwar». *Rand Corporation*. Sist besøkt 30.10.2013 http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
Lunde, Leiv og Henrik Thune (2013). *Hva Norge kan være i verden*. 1. utg. Oslo: Cappelen Damm.
Lunde, Leiv og Iselin Stensdal (2013) «Norsk ressurs- og miljøpolitikk mot 2030: Landing i Kina eller på månen?». I Odd Mølster og Åsmund Weltzien (red.), *Norge og det nye verdenskartet*. Oslo: Cappelen Damm.
Lunde, Leiv, Henrik Thune, Eiler Fleischer, Leo Grünfeld og Ole Jacob Sending (2008) *Norske interesser: Utenrikspolitikk for en globalisert verden*, 1. utg. Cappelen Damm, Oslo
Maurer, Tim (2011) *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?*, Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School
McKinsey & Company Global Institute (2013). *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*. Sist besøkt 30.10.2013 http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters
Ministry of Security and Justice (Nederland) (2010). *The National Cyber Security Strategy (NCSS)*. Sist besøkt 30.10.2013 https://www.ncsc.nl/english/organisation/about-the-ncsc/background.html
Nasjonal Sikkerhetsmyndighet (NSM) (2012). *NorCERT Kvartalsrapport for 4. kvartal 2012*. Sist besøkt 30.10.2013 https://www.nsm.stat.no/Documents/NorCERT/2012/Q4-12-NORCERT_web.pdf
Norheim-Martinsen, Per M. (2009). EU capabilities for a comprehensive approach: Broad interoperability as comparative advantage, FFI-rapport 2009/01300
Norman, Victor D (2013) «Farvel til Europa? Norsk utenriks- og handelspolitikk i en ny verden» I Odd Mølster og Åsmund Weltzien (red.) (2013) *Norge og det nye verdenskartet*. Oslo: Cappelen Damm.
Norton (2012). *2012 Norton Cybercrime Report*. Sist besøkt 30.10.2013 http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
NOU (2007:2): *Lovtiltak mot datakriminalitet*, Justis- og beredskapsdepartementet. Sist besøkt 30.10.2013 http://www.regjeringen.no/nb/dep/jd/dok/nouer/2007/nou-2007-2/4/3.html?id=449737
NOU (2013:2): *Hindre for digital verdiskapning*, Fornyings-, administrasjons-, og kirkedepartementet. Sist besøkt 30.10.2013 http://www.regjeringen.no/nb/dep/fad/dok/nouer/2013/nou-2013-2.html?id=711002
Næringslivets Sikkerhetsråd (2013) Mørketallsundersøkelsen. Informasjonssikkerhet og datakriminalitet. Sist besøkt 29.10.2013 http://www.nsr-

org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/moerketall_2012.pdf
Organisation for Economic Co-operation and Developent (OECD) (2008). The Seoul Declaration for the Future of the Internet Economy. Sist besøkt 30.10.2013 http://www.oecd.org/internet/consumer/40839436.pdf
Pew Research Global Attitudes Project (2013) "Economic Crisis Now An EU Crisis". Kap. 2 i "The New Sick Man of Europe: the European Union". Sist besøkt 29.10.2013 http://www.pewglobal.org/2013/05/13/chapter-2-economic-crisis-now-an-eu-crisis/
Politidirektoratet (2012). *Politiet I det digitale samfunnet. En arbeidsgrupperapport om: Elektroniske spor, IKT-kriminalitet og politiarbeid på Internett*. Sist besøkt 30.10.2013 https://www.politi.no/vedlegg/rapport/Vedlegg_1866.pdf
Politiets Sikkerhetstjeneste (2013). *Åpen Trusselvurdering 2013*. Sist besøkt 29.10.2013 http://www.pst.no/media/58980/PSTs_tv2013_web.pdf
Politihøgskolen Forskning (2013) Inger Marie Sunde Sunde (red) *Forebygging av radikalisering og voldelig ekstremisme på internett*. Sist besøkt 29.10.2013 http://www.regjeringen.no/pages/38510685/Rapport_forebygging-rad-eks.pdf
Rattray, Gregory J og Jason Healey (2011) «Non-state actors and cyber conflict». Kapittel 5 i Kristin M Lord og Travis Sharp (red.) *America's Cyber Future. Security and Prosperity in the Information Age*. Washington D.C.: Center for a New American Security.
Rid, Thomas (2013). *Cyber War Will Not Take Place*. London: Hurst & Company.
St.meld. nr. 15 (2008-2009): Interesser, ansvar og muligheter. Hovedlinjer i norsk utenrikspolitikk. Utenriksdepartementet.
St.meld. nr. 17 (2006-2007): *Eit informasjonssamfunn for alle*, Fornyings-, administrasjons-, og kirkedepartementet. Sist besøkt 29.10.2013 http://www.regjeringen.no/nn/dep/fad/dokument/proposisjonar-og-meldingar/stortingsmeldingar/20062007/stmeld-nr-17-2006-2007-/9/4/3.html?id=441616
Statistisk sentralbyrå (SSB) (2013). *Utenrikshandel med varer, September 2013, foreløpige tall*. Publisert 15. oktober 2013. Sist besøkt 30.10.2013 http://www.ssb.no/utenriksokonomi/statistikker/muh
Suny, Ronald Grigor (1994) *The Making of the Georgian Nation*. 2. Utg. Indiana: Indiana University Press.
Trustwave (2013). *Global Security Report*. Sist besøkt 30.10.2013 http://www.trustwave.com

