Introduksjon

Som en del av den russiske invasjonen i februar 2022 ble Ukraina bombardert med 40 destruktive cyberangrep, som til sammen rammet hundrevis av datasystemer i ukrainske medieorganisasjoner og offentlige etater (Microsoft, 2022, 2023). I kjølvannet av Israels krig mot Hamas i oktober 2023 har politiske aktivister angrepet og utilgjengeliggjort både israelske og palestinske nettsider (Newman & Burgess, 2023). I juli 2023 knelte statlige online-tjenester og den viktigste betalingstjenesten i Kenya under såkalte tjenestenektangrep utført av grupperingen Anonymous Sudan (Sambuli, 2023). I Norge har Stortingets og departementenes e-postsystemer flere ganger blitt infiltrert av utenlandsk etterretning (Staff, 2020; Alnes et al., 2021; Bulai & Haraldsen, 2023). Valgpåvirkning og såkalte trollfabrikker har blitt omtalt som en gift for demokratiet og en eksistensiell trussel mot borgernes tillit.

Dette er bare noen få utvalgte eksempler på hvordan cyberdomenet har blitt brukt som arena og verktøy i krigføring og konflikt. Cyberdomenet utgjør i dag en sentral del av moderne krigføring. Men hvordan skiller maktbruk og krigføring i cyberdomenet seg fra andre og mer tradisjonelle former for maktutøvelse? I denne boken gjør vi et dypdykk i begrepet cybermakt og presenterer denne nye arenaen for et norsk publikum. Boken samler bidrag fra en rekke disipliner og fagtradisjoner, og inkluderer forfattere med operativ erfaring med håndtering av cybersikkerhetshendelser.

Digitaliseringen av alle sider og aspekter av samfunnet er historisk sett ny. Men den har beveget digital sikkerhet fra et teknologisk fagområde til et globalt strategisk tema. Dette fører også med seg nye former for rivalisering mellom stater. Tid og rom i cyberdomenet er unikt og ulikt andre krigføringsdomener. Rivaliserende parter kan bygge sin egen slagmark, og avstand og tidsforsinkelse korresponderer ikke med hvordan vi er vant til å tenke. Lange kjeder av gjensidige avhengigheter kan skape uventede effekter. For en angriper er det nesten bare fantasien som setter grenser, og kjøreregelene for hva som er lov og akseptabelt er i beste fall umodne. Vi kan alltid stille spørsmål om hvorvidt det er krigens natur *eller* krigens karakter som endrer seg, men det som er sikkert, er at etter hvert som *cyber* omfavner stadig flere aspekter ved sikkerhetspolitikken, akselererer også diskusjonen om hvorvidt domenet vil resultere i et nytt uttrykk for makt.[1]

Vårt utgangspunkt er at mange spørsmål rundt cyberkrig, cyberoperasjoner og cybermakt fremdeles er uavklart og må undersøkes empirisk.[2] Vi trenger solide analyser av hvordan det digitale rom brukes

[1] For ytterligere diskusjon, se for eksempel Strachan og Scheipers (2011), Echevarria (2005), Halpin et al. (2006) og Sloan (2002).
[2] Vi har valgt å ikke dykke særlig langt inn i diskusjon rundt kategorisering av cyberkrig versus cyberfred, og hvordan en slik tilstand vil vise seg i praksis. Tematikken tangeres dog av Cooper (kapittel 11) og Lein et al. (kapittel 10) med vurderinger av det juridiske bakteppet rundt cyberoperasjoner. Aannø (kapittel 4) inkluderer en vurdering av internasjonale normers potensial for avskrekking.

