Internasjonal POLITIKK Årgang 71 | Nr. 2 | 2013 | 221–228 | ISSN 0020-577X

FOKUS: CYBERSPACE

Cyberspace og sikkerhet

HANS-INGE LANGØ
M.A., vitenskapelig assistent, NUPI
hil@nupi.no

KRISTIN BERGTORA SANDVIK
S.J.D., seniorforsker, PRIO
bergtora@prio.no

Cybersikkerhet har de siste par årene seilt opp som en vesentlig utfordring for nasjonalstaten og det internasjonale samfunnet. Mens spørsmålet har fått massiv mediedekning og betydelig oppmerksomhet fra sivile og militære beslutningstagere, har den politiske tilnærmingen vært fragmentert. I tillegg finnes det liten enighet i akademia og fagmiljøer om hva fremveksten av informasjons- og kommunikasjonsteknologi vil bety for sikkerhet, nasjonalt og internasjonalt. Utviklingen av effektive strategier for å sikre cybersikkerhet reiser kompliserte spørsmål om forholdet mellom militær og sivil makt, offentlig regulering og privat initiativ og nasjonale og overnasjonale institusjoner. Denne fokusspalten har som målsetting å gi en bred innføring i den akademiske debatten rundt militærstrategiske og rettslige så vel som samfunnsmessige og teknologiske aspekter ved cybersikkerhet. I denne introduksjonen skal vi kort skissere et bakteppe for temaet. Først diskuterer vi viktige definisjoner rundt cyberspace og tilknyttede konsepter, dernest hvordan aktører kan bruke cyberspace til fiendtlige handlinger, og så hvordan status er i Norge når det gjelder nasjonal cybersikkerhet. Til sist introduserer vi de forskjellige bidragene i denne spalten.

Cyberspace og cybersikkerhet

Cyberspace er et diffust begrep som åpner for flere forskjellige definisjoner. Det er likevel en generell enighet om at cyberspace er et informasjonsmiljø eller -domene som er karakterisert av bruken av elektronikk og det elektromagnetiske spekteret for å skape, lagre, modifisere, utveksle og utnytte informasjon gjennom nettverk som bruker informasjons- og kom-

munikasjonsteknologi (Kuehl 2009: 28). Videre blir cyberspace ofte inndelt i tre lag. Det første laget er det rent *fysiske*, som består av datamaskiner, kabler, rutere og lignende. Det andre laget er det *syntaktiske*. Her ligger programvaren, og den behandler informasjonen i nettverket og styrer prosessene for hvordan informasjonen behandles og hvordan selve datasystemene opererer. Det tredje og siste laget er det *semantiske*. Dette kan kanskje best forstås som broen mellom mennesker og maskiner. Det semantiske laget viser informasjon som er relevant for brukerne, og bidrar til å skape det sosiale fellesskapet vi får når flere kobler seg opp mot samme nettverk (f.eks. internett) (Libicki 2007).

Når vi snakker om cybersikkerhet, snakker vi i første rekke om trusler mot individer, organisasjoner eller samfunn gjennom og i dette cyberspace-miljøet. Nøyaktig hvilken form denne trusselen tar varierer. Cybersikkerhet er i dag et område som berører en rekke sektorer og problemstillinger. Den voldsomme utbredelsen av IKT de siste to tiårene og integreringen av IKT på tvers av sektorer og samfunnslag, betyr at alle deler av samfunnet er berørt. Informasjonsrevolusjonen betyr også at grensene mellom disse sektorene viskes ut fordi det har oppstått gjensidig avhengighet. Hvis vi tar for oss hver enkelt av dimensjonene vi nevnte ovenfor, kan vi si at cyberspace har et tydelig sikkerhetspolitisk tilsnitt. En lang rekke stater enten vurderer å bruke eller har allerede brukt cyberdimensjonen i større operasjoner. Disse militære operasjonene kan være rettet mot andre staters militære systemer, men også mot sivil og privat sektor. Cybersikkerhet har også et betydelig økonomisk aspekt siden mange kriminelle organisasjoner bruker cyberspace for å svindle enkeltindivider og organisasjoner for betydelige beløp. Videre har cybersikkerhet et samfunnsmessig aspekt. Som illustrert i denne fokusspaltens bidrag om den sosiale dimensjonen av cyberspace, kan IKT ikke bare skape sosiale bevegelser og politisk endring, men også brukes av stater til å overvåke – og i ytterste konsekvens kontrollere – befolkningen.