8.3 Avisartikler

AFP (2013). Georgian Dream candidate wins presidential vote. *France24*, 27. oktober 2013. Sist besøkt 30.10.2013 http://www.france24.com/en/20131027-georgia-dream-margvelashvili-wins-presidential-vote-saakashvili
Antidze, Margarita og Timothy Heritage (2013) Billionaire PM cements grip in Georgia, ally elected president, *Reuters*, 27. oktober 2013. Sist besøkt 30.10.2013 http://uk.reuters.com/article/2013/10/27/uk-georgia-election-idUKBRE99P0AD20131027
Arnsdorf, Isaac (2013). Phantom Ships Expose Weakness in Vesse-Tracking System. *Bloomberg*, 29. oktober 2013. Sist besøkt 30.10.2013 http://www.bloomberg.com/news/2013-10-29/phantom-ships-expose-weakness-in-vessel-tracking-system-freight.html
BBC (2013a) Syria fears keep markets jittery as oil price steadies, BBC, 28. august 2013. Sist besøkt 29.10.2013 http://www.bbc.co.uk/news/business-23860841
BBC (2013b) US-China cyber security working group meets. *BBC*, 9. juli 2013. Sist besøkt 30.10.2013 http://www.bbc.co.uk/news/world-asia-china-23177538
Berkow, Jameson (2012). Nortel hacked to pieces. *Financial Post*, 25. februar 2012. Sist besøkt 30.10.2013 http://business.financialpost.com/2012/02/25/nortel-hacked-to-pieces/
Børresen, Mette Finborud, Reidar Gregersen og Arne Sørenes (2013). Gjøvik får senter for cybersikkerhet. *NRK*, 11. juni 2013. Sist besøkt 30.10.2013 http://www.nrk.no/ho/senter-for-cyber-sikkerhet-i-gjovik-1.11075208