Referanse: Berrefjord, V. R. & Lund, M. S. (2024). Introduksjon. I V. R. Berrefjord & M. S. Lund (Red.), *Cybermakt – en tverrfaglig innføring* (s. 12–22). Universitetsforlaget.

som arena for maktkamp, hvor stater posisjonerer seg gjennom insentiver, postulering og allianser, men også som en mer vidtfavnende plattform for strategisk manipulasjon og påvirkning. Denne boken tar derfor i stor grad utgangspunkt i *cyberoperasjoner*, som en samlebetegnelse for staters makt*utøvelse* i cyberdomenet. Altså er operasjonene uttrykk for hvordan stater utøver sitt virke i den hensikt å bygge eller bruke sin makt. Vi har valgt å rette oppmerksomheten mot operasjoner hvor staten er toneangivende, enten det er som den operative aktør eller som instruerende myndighet i partnerskap med kriminelle eller kommersielle partnere.[3] Vi retter oss også inn mot *operasjonell* maktutøvelse og bruker en del plass på å empirisk presentere hvordan operasjonene blir gjennomført. Dette gir en noe deskriptiv natur, det er et valg vi har tatt fordi vi søker å gi leseren et grunnlag for å forstå og vurdere fremtidige cyberhendelser.

Tilbakeblikk

Cybersikkerhet er ikke lenger et rent teknologisk fagområde, og mange ulike akademiske disipliner har fattet interesse for feltet. Det siste tiåret har særlig litteratur fra internasjonale relasjoner og sikkerhetsstudier blitt brukt for å forstå hvordan stater kan bruke det digitale domenet for politisk og militære formål (Cavelty & Wenger, 2020; se også Borghard & Lonergan, 2017; Kello 2017; Maness & Valeriano, 2016; Zuiderveen Borgesius et al., 2018), og juridisk litteratur for å etablere anvendelse av juridiske og folkerettslige normer i cyberdomenet (Schmitt, 2017; Osula & Rõigas, 2016).

En kort innføring er nyttig: Da cybermakt og cyberoperasjoner først kom på banen var det i form av en frykt for at sårbar infrastruktur gjennom dominoeffekter kunne ende opp i et «Cyber Pearl Harbor». Arquilla og Ronfeldts (1993) definerende artikkel «Cyberwar is coming!» slår eksempelvis fast at cyberkrig representerte et paradigmeskifte innen teknologi og doktrine, som i ytterste konsekvens kan utfordre den eksisterende verdensorden. Det innebar et krise-krig-spekter med mulighet for total samfunnskollaps etter hvert som digital avhengighet brer om seg. Dette perspektivet ble etter hvert popularisert gjennom filmer og TV-serier hvor et eneste tastetrykk kan skru av livsviktige tjenester som strøm, vann, helsevesen og transport. Drivkraften i historien ble dermed heltens dramatiske kamp mot klokken, ikke en bred digital grunnsikring og et apparat for hendelseshåndtering.

En annen anskuelse på domenets potensial kan illustreres med Eric Gartzke, Thomas Rid og Ben Buchanan. Gartzke (2013) utfordret raskt Arquilla og Ronfeldt med at cyberkrig må måles etter hvorvidt den tilbyr et selvstendig politisk instrument tilsvarende (trussel om) tvang og makt, i tråd med Clausewitz' anskuelse av krig som en forlengelse av politikken. Gartzke argumenterte videre for at cyberoperasjoner ikke makter dette, og at det digitale domenet kun tilbyr et supplerende middel som vil forsterke status quo. Thomas Rids sentrale verk *Cyberwar will not take place* (2013) tar også

[3] Cyberdomenets natur kompliserer attribusjon, og det vil eksistere gråsoner samt hybride modeller med for eksempel strategiske partnerskap av statssponsende grupperinger, kriminelle eller saksdrevne kollektiver. Dette ligger som et bakteppe i flere kapitler, og diskusjon rundt hvem som er stridende, behandles direkte av Cooper (kapittel 11).

utgangspunkt i Clausewitz' forståelse av krigens formål. Han argumenterer for at den reelle cybertrussel er langsiktig strategisk bruk av cyberdomenet, altså spionasje, sabotasje og subversjon (som kan oversettes til undergraving) hvor konstante små kutt eroderer eierskap over egen informasjon, systemers integritet, informasjons troverdighet og samfunnets samhold (Rid, 2012, 2013, 2020). Ben Buchanans (2020) nyere bok *The hacker and the state* funderes i geopolitikken og anser tilsvarende cyberangreps forming (shaping) av mellomstatlige forhold som basert på tre pilarer: spionasje, angrep og destabilisering (Buchanan, 2020, s. 8).