Det politiske aspektet: Nye internett, nye trusler

Fordi internett er i stadig endring, er også ideer om cybersikkerhet og om forholdet mellom cyberspace og sikkerhet dynamiske: kjernen i første generasjons internett, det såkalte «Web 1.0» var bygging av IKT-infrastruktur, tilgjengeliggjøring og kommersialisering, mens Web 2.0 brakte med seg sosiale medier. Vi er nå over i «Web 3.0»-fasen hvor mobile internett, nettskyer og det såkalte «tingenes internett» smelter sammen den virtuelle og fysiske verden på nye måter. Mens internett i sin aller første fase var preget av utopiske og libertarianske ideer om en grenseløs verden, uttrykker mange kommentatorer i dag bekymring over at vi nå ser slutten

på internett: for det første fordi sosiale medier opererer som «inngjerdede hager» (slik som Apples «app»-system), og dette hindrer nyskapning (Zittrain 2008). For det andre, fordi internett i stadig større grad er gjennomkontrollert og gjennomregulert av ulike nasjonale myndigheter (Wu & Goldsmith 2008): mens internett i det store og hele var «åpent» frem til 2000, fant makthavere i årene etter stadig nye måter å begrense internettilgang på (Deibert et al. 2008) – for eksempel gjennom blue coat-teknologier som gjør det mulig å filtrere, sensurere og overvåke informasjon (Citizen Lab 2013).

Etter hvert som det har blitt utviklet en mer sofistikert overvåknings- og kontrollteknologi (Deibert et al. 2010), har man gått over i en ny fase hvor internett er åsted for interessekamp mellom nasjonale myndigheter, internasjonale selskap, sosiale bevegelser og internettaktivister (Deibert et al. 2011). Reaksjonene mot nettstedet Wikileaks og hacktivistgruppen Anonymous er eksempler på at mens cyberspace skaper muligheter for å forstyrre makthaverne så slår makten tilbake, også utenfor cyberspace. Mens konvensjonell visdom tilsa at internett vil gjøre det vanskelig for autoritære regimer å overleve, ser man at myndigheter har overvåket mobilisering via sosiale medier som Twitter og Facebook for å kunne forfølge aktivister. Mange autoritære regimer holder seg nå med et eget internettpoliti. Det er verdt å merke seg at mens anvendelse av evnen til å «skru av» internett – den såkalte «kill switch» – ble møtt med fordømmelse i Egypt og Syria, har både amerikanske og britiske politikere luftet muligheten for at en slik «kill switch» bør være en del av den politiske verktøykassen.[1]

Nettverksangrep

Ut fra et teknisk perspektiv er den største trusselen mot cybersikkerhet såkalte nettverksangrep, hvor eksterne aktører skaffer seg tilgang til nettverk gjennom hacking. Hacking betyr at en aktør bruker såkalt skadevare (malware) som «trojanere» og «ormer» for å utnytte en sårbarhet i datasystemet til målet. En hittil ukjent sårbarhet kalles *zero-day vulnerability* og kan finnes i en rekke forskjellige programvarer. Dette kan enten gjøres mot en automatisert datamaskin eller ved å lure en bruker i den andre enden til å åpne et epostvedlegg som inneholder skadevare og dermed gir adgang til vedkommendes datamaskin og dermed organisasjonens nettverk. Når hackeren har fått tilgang til datasystemet, kan de stjele, manipulere eller slette informasjon. Stjeling av informasjon kan ha rent krimi-

1. Cybersikkerhetsproblematikken overlapper også med spørsmålet om styringen av internett og rollen til grupper som Internet Governance Forum, the Internet Engineering Task Force og ICANN. Vi går ikke nærmere inn på disse problemstillingene her.