Brooks, Bradley og Frank Bajak (2013). Brazil looks to break from US-centric Internet. *AP*, 17. september 2013. Sist besøkt 30.10.2013 http://news.yahoo.com/brazil-looks-break-us-centric-internet-040702309.html
Bruaset, Ingvild og Carl Alfred Dahl (2012). Svartelistet selskap leverer Norges nye mobilnett. *Aftenposten*, 10. oktober 2012. Sist besøkt 15.11.2013 http://www.aftenposten.no/okonomi/Svartelistet-selskap-leverer-Norges-nye-mobilnett-7013156.html
Crawford, Michael (2006). Utility hack led to security overhaul. *Computerworld*, 16. februar 2006. Sist besøkt 30.10.2013 http://www.computerworld.com/s/article/108735/Utility_hack_led_to_security_overhaul
Coughlan, Sean (2013). £7.5m university fund to train cybersecurity experts. *BBC News*, 9. mai 2013. Sist besøkt 30.10.2013 http://www.bbc.co.uk/news/education-22450544
Crawford, Michael (2006). Utility hack led to security overhaul. Computerworld, 16. februar 2006. Sist besøkt 30.10.2013 http://www.computerworld.com/s/article/108735/Utility_hack_led_to_security_overhaul
Dahl, Carl Alfred og Ingvild Bruaset (2012). Staten overlater datasikkerheten til Telenor. *Aftenposten* 15. november 2012. Sist besøkt 15.11.2013 http://www.aftenposten.no/okonomi/Staten-overlater-datasikkerheten-til-Telenor-7017328.html
Dewey, Caitlin (2013) Map: More than half of humanity lives within this circle. Artikkel publisert I the Washington Post 7 mai 2013. Sist besøkt 29.10.2013 http://www.washingtonpost.com/blogs/worldviews/wp/2013/05/07/map-more-than-half-of-humanity-lives-within-this-circle/
Eikeseth, Unni (2013). Meiner europeisk supernett må på plass for å nå fornybar-mål I EU *NRK Nettavis*, 14. juni 2013. Sist besøkt 30.10.2013 http://www.nrk.no/viten/klimamal-avheng-av-nytt-supernett-1.11080486
Færås, Arild (2013). USA til Norge: Vi PRISM-overvåker ikke nordmenn uten mistanke. *Aftenposten*, 3. september 2013. Sist besøkt 30.10.2013 http://www.aftenposten.no/nyheter/iriks/USA-til-Norge---Vi-PRISM-overvaker-ikke-nordmenn-uten-mistanke-7296578.html#.UmBGA1DIaco
Fisher, Max (2013) Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?. *The Washington Post*, 23. april 2013. Sist besøkt 30.10.2013 http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/
FNs Nyhetssenter (2012) New UN campaign highlights financial and social costs of transnational organized crime. Publisert 16. juli 2012. Sist besøkt 30.10.2013 http://www.un.org/apps/news/story.asp/html/realfile/story.asp?NewsID=42480&Cr=Drugs&Cr1=#.UnDXCPlLOcp
Gallagher, Ryan (2013). Skype under investigation in Luxembourg over link to NSA. *The Guardian*, 11 .oktober 2013. Sist besøkt 30.10.2013 http://www.theguardian.com/technology/2013/oct/11/skype-ten-microsoft-nsa
Greenberg, Andy (2012). Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits. *Forbes*, 23. mars 2012. Sist besøkt 30.10.2013 http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/
Gross, Doug (2013). Google boss: Entire world will be online by 2020. *CNN*, 15. april 2013. Sist besøkt 30.10.2013 http://edition.cnn.com/2013/04/15/tech/web/eric-schmidt-internet
Helgesen, Ole Ketil (2013). Industriroboter skal revolusjonere oljebransjen. *Teknisk Ukeblad*, 30. oktober 2012. Sist besøkt 30.10.2013 http://www.tu.no/petroleum/2012/10/30/industriroboter-skal-revolusjonere-oljebransjen
Hillestad, Linn Kongsli, Espen Sandli og Ola Strømman (2013). I verste tilfelle kan liv gå tapt. *Dagbladet*, 17. oktober 2013. Sist besøkt 30.10.2013 http://www.dagbladet.no/2013/10/17/nyheter/innenriks/datasikkerhet/nullctrl/28572676/
Hofmann, Marcia og Trevor Timm (2012). "Zero-day" exploit sales should be key point in cybersecurity debate. *Electronic Frontier Foundation*, 29. mars 2012. Sist besøkt 30.10.2013