Tar vi et empirisk utgangspunkt, kan oppdagelsen av skadevaren Stuxnet og den påfølgende avsløringen av Operation Olympic Games (2010), Snowden-avsløringene (2013) og Cambridge Analytica-skandalen (2018) anses som milepæler i forståelsen av cyberoperasjonenes antatte potensial. Stuxnet og Olympic Games var en sofistikert cyberoperasjon mot et antatt sikkert anlegg (for anrikning av uran) som var avskåret fra internett, og som viste at man kunne skape kinetiske effekter i den fysiske verden via cyberdomenet (se Aanonsen, Jakobsen og Schia, kapittel 1 i denne boken). Edward Snowdens dokumentlekkasjer allmenngjorde klassifiserte, globale overvåkningsprogrammer og hvordan tette bånd mellom private og statlige organer bygget opp under cybermakten. Cambridge Analyticas kommersielle salg av mikromålrettede digitale kampanjer satte en ny fasett av sosiale medier på agendaen. Tidligere ble de sosiale mediene i hovedsak ansett som en sosio-politisk kommunikasjonsplattform, og fra et sikkerhetspolitisk perspektiv primært relevant som en tilrettelegger og mulig akselerator for folkebevegelser som sett under den arabiske våren. Manipulasjon eller såkalt *weaponification* av store data løftet valgpåvirkning og russiske trollfabrikker inn i hva vi kan anse som cyberoperasjoner. Nå ser vi tendenser til at den såkalte overvåkningsøkonomiens stadig mer detaljrike digitale datainnsamling blir koblet opp mot fundamentale risikoer for operasjonell sikkerhet og etterretning i tillegg til personvern, individets autonomi og frie vilje. (Se for eksempel Christl, 2017; Lyon, 2007; Zuboff, 2019 og Twetman & Bergmanis-Korats, 2021).

Maktutøvelse i cyberdomenet

Også i cyberdomenet er makt sentralt. Maktbegrepet utgjør derfor et naturlig utgangspunkt for undersøkelsene våre. I sin simpleste form handler makt om å få det som man vil. I en mellomstatlig relasjon spiller dette seg ut ved at stat A kan få stat B til å oppføre seg slik stat A ønsker (Dahl, 1957). Steven Lukes skiller mellom beslutningsmakt, ikke-beslutningsmakt og ideologisk makt (Lukes, 1974). Hard makt blir i så måte en aggressiv form for makt, hvor typisk økonomiske eller militære midler anvendes for å fremme egne målsettinger. Det kan forstås som evne til å påtvinge andre noe (Wilson, 2008). Myk makt er på den annen side evnen til å lede gjennom tiltrekningskraft (Nye, 2010, 2011, 2017). Joseph S. Nye forklarer det som følger:

> *Power is the ability to affect others to get the outcomes one prefers, and that can be accomplished by coercion, payment, or attraction and persuasion. Soft power is the ability to obtain preferred outcomes by attraction rather than coercion or payment.* (Nye, 2017)

Hard makt blir altså evnen til å *pålegge* noen å gjøre noe; ved hjelp av pisk eller gulrot, ved kommunikasjon, diplomati eller tvang. Myk makt omhandler derimot As evne til å forme Bs *vilje.* Altså i hvilken grad A bruker ideologi, kultur, eksempler eller institusjoner til å overtale eller forme Bs strategier. Når vi i bokens struktur gjør et skille mellom hard og myk cybermakt, er det denne forståelsen av hard og myk makt som ligger til grunn.