nelle formål, som å stjele kredittkortinformasjon. Dette kan gjøres ved å infisere en datamaskin med skadevare og så hente ut den nødvendige informasjonen. Enkelte grupper gjør dette i stor skala og ender da opp med hundrevis, om ikke tusenvis, av infiserte datamaskiner de kan bruke til å sende spam eller lansere cyberangrep mot betaling. Disse nettverkene kalles botnet og brukes ofte i cyberangrep. Stjeling av informasjon kan også være spionasje rettet mot enten selskaper eller statlige organer med mål å hente ut sensitive opplysninger. Manipulering av informasjon er mindre vanlig, men vil i teorien bety at fiendtlige aktører forsøker å skape forvirring og påvirke beslutningsprosesser hos en motpart uten at vedkommende er klar over dette. Sletting av informasjon har lignende formål, men det er da lettere for motparten å se at nettverket har blitt infiltrert. Denne typen inntrenginger blir kalt utnyttelsesoperasjoner (cyber network exploitation) og skiller seg fra angrep ved at de ikke direkte lammer en motparts operasjonelle kapabiliteter.

Cyberangrep kan bruke de samme metodene for å få tilgang til nettverk, men skiller seg fra utnyttelse med hvilken hensikt operasjonen har. Den mest vanlige formen for angrep er såkalte Denial of service-angrep. Angriperen vil da sende en stor mengde forespørsler til en motparts server over internett for å overvelde nettverket og gjøre det ute av stand til å opprettholde sine vanlige funksjoner. Hvis angriperen bruker et botnet til å gjøre dette, kalles det Distributed Denial of Service (DDoS). Disse formene for angrep har ikke som mål å få tilgang til nettverket, men isteden utnytte nettverkets tilgang til internett for å stoppe andres bruk av nettverket. Dette kan gjøres for å lamme internettjenester som nettbanker eller vanlige nettsider folk besøker.

Cyberangrep som bruker inntrenging har ofte lengre varighet og større effekt. Disse angrepene kan tukle med programvareprosessene innad i et nettverk for å lamme nettverket, men de kan også brukes for å påvirke prosesser utenfor cyberspace. Det meste kjente eksemplet på dette er Stuxnetormen, en meget sofistikert skadevare som brukte flere zero-day sårbarheter. Datanettverket i det iranske atomanlegget i Natanz ble infisert av Stuxnet. Ormen spredde seg så til systemene som styrte sentrifugene for urananrikelse hvor den manipulerte omdreiningene for så over tid ødelegge selve sentrifugene. USA og Israel skal ha stått bak operasjonen og viser noen av de avanserte kapabilitetene disse landene sitter på innen cybersikkerhet. Slike virtuelle angrep mot fysiske prosesser er så langt sjeldne, men mange stater er bekymret for utviklingen. I teorien kan angripere bruke slike metoder for å ødelegge vitale komponenter i kritisk infrastruktur som strømstasjoner, vannverk og telekommunikasjonsanlegg. Vi vil da potensielt se effekter tilsvarende det vi får under naturkatastrofer når strøm eller telenett blir satt ut av spill.

Hvem er aktørene?

De siste årene har vi sett en rekke typer aktører utføre cyberoperasjoner. Kriminelle organisasjoner tjener penger på å lure til seg kredittkortinformasjon, mens stater eller tilknyttede hackere stjeler informasjon fra private selskaper (ofte forsvarsleverandører) eller andre stater. Slike former for cyberkriminalitet får nå store økonomiske konsekvenser: Shamoon-virus, angrep mot Saudi-Arabias statlige oljeselskap ARAMCO i 2012, antas å ha vært det mest alvorlige angrepet mot næringsinteresser så langt (Kirk 2012). I en periode ble cyberterror fremstilt som en mulig trussel, men det finnes ingen eksempler på terrorister som har utført cyberangrep. Terrorister og terrornettverk bruker derimot internett til å spre sine ideologiske budskap, organisere seg og samle inn penger. Anders Behring Breiviks manifest er et eksempel på hvordan noen kan la seg inspirere av ekstremisme på internett og så bruke samme kanal til å spre sitt budskap. Cyberangrep fra ikke-statlige aktører kommer isteden ofte fra såkalte hacktivister (for eksempel gruppen Anonymous) som utfører angrep for å få oppmerksomhet rundt politiske saker, og vi har også sett eksempler på patriotiske hackere som utfører cyberangrep mot fiender av nasjonalstaten: de mest kjente eksemplene her er cyberangrepene mot Estland i 2007 og Georgia i 2008, hvor det antas at russiske hackere støttet av den russiske staten stod bak.