https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate
Hopkins, Nick (2013). 'Cyber Jedi' schools contest a new hope for Britain's IT empire to strike back. *The Guardian*, 28. april 2013. Sist besøkt 30.10.2013 http://www.theguardian.com/technology/2013/apr/28/cyber-jedi-contest-britain-empire
Hutton, Rober (2013). U.K. Sets Up Cybersecurity Center to Coordinate Computer Defense. *Bloomberg*, 27. mars 2013. Sist besøkt 30.10.2013 http://www.bloomberg.com/news/2013-03-27/u-k-sets-up-cybersecurity-center-to-coordinate-computer-defense.html
Jame, Fred (1999) China, Taiwan in Web hacking 'war'. *ZDNet*, 11. august 1999. Sist besøkt 30.10.2013 http://www.zdnet.com/news/china-taiwan-in-web-hacking-war/103001
Johansen, Per Anders (2013). Spionerte på Telenor-sjefer, tømte all e-post og datafiler. *Aftenposten*, 17. mars 2013. Sist besøkt 30.10.2013 http://www.aftenposten.no/nyheter/Spionerte-pa-Telenor-sjefer_-tomte-all-e-post-og-datafiler-7149813.html#.UZN5LbVA1p4
Jørgenrud, Marius (2013). Hemmelig svensk brannmur. *Digi*, 10. januar 2013. Sist besøkt 30.10.2013 http://www.digi.no/909250/hemmelig-svensk-brannmur
Kirkenes, Leiv Martin (2011). Smart strøm med komplikasjoner. *IDG/Computerworld*, 19. september 2011. Sist besøkt 30.10.2013 http://www.idg.no/computerworld/article220814.ece
Leyden, John (2009). Russian spy agencies linked to Georgian cyberattacks. *The Register*, 23. mars 2009. Sist besøkt 30.10.2013 http://www.theregister.co.uk/2009/03/23/georgia_russia_cyberwar_analysis/
Lie, Øyvind (2013). Strømbrudd hindret gasseksport fra Ormen lange, *Teknisk Ukeblad*, 7. mars 2013. Sist besøkt 29.10.2013 http://www.tu.no/kraft/2013/03/07/strombrudd-hindret-gasseksport-fra-ormen-lange
Long, Colleen og Martha Mendoza (2013). Bank Heist impressed cyber crime experts. *NBC News*, 10. mai 2013. Sist besøkt 30.10.2013 http://www.nbcnews.com/technology/bank-heist-impressed-cyber-crime-experts-1C9881411
Matlack, Carol (2013) Chinese Workers — in Greenland?, *Bloomberg Businessweek* 10. februar 2013. Sist besøkt 29.10.2013 http://www.businessweek.com/articles/2013-02-10/chinese-workers-in-greenland
Menn, Joseph (2013). New Snowden documents say NSA can break common internet encryption *Reuters*, 5. september 2013. Sist besøkt 30.10.2013 http://mobile.reuters.com/article/topNews/idUSBRE98413720130905
Naraine, Ryan (2012). Nortel hacking attack went unnoticed for almost 10 years. *ZDNet*, 14. februar 2012. Sist besøkt 30.10.2013 http://www.zdnet.com/blog/security/nortel-hacking-attack-went-unnoticed-for-almost-10-years/10304
Nilsen, Terje (2013). Høgskolen får fem millioner .*Oppland Arbeiderblad*, 12 oktober 2013. Sist besøkt 30.10.2013 http://www.oa.no/nyheter/article6914158.ece
NTB (2010) Banksystemene driftes i Ukraina *Teknisk Ukeblad*, 4. mars 2010. Sist besøkt 29.10.2013 http://www.tu.no/it/2010/03/04/banksystemene-driftes-i-ukraina
Olson, Parmy (2013). Encryption App Silent Circle Shuts Down E-Mail Service 'To Prevent Spying'. *Forbes Magazine*, 9. august 2013. Sist besøkt 30.10.2013 http://www.forbes.com/sites/parmyolson/2013/08/09/encryption-app-silent-circle-shuts-down-e-mail-service-to-prevent-spying/
Perlroth, Nicole og Quentin Hardy (2013). Bank Hacking Was the Work of Iranians, Officials Say. *The New York Times*, 8. januar 2013. Sist besøkt 30.10.2013 http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?pagewanted=1&_r=2&
Poulsen, Kevin (2003). Slammer worm crashed Ohio nuke plan network. *Security Focus*, 19. august 2003. Sist besøkt 30.10.2013 http://www.securityfocus.com/news/6767
Prohic, Dino og Rune Alstadsæter (2005). Norske soldater i skandalevideo. *Nrk Nettavis*, 17. mai 2005. Sist besøkt 30.10.2013 http://www.nrk.no/nyheter/innenriks/4750027.html
Protalinsky, Emil (2012). NSA: Cybercrime is 'the greatest transfer of wealth in history'. *ZDNet*, 10. juli 2012. Sist besøkt 30.10.2013 http://www.zdnet.com/nsa-cybercrime-is-the-greatest-transfer-of-wealth-in-history-7000000598/

