Internasjonal POLITIKK
Årgang 74 | Nr. 4 | 2016 | ISSN 1891-5580

Bokanmeldelse

The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age

Adam Segal

New York: PublicAffairs, 2016

Anmeldt av Siri Strand*,
MSc student ved King's College London, London

En stats mulighet til å skaffe seg makt og innflytelse har tradisjonelt sett befunnet seg langs en akse fra diplomati til militærmakt. De siste årene har handlingsrommet mellom disse ytterpunktene imidlertid vokst i takt med betydningen av cyberspace. I sin siste bok, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* beskriver Adam Segal en verden der stater i stadig større grad benytter hackerangrep mot hverandre for å stjele økonomiske og militære hemmeligheter, og for å skade infrastruktur. Masseovervåkning anses for å være et effektivt virkemiddel for å skaffe seg kontroll, mens kombinasjonen av teknologi og strategisk kommunikasjon benyttes for å påvirke holdninger og skape nye narrativer. 'The hacked world order' er betegnelsen Segal bruker for å beskrive den nåværende verdensorden – en verdensorden der nye spilleregler og maktmidler gjelder. De statene som mestrer å utnytte det digitale handlingsrommet til sin fordel, vil også være de som i størst grad kommer til å påvirke verdenspolitikken i årene fremover.

Det er ikke overraskende at stater i stadig større grad anser internett for å være et sikkerhetspolitisk anliggende. I dagens verden er olje- og gassleveranser, strømnettet og finansmarkedene avhengige av et velfungerende internett. Det at stater benytter seg av kommunikasjons- og informasjonsteknologi for å oppnå nasjonale interesser er derimot ikke nytt, noe Segal også bemerker. Likevel mener Segal at det er snakk om et så fundamentalt skifte i hvordan stater operer at det er snakk om en ny tidsregning – et 'year zero' – i internasjonal politikk. Han argumenterer for at på samme måte som historikere anser 1947 som starten på den kalde krigen, kommer vi til å se tilbake på perioden mellom juni 2012 og juni 2013 som året da cyberspace ble en arena for utøvelse av statsmakt.

Mange akademikere med cybersikkerhet som fagfelt vil være skeptiske til å innføre et slikt skille. Den sikkerhetspolitiske utviklingen i cyberspace anses av flere for å ha trekk som minner mer om en *evolusjon* enn en *revolusjon*. Likevel kobler Segal

*Korrespondanse: Siri Strand, King's College London, London. Email: siri.strand@kcl.ac.uk

Citation: Siri Strand (2016). «The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age». Bokanmeldelse, Internasjonal Politikk, 74, 4: 1–4. http://dx.doi.org/10.17585/ip.v74.622

tre sentrale hendelser til perioden mellom juni 2012 og juni 2013, som han mener definerer et slikt skille for utviklingen innen sikkerhetspolitikk: Stuxnet-angrepet, økt oppmerksomhet rundt digital spionasje, og Snowden-avsløringene.

Ifølge Segal markerte Stuxnet-angrepet et vendepunkt fordi det viste at USA hadde utviklet offensive 'cybervåpen' som kunne forårsake fysisk ødeleggelse i en annen stat – og var villige til å bruke dem. I 2012 ble det kjent at amerikanske myndigheter, i samarbeid med Israel, hadde gjennomført et angrep mot Irans atomvåpenprogram med dataormen Stuxnet. Angrepet var en suksess for USA, og Segal argumenterer for at det blir stående som et eksempel til følge for andre, blant annet på grunn av de lave økonomiske og politiske kostnadene forbundet med operasjonen.

Ifølge Segal var det også i denne perioden politikere i USA fikk øynene opp for de enorme verdiene som går tapt hvert år på grunn av hackerangrep og digital industriell spionasje. I 2012 definerte sjefen for NSA, Keith Alexander, kinesiske spionasjeangrep mot amerikansk næringsliv som «the greatest transfer of wealth in history». I 2013 tok president Barack Obama initiativ til forhandlinger med president Xi Jinping for å stanse denne formen for økonomisk aktivitet. De diplomatiske forhandlingene har imidlertid gitt få resultater, og det er i følge Segal grunn til å tro at problemet bare kommer til å vokse i årene fremover.

I følge Segal kulminerte 'year zero' med Snowden-avsløringene som viste hvordan NSAs overvåkningsprogram ga myndighetene tilgang til å analysere private e-poster, telefonsamtaler og tekstmeldinger. At overvåkningsprogrammet omfattet Brasils president Dilma Rousseff, Tysklands forbundskansler Angela Merkel og minst tretti andre statsledere satte forholdet mellom USA og resten av verden på prøve. USA, som både har vært den sterkeste kritikeren av kinesisk cyberspionasje, og beskytter av et fritt og åpent internett, ble beskyldt for å være både arrogante og dobbeltmoralske. Avsløringene bidro til å forsterke ønsket fra andre stater om å begrense amerikansk innflytelse og dominans i cyberspace. Kina og Russland brukte avsløringene som argument for å få økt oppslutning rundt sitt ønske om å gi FN «makten» over internett.

Boken konkluderer med at disse hendelsene markerte starten på det mange omtaler som et militært 'våpenkappløp' i cyberspace, og satte i gang en debatt rundt hvilke regler som skal gjelde for staters handlinger i cyberdomenet. Hvem skal utforme reglene og hvordan skal man sørge for at reglene overholdes? «Kampen om cyberspace» er også en kamp om hvilke normer og regler som skal få dominere det digitale domenet.