Cybersikkerhet i Norge

Cybersikkerhet har så langt bare i begrenset grad vært ansett som en utenrikspolitisk utfordring. Norge deltar i et nordisk CERT-samarbeid og har i tillegg uformelt bilateralt samarbeid med flere land. Samtidig er er Norge «contributing nation» (ikke «sponsoring nation») til NATOs «Cooperative Cyber Defence Centre of Excellence» (CCDCOE) i Estland. På nasjonalt nivå er ansvaret for cybersikkerhet i Norge i stor grad desentralisert og organisert etter sektorprinsippet. Det nyetablerte Cyberforsvaret er ansvarlig for å beskytte den militære infrastrukturen, mens den sivile siden av det offentlige er mer fraksjonert. NorCERT, som ligger under Nasjonal sikkerhetsmyndighet (NSM), er et nasjonalt senter for håndtering av alvorlige cyberangrep mot samfunnskritisk infrastruktur og informasjon, både i privat og sivil offentlig sektor. De har en forebyggende og koordinerende rolle, men kan også bistå andre organisasjoner med ekspertise under angrep. I tillegg finnes det flere responsmiljøer i enkelte viktige samfunnssektorer, som Forsvaret, helse- og omsorgssektoren og justissektoren, På departementsnivå er ansvaret delt: Justis- og beredskapsdepartementet (JD) har samordningsansvar for samfunnets sivile sikkerhet, mens

Fornyings-, administrasjons- og kirkedepartementet (FAD) har et koordinerende ansvar for regjeringens IKT-politikk. Forsvarsdepartementet (FD) har ansvaret for IKT-sikkerhet i militær sektor, mens Samferdselsdepartementet (SD) har som sektordepartement ansvar for IKT-sikkerheten knyttet til elektroniske kommunikasjonsnett og -tjenester, som Internett.

Myndighetene har i flere år jobbet med å møte de nye utfordringene i cyberspace, men arbeidet med å utvikle en ny nasjonal cyberstrategi har tatt lang tid. Et tidlig utkast fra NSM i 2009 møtte sterk motstand fra flere hold og ble senere skrinlagt til fordel for en bredere prosess. I desember 2012 ble den nye strategien for informasjonssikkerhet offentliggjort, utarbeidet i samarbeid mellom FAD, FD, JD og SD.[2] Strategien legger opp til en tredeling av ansvaret for cybersikkerhet. Myndighetene har ansvaret for at IKT-infrastrukturen er godt sikret, mens private og offentlige virksomheter sørger for sin egen informasjonsinfrastruktur for å sikre både egen virksomhet og sine kunder og brukere. Sist, men ikke minst sier strategien at den enkelte borger også må ta «selvstendig initiativ for å beskytte sin identitet, sitt eget personvern og sine egne økonomiske verdier på nett» (FAD 2012: 8).

Det finnes dermed ingen overhengende nasjonal organisasjon for cybersikkerhet, og myndighetene er isteden avhengig av at de respektive departementene og deres direktorater og etater samarbeider. Flere aktører har uttrykt sin skepsis til en sektorprinsipiell tilnærming til nasjonal cybersikkerhet, blant annet fordi angrep ofte går på tvers av sektorer og krever utstrakt samarbeid og informasjonsdeling, men det er lite som tyder på at dagens struktur vil endres med det første. Det privat næringsliv spiller en viktig rolle innen nasjonal cybersikkerhet. Telenor har her en unik rolle som eier av kritisk infrastruktur og innehaver av fagekspertise. Med bakgrunn i deres forhold til privat næringsliv og sensorer i sitt nettverk, kan de oppdage angrep først og i enkelte tilfeller spille rollen som førsteforsvarer.[3] Samtidig er det utfordringer når det gjelder informasjonsdeling mellom offentlig og privat sektor. Aktører i næringslivet har i lengre tid etterlyst mer informasjon fra offentlige myndigheter, og den nye nasjonale strategien for informasjonssikkerhet legger opp til mer samarbeid mellom det private og det offentlige.