Ring, Tim (2013). UK National CERT launch postponed. *SC Magazine*, 15. oktober 2013. Sist besøkt 30.10.2013 http://www.scmagazineuk.com/uk-national-cert-launch-postponed/article/316357/
Rossen, Eirik (2013). "Prism-garanti" tidoblet trafikken til Jotta. *Digi*, 26. juli 2013. Sist besøkt 30.10.2013 http://www.digi.no/920022/prism-garanti-tidoblet-trafikken-til-jotta
Rossen, Eirik (2013). Sterkt imot granskning av Huawei. *Digi*, 15. mai 2013. Sist besøkt 11.11.2013 http://www.digi.no/916583/sterkt-imot-granskning-av-huawei
RT (2013). Electronic al-Qaeda Army claims to have hacked US government websites. *RT*, 11. mars 2013. Sist besøkt 30.10.2013 http://rt.com/usa/hacked-us-government-websites-112/
Sanger, David E (2013). Budget Documents Detail Extent of U.S. Cyberoperations, *the Washington Post*, 31. august 2013. Sist besøkt 30.10.2013 http://www.nytimes.com/2013/09/01/world/americas/documents-detail-cyberoperations-by-us.html?_r=0
Shauk, Zain (2013a). Malware offshore: Danger lurks where the chips fail. *Fuelfix*, 29. april 2013. Sist besøkt 30.10.2013 http://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/
Shauk, Zain (2013b). Malware on oil rig computers raises security fears. *The Houston Chronicle*, 23. februar 2013. Sist besøkt 30.10.2013 http://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php?t=1b259d62f3b05374ef&t=1b259d62f3&t=1b259d62f3
Shelton ,Tracey (2013) Cyber Warfare: the Pirates of Aleppo. *Global Post*, 22. mai 2013. Sist besøkt 30.10.2013 http://www.globalpost.com/dispatch/news/regions/middle-east/syria/130515/cyber-warfare-the-pirates-aleppo-syria-turkey
Sonne, Paul og Margaret Coker (2011). Firms Aided Libyan Spies. First Look Inside Security Unit Shows How Citizens Were Tracked. *The Wall Street Journal*, 30. august 2011. Sist besøkt 30.10.2013 http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388
Spiegel Online International (2013a). Belgacom Attack: Britains GCHQ Hacked Belgian Telecoms Firm. *Spiegel Online International*, 20. september 2013. Sist besøkt 30.10.2013 http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html
Spiegel Online International (AFTERMATH) (2013b). NSA Aftermath: German Firms Scramble to Boost Data Protection. *Spiegel Online International*, 6. august 2013. Sist besøkt 30.10.2013 http://www.spiegel.de/international/world/companies-in-germany-scramble-to-strengthen-data-protection-abilities-a-914922.html
Stangeland, Glenn (2013). Dette er brønnene vi venter på. *Offshore.no*, 30. juli 2013. Sist besøkt 30.10.2013 http://www.offshore.no/sak/59333_dette_er_broennene_vi_venter_paa
Stewart, Phil og David Alexander (2012). U.S. Troops Face Administrative Punishments Over Koran Burning, Urination Video *The Huffington Post*, 27. august 2012. Sist besøkt 30.10.2013 http://www.huffingtonpost.com/2012/08/27/us-troops-koran-burning-urination_n_1833910.html
Sunde, Harald og Trygve Slagsvold Vedum (2013). Norsk matproduksjon – en del av vår samlede beredskap. *Nationen*, 04.08.2013. Sist besøkt 29.10.2013 http://www.nationen.no/2013/08/04/politikk/kommentar/kronikk/matsikkerhet/beredskap/8204907/
The Huffington Post (2012). Nortel Collapse Linked to Hacking Attack. *The Huffington Post*, 15. februar 2012. Sist besøkt 30.10.2013 http://www.huffingtonpost.ca/2012/02/15/nortel-collapse-hackers_n_1280435.html
Tsukayama ,Hayley (2013). After PRISM reports, Swiss data bank sees boost. *The Washington Post*, 8. juli 2013. Sist besøkt 30.10.2013 http://articles.washingtonpost.com/2013-07-08/business/40431184_1_privacy-and-data-protection-data-centers-prism
TV2 (2013). Hacket! Telenor-toppenes PCer tappet av indiske dataspioner. *TV2.no*, 20. mai 2013. Sist besøkt 30.10.2013 http://www.tv2.no/nyheter/innenriks/krim/hacket-telenortoppenes-pcer-tappet-av-indiske-dataspioner-4049263.html