Adam Segals bok er et omfattende prosjekt som dekker de fleste 'cyber-relaterte' utfordringer statsledere må forholde seg til i det tjueførste århundret. Ambisjonen om å dekke det brede bildet går imidlertid på bekostning av dybden i analysene. Boken inneholder lite ny empiri som bidrar til å belyse de pågående diskusjonene fra et nytt perspektiv. En erfaren leser vil kjenne igjen de fleste argumentene og eksemplene som presenteres i boken fra annen litteratur som dekker tematikken (Kaplan 2016; Stevens 2015; Clark 2010). De mer teoretiske bidragene i kapittel to bidrar derimot med nye perspektiver på et tema som ikke er like godt dekket i

tidligere litteratur, nemlig de maktpolitiske. Hva utgjør makt i cyberspace? Hvordan påvirker dette utformingen og gjennomføringen av internasjonal politikk? Og hva mener stater de *kan* og *bør* bruke denne makten til?

En positiv side ved at Segals bok dekker et bredt spekter av temaer, er at den også diskuterer en «mykere» form for maktutøvelse – nemlig *informasjonskrigføring*. Adam Segal beskriver hvordan digital strategisk kommunikasjon kan være vel så effektivt som andre maktmidler for å oppnå nasjonale interesser. Både beskrivelsene av «Twitter-krigen» mellom Israel og Hamas i 2014, kinesiske og russiske 'nettroll' som sprer nasjonalistisk propaganda og Vestens kamp mot ISIL i sosiale medier er interessant lesning. Boken avslutter noe overraskende med et kapittel om Brasils rolle i maktkampen om cyberspace, og landets innsats for å reformere den globale styringen av internett. Kapittelet belyser en viktig trend i den pågående diskusjonen om fremtidens internett, nemlig at ønsket om større «digital suverenitet» og deamerikanisering av internett ikke bare kommer fra stater som i utgangspunktet er USA-kritiske.

Inntrykket man sitter igjen med etter å ha lest Adam Segals siste bok er, ikke overraskende, at ny teknologi gjør internasjonal politikk mer kompleks og mindre forutsigbar. Segal beskriver en verden der hele 29 land har opplyst at de har evne til å utføre offensive cyberangrep, og hvor antallet stiger hvert år. I likhet med mange andre frykter Segal at dette vil kunne bidra til mer komplekse konfliktsituasjoner. Det er svært vanskelig – noen vil si umulig – å fastslå hvem som er avsenderen av et cyberangrep. Selv om det i noen tilfeller er mulig å spore hvor et angrep kommer fra, vil det fortsatt være en sjanse for at den identifiserte staten kun har blitt brukt som «gjennomfartskanal» for å skjule den opprinnelige avsenderen. Dette kan skape forvirring og ustabilitet, som historisk har vært en farlig kombinasjon i internasjonal politikk.

Henry Kissinger skriver i sin bok *World Order* (2014) at «cyberspace challenges all historical experience». Adam Segal fremstiller derimot cyberspace som en arena der politisk spenning mellom ulike aktører, i større grad enn tidligere, settes på prøve. Hvordan ny teknologi endrer maktbalansen mellom private og offentlige aktører, og mellom mektige og mindre mektige stater er viktig tematikk i denne diskusjonen.

Et vanlig syn her, er at cyberspace legger til rette for at nye aktører får økt makt på bekostning av de tradisjonelle stormaktene. Dette begrunnes med at teknologiske våpen tilrettelegger for asymmetrisk krigføring, og at de mektigste statene er mer teknologiske og dermed mer sårbare for digitale angrep. Segal peker på flere sannsynlige eksempler, deriblant cyberterrorisme og 'hacktivisme', som kan underbygge en slik teori.

Samtidig er et viktig bidrag i Segals bok at den nyanserer dette bildet ved å beskrive hvordan økonomiske ressurser, en høyt utdannet befolkning, og evne til å utvikle ny teknologi fortsatt vil gi relativ makt for de store aktørene. USA er fortsatt verdensledende innen teknologiutvikling og har utnyttet dette til å skaffe seg en ledende posisjon i cyberspace, mens Kina og Russland følger etter. Både Frankrike og Storbritannia var tidlig ute med å offentliggjøre at de hadde offensive

'cybervåpen'. Israel har uttalt at landet ønsker å bli en 'world cyber power', og står alene for 13 prosent av all verdens forskning på cybersikkerhet.

Ifølge forfatteren kan det altså på mange måter se ut som om flere av de tradisjonelle mønstrene i maktpolitikken fortsatt gjelder. Selv om både Kina og Russland trolig er i stand til uføre angrep mot strømnettet i de fleste områder, har de liten grunn til å gjøre det dersom deres vitale interesser ikke er truet. De potensielle politiske og økonomiske kostandene vil være for høye.

Segal skiller seg fra mengden med sitt bidrag til diskusjonen om cybersikkerhet. Han klarer å skrive en bok som beskriver de alvorlige utfordringene vi står overfor, uten å gå for langt i retningen av dommedagsprofetier, eller skape mistanke om at han bedriver lobbyvirksomhet for det stadig voksende 'cyber military-industrial complex'. *The Hacked World Order* er først og fremst en god introduksjonsbok for lesere som ønsker å bli kjent med en tematikk som kommer til å bli mer aktuell fremover. Til tross for at boken kan fremstå som lite strukturert, er dette en forholdsvis lettlest bok som ikke krever kjennskap til de tekniske aspektene ved cybersikkerhet. De som interesserer seg for, eller jobber med tematikken vil kjenne til Segals argumenter. De fleste politikere og beslutningstakere vil derimot ikke gjøre det, og spørsmålene som reises i boken fortjener en diskusjon.

Referanser

Clarke, Richard A. (2010) *Cyberwar: The Next Threat to National Security and What to do about It*. New York: HarperCollins Publishers.

Kaplan, Fred. (2016) *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster.

Stevens, Tim. (2015) *Cybersecurity and the Politics of Time*. Cambridge: Cambridge University Press.