2. Nasjonal strategi for informasjonssikkerhet og tilhørende handlingsplan 2012.

3. Dette skjedde da Nobelinstituttets hjemmeside ble hacket i 2010 og brukt til å spre skadevare til alle Firefox-brukere som besøkte nettsiden. Telenors kunder var de første som oppdaget unormal trafikk på nettet, og Telenor varslet da myndighetene om infiseringen samtidig som de utførte sin egen analyse av skadevaren og dens funksjon og formål.

Fokusspaltens bidrag

Cybersikkerhet er en teknisk, en samfunnsmessig og en menneskelig utfordring (Betz 2012).

Vår målsetting for denne fokusspalten har vært å kombinere akademiske og operasjonelle perspektiver på cybersikkerhet, samt å ha en tverrfaglig tilnærming. Representert i dette nummeret er samfunnsforskere, juridiske eksperter og militære eksperter.

I det første bidraget gir Hans-Inge Langø en oversikt over hovedretningene i den akademiske debatten rundt cybersikkerhet. Deretter følger to bidrag om cyberkrigføring: Roger Johansen diskuterer hvordan en småstat som Norge bør innrette Forsvaret for å utnytte cyberteknologien og samtidig håndtere det nye trusselbildet. Kristin Bergtora Sandvik undersøker forholdet mellom cyberkrig og internasjonal rett, og spør hvordan cybersikkerhet har gått fra å være et datasikkerhetsproblem til å bli et militært anliggende, og hvilken rolle internasjonal rett spiller i denne prosessen. De to siste bidragene fokuserer på sivile aspekt ved cybersikkerhet. Kari Steen-Johnsen, Bernard Enjolras og Dag Wollebæk viser hvordan sosiale medier skaper nye dilemmaer der samfunnets interesser kan stå i motsetning til individenes sivile rettigheter, særlig rettigheter knyttet til personvern og ytringsfrihet. I det siste bidraget analyserer Mareile Kaufmann konseptet «resiliens» som en metode for sikring av kritisk informasjonsinfrastruktur, med fokus på EUs arbeid.

Litteratur

Betz, David (2012) *Connectivity, War & Beyond Cyber War*. Tilgjengelig på http://kingsofwar.org.uk/2012/11/connectivity-war-beyond-cyber-war/comment-page-1/. Lesedato 15.01.2013.

Citizen Lab (2013) *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools*, Research Brief (13). Tilgjengelig på https://citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf

Deibert, Ronald J., John G. Palfrey, Rafal Rohozinski & Jonathan Zittrain (red.) (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge: MIT Press.

Deibert, Ronald J., John G. Palfrey, Rafal Rohozinski & Jonathan Zittrain (red.) (2010) *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge: MIT Press.

Deibert, Ronald J., John G. Palfrey, Rafal Rohozinski & Jonathan Zittrain (red.) (2011) *Access Contested: Security, Identity and Resistance in Asian cyberspace*. Cambridge: MIT Press.

Fornyings-, administrasjons- og kirkedepartementet (FAD) (2012) Nasjonal strategi for informasjonssikkerhet. Oslo: Departementenes servicesenter.

Kirk, Jeremy (2012) *Saudi Aramco restores internal network after malware*. Tilgjengelig på http://www.cso.com.au/article/434669/saudi_aramco_restores_internal_network_after_malware_attack/. Lesedato 15.01.2013.

Kuehl, Daniel T. (2009) From Cyberspace to Cyberpower: Defining the Problem. I Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz (red.) *Cyberpower and National Security*. Washington D.C.: National Defense University Press.

Libicki, Martin C. (2007) *Conquest in Cyberspace: National Security and Information Warfare* New York, NY: Cambridge University Press.

Zittrain, J. (2008) *The Future of the Internet and How to Stop It*. Yale University Press. Tilgjengelig på http://futureoftheinternet.org/static/ZittrainTheFutureoftheInternet.pdf. Lest 13.03.2012.

Wu, Tim & Jack Goldsmith (2008) *Who Controls the Internet – Illusions of a Borderless World*. Oxford: Oxford University Press.