Valentino-Devries, Jennifer, Paul Sonne og Nour Malas (2011). U.S. Firm Acknowledges Syria Used Its Gir to Block Web. *The Wall Street Journal*, 29. oktober 2011. Sist besøkt 30.10.2013 http://online.wsj.com/news/articles/SB10001424053111904199404576538721260166388

Welsh, Hugh (2013) .Why Manufacturing Jobs Are Returning to America For The First Time In Decades. *Business Insider*, 27. februar 2013. Sist besøkt 30.10.2013 http://www.businessinsider.com/manufacturing-jobs-returning-to-america-2013-2

Whittaker, Zack (2013). U.S. cloud industry stands to lose $35 billion amid PRISM fallout. *ZDNet*, 6. august 2013. Sist besøkt 30.10.2013 http://www.zdnet.com/u-s-cloud-industry-stands-to-lose-35-billion-amid-prism-fallout-7000018974/

Zachariassen, Espen (2011). Banken tilbake til Ukraina, *Teknisk Ukeblad* 18. oktober 2011. Sist besøkt 29.10.2013 http://www.tu.no/it/2011/10/18/banken-tilbake-til-ukraina

Zachariassen, Espen (2013). Data fra landets strømkunder kan bli lagret i Danmark. *Teknisk Ukeblad*, 15. mars 2013. Sist besøkt 30.10.2013 http://www.tu.no/it/2013/03/15/data-fra-landets-stromkunder-kan-bli-lagret-i-danmark

Zelin, Aaron Y og Charles Lister (2013). The crowning of the Syrian Islamic Front. *Foreign Policy*, 24. juni 2013. Sist besøkt 30.10.2013 http://mideast.foreignpolicy.com/posts/2013/06/24/the_crowning_of_the_syrian_islamic_front

8.4 Internettressurser

Anonymous (1) Lanseringen av #OpAttackSyria på tekstdelingsstedet Pastebin. Sist besøkt 30.10.2013 http://pastebin.com/wF2ZLxKy

Atlanterhavsrådet (1), Cyber Command Expanding Five Fold. Sist besøkt 30.10.2013 http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-command-expanding-five-fold

Atlanterhavsrådet (2), Russian Military Creating Cyber Warfare Branch. Sist besøkt 30.10.2013 http://www.atlanticcouncil.org/blogs/natosource/russian-military-creating-cyber-warfare-branch

Boscovich, Richard Domingues (2013). Microsoft works with financial services industry leaders, law enforcement and others to disrupt massive financial cybercrime ring. Sist besøkt 11.11.2013 http://blogs.technet.com/b/microsoft_blog/archive/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring.aspx

CCD COE, http://ccdcoe.org/, sist besøkt 29.08.13

Datatilsynet (BREV). Overvåkningsprogrammet PRISM, brev til Justis- og beredskapsminister Grete Faremo 20 august 2013. Sist besøkt 30.10.2013 http://www.datatilsynet.no/Global/05_vedtak_saker/2013/13-00894-1%20Overv%C3%A5kningsprogrammet%20PRISM%20484438_2_1.pdf

Datatilsynet, http://www.datatilsynet.no/personvern/Hva-er-personvern/, sist besøkt 29.08.13

EDA (1) http://eda.europa.eu/Aboutus/Whatwedo/eda-strategies/Capabilities, sist besøkt 29.08.13

EDA (2) http://www.eda.europa.eu/info-hub/news/2013/02/06/eda-participates-in-cyber-defence-conferences, sist besøkt 29.08.13

ENISA, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report, sist besøkt 29.08.13

EU, http://europa.eu/rapid/press-release_IP-13-94_en.htm?locale=en, sist besøkt 29.08.13

Europarådet (1), http://hub.coe.int/web/coe-portal/what-we-do/rule-of-law/cybercrime?dynLink=true&layoutId=36&dlgroupId=10226&fromArticleId=;, sist besøkt 31.10.13

Europarådet (2), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG, sist besøkt 31.10.13

Europarådet (3), http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm, sist besøkt 31.10.13

FFI (1) FFI-FAKTA AISSat-1. Sist besøkt 29.10.2013 http://www.ffi.no/no/Publikasjoner/Documents/AISSAT-1_Norges%20foerste%20nasjonale%20overvaakingssatellitt.pdf
Finansdepartementet (1) Retningslinjer for observasjon og utelukkelse fra SPUs investeringsunivers. Sist besøkt 30.10.2013 http://www.regjeringen.no/nb/dep/fin/tema/statens_pensjonsfond/ansvarlige-investeringer/retningslinjer-for-observasjon-og-uteluk.html?id=594254
FN (1), http://www.un.org/en/aboutun/index.shtml, sist besøkt 29.08.13
FN (2), http://www.un.org/en/mainbodies/secretariat/, sist besøkt 29.08.13
FN (3), http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html, sist besøkt 29.08.13
FN (4), http://www.un.org/en/peacekeeping/contributors/2013/jan13_2.pdf, sist besøkt 29.08.13
FN (5) Maktbruk i folkeretten. Sist besøkt 29.10.2013 http://www.fn.no/Tema/Folkerett/Viktige-temaer-i-folkeretten/Maktbruk-i-folkeretten
Forsvaret (1) Dette er NbF. Sist besøkt 29.10.2013 http://forsvaret.no/aktuelt/publisert/nyheter/documents/nbf-brosjyre.pdf
Forsvarsdepartementet (1). Signerte avtale om forsvarssamarbeid med Georgia. Sist besøkt 30.10.2013 http://www.regjeringen.no/nb/dokumentarkiv/stoltenberg-ii/fd/Nyheter-og-pressemeldinger/Nyheter/2012/signerte-avtale-om-forsvarssamarbeid-med.html?id=706283
Huwei (1) Huawei Europe Fact Sheet. Sist besøkt 15.11.2013 http://www.huawei.com/en/about-huawei/newsroom/resources/europe/
ICANN (1) Montevideo Statement on the Future of Internet Cooperation. Sist besøkt 30.10.2013 http://www.icann.org/en/news/announcements/announcement-07oct13-en.htm
Internet Society (1) A Brief History of the Internet & Related Networks. Sist besøkt 29.10.2013 http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet-related-networks
INTERPOL (1) Cybercrime. Sist besøkt 30.10.2013 http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
ITU (2013a) Datautforsker på ITUs nettsider. Sist besøkt 29.10.2013 http://www.itu.int/ITU-D/ict/statistics/explorer/index.html
ITU (2013b) ICT Facts and Figures Sist besøkt 29.10.2013 http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf
Jottacloud (1) Det er dine filer. Garantert! Sist besøkt 30.10.2013 http://www.jottacloud.com/nb/det-er-dine-filer-garantert/
Leira, Halvard og Ole Jacob Sending (2013b). Norge og globale maktforskyvninger. Blogginnlegg på Refleksprosjektets hjemmesider. Sist besøkt 29.10.2013 http://blogg.regjeringen.no/refleks/2013/05/08/norge-og-globale-maktforskyvninger/
NATO (1), http://www.nato.int/cps/en/natolive/topics_49633.htm, sist besøkt 29.08.13
NATO (2) http://www.nato.int/cps/en/natolive/topics_78170.htm, sist besøkt 29.08.13
NATO (3) http://www.nato.int/cps/en/natolive/news_65107.htm, sist besøkt 29.08.13
NATO (4) http://www.nato.int/cps/en/natolive/topics_66470.htm, sist besøkt 29.08.13
NATO (5) http://www.nato.int/cps/en/natolive/topics_69332.htm, sist besøkt 29.08.13
NATO ACO, http://www.aco.nato.int/saceur/looking-ahead-building-bridges-three-big-issues.aspx, sist besøkt 29.08.13
NORDEFCO, http://www.nordefco.org/The-basics-about-NORDEFCO, sist besøkt 29.08.13
Norges delegasjon til FN, http://www.norway-geneva.org/unitednations/humanrights/17th-session-of-the-Human-Rights-Council/, sist besøkt 29.08.13
NRK, http://www.nrk.no/nyheter/verden/1.8178990, sist besøkt 29.08.13
NSM (1) Om NSM: Organisasjon. Sist besøkt 29.10.2013 https://www.nsm.stat.no/Om-NSM/Organisasjon/
NSM (2) Varslingssystem for Digital Infrastruktur (VDI). Sist besøkt 29.10.2013 https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/VDI/

NSM (3). Hva er NorCERT?. Sist besøkt 30.10.2013 https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/Om-NorCERT/

Oslo Militære Samfunn, *Foredrag av Sjef Cyberforsvaret* http://www.oslomilsamfund.no/oms_arkiv/2013/2013-02-18-Sundseth.html, sist besøkt 29.08.13

OSSE, http://www.osce.org/home/76011, sist besøkt 29.08.13

Oxford Dictionaries, http://oxforddictionaries.com/definition/english/globalization, sist besøkt 29.08.13

Port- og teletilsynet, http://www.npt.no/aktuelt/nyheter/ny-traktat-om-internasjonal-teleregulering, siste besøkt 29.08.13

Regjeringen (1), http://www.regjeringen.no/nb/sub/europaportalen/fakta-115259/kort-om-eu.html?id=685170, sist besøkt 29.08.13

Regjeringen (2), http://www.regjeringen.no/nb/sub/europaportalen/norge-og-eu/utenriks-sikkerhetspolitisk-samarbeid.html?id=684931, sist besøkt 29.08.13

Regjeringen (3), http://www.regjeringen.no/nb/dep/ud/tema/sikkerhetspolitikk/osse.html?id=442642, sist besøkt 29.08.13

Regjeringen (4), http://www.regjeringen.no/nb/dep/fd/tema/forsvarspolitikk/nordisk-forsvarssamarbeid-nordefco.html?id=532212, sist besøkt 29.08.13

Regjeringen (5), http://www.regjeringen.no/nb/dep/ud/tema/sikkerhetspolitikk/europaradet/norge.html?id=578539, sist besøkt 31.10.13

Schneier, Bruce (2013). Lavabit E-Mail Service Shut Down. Blogginnlegg 9 august 2013. Sist besøkt 30.10.2013 https://www.schneier.com/blog/archives/2013/08/lavabit_e-mail.html

SilentCircle (1), Announcing The Dark Mail Alliance – Founded by Silent Circle & Lavabit. Sist besøkt 30.10.2013 http://silentcircle.wordpress.com/2013/10/30/announcing-the-dark-mail-alliance-founded-by-silent-circle-lavabit/

Statnetts hjemmesider (1) Statnett blir partner i nytt nasjonalt senter i cyber- og informasjonssikkerhet. Sist besøkt 30.10.2013 http://www.statnett.no/Media/Nyheter/Nyhetsarkiv-2013/Statnett-blir-partner-i-nytt-nasjonalt-senter-i-cyber--og-informasjonssikkerhet/

Statoils nettsider (1). Sist besøkt 30.10.2013 http://www.statoil.com/no/about/pages/default.aspx

Teknisk Ukeblad, http://www.tu.no/it/2012/07/03/norsk-tillitskultur-passer-darlig-i-cyberspace, sist besøkt 29.08.13

Thon, Roar (2013). Det du gjør på nettet har konsekvenser i det virkelige liv! Forstått? Sikkerhetsbloggen, NSM 1. juli 2013. Sist besøkt 30.10.2013 http://blogg.nsm.stat.no/archives/3927

Utenriksdepartementet (2) Strategiske satsinger – resultater og prioriteringer. Sist besøkt 29.10.2013 http://www.regjeringen.no/nb/dep/ud/kampanjer/nordomradeportalen/strategiske_satsinger.html?id=663580

Utenriksdepartementet (2013). Cyberdomenet i et utenrikspolitisk perspektiv. Tale holdt av daværende utenriksminister Espen Barth Eide under Cyberkonferansen 2013. Sist besøkt 29.10.2013 http://www.regjeringen.no/nb/dokumentarkiv/stoltenberg-ii/ud/taler-og-artikler/2013/cyber_sikkerhet.html?id=725440

Utenriksdepartementet, http://www.regjeringen.no/nb/dep/ud/tema/fn/fn-systemet.html?id=447123, sist besøkt 29.08.13

Verdensbanken, http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:20687836~menuPK:282840~pagePK:210058~piPK:210062~theSitePK:282823,00.html, sist besøkt 29.08.13