Med dette i mente er det her hensiktsmessig å ta utgangspunkt i en vid forståelse av makt i det digitale domenet som «staters bruk av sine cyberkapabiliteter for å realisere nasjonale målsettinger» (Voo et al., 2022, s. 7; vår oversettelse). Rammeverket National Cyber Power Index, som blir vedlikeholdt av Belfer Center for Science and International Affairs ved Harvard University, omfavner for eksempel en rekke aspekter ved statens cyberstrategi, offensive og defensive kapabiliteter, ressursbruk, privat sektor, arbeidskrafts kompetanse og et lands innovasjonsevne. Slik tilbys en mer holistisk inngang for å analysere hvordan stater utnytter det digitale domenets potensial langs syv parametere: innlandsovervåkning, utlandsetterretning, normsetting og evne til informasjonsmanipulasjon, økonomisk vekst, ødeleggelse av motparts infrastruktur og defensiv styrkeoppbygging (Voo et al., 2020a, 2020b, 2022). Med et slikt utgangspunkt blir *cybermakt* et resultat av *både* kapabilitet *og* evne til å realisere sin intensjon (Voo et al., 2020a).

Cyberoperasjoner blir i så måte byggesteinene i strategisk bruk av det digitale domenet. Men, som denne boken vil vise, finnes det ikke noen allmenn akseptert definisjon, forståelse eller avgrensing av hva som *utgjør* en cyberoperasjon. Noen kretser – særlig de militære – vil operere med snevre definisjoner av cyberoperasjoner og avgrense dem til teknisk utnyttelse av sikkerhetshull i programvare. Andre vil inkludere et bredt spekter av aktiviteter utført i eller gjennom cyberdomenet, herunder spionasje, hybrid krigføring, valgmanipulasjon og påvirkningsoperasjoner. Hvordan en cybertrussel forstås, legger føringer for strategisk beredskap og hendelseshåndtering. Alle trenger ikke være enig eller jobbe likt, men fordi digitalisering er samfunnsovergripende, er det særdeles viktig at de ulike leirene utvikler en gjensidig respekt for hverandres virkelighetsforståelse, trusselvurdering og taktiske verktøykasse.

Bokens tilnærming

I denne antologien har vi samlet en rekke eksperter for å diskutere hva *de* anser som de mest sentrale problemstillingene og eksemplene på hvordan stater har anvendt det digitale rom for maktakkumulasjon, og hva som kreves for å bygge robusthet i cyberdomenet. Disse eksemplene illustrerer altså hva et mangesidig kollegium anser som vannskiller i cyberdomenets relativt korte historie. Eksemplene spenner fra mer velkjente cyberangrep som Stuxnet, NotPetya og den

amerikanske presidentvalgkampen i 2016, til mindre kjente operasjoner som Operation Glowing Symphony, Pegasus-spionvaren og håndteringen av cyberangrep mot statsforvalterne og Helse Sør-Øst. Slik bidrar vi til å styrke bruken av empiri i studiet av cyberoperasjoner og tilgjengeliggjør kunnskap og forståelse for et bredt publikum. Mange av casene presenteres i dybden på norsk for første gang.

Bokens bidragsytere inkluderer statsvitere, psykologer, sosiologer, informatikere, jurister, offiserer og filosofer. En rekke av forfatterne har også skrevet omfattende om cyberrelaterte tema tidligere. De har fått mulighet til å skrive i sine respektive fagtradisjoner og med egne definisjoner og problemforståelser. Flere av forfatterne er også operative innen sine disipliner og trekker dermed på egenerfaring med for eksempel hendelseshåndtering av større cyberhendelser. Dette anser vi som en styrke og et utgangspunkt for antologiens prosjekt. I samme ånd er det en målsetting at boken ikke skal ha et rent akademisk preg. Den inkluderer derfor også kapitler fra praksisfeltet. Kildene er derfor mangfoldige: fagfellevurdert forskning og staters avgraderte strategidokumenter; en rekke rapporter fra forskningsprosjekter, tenketanker, ikke-statlige organisasjoner og cybersikkerhetsfirma; i tillegg til nasjonale og internasjonale nyhetssaker. Kildene er norske og engelske, og har en vridning mot sekundærkilder for å sikre ugradert innhold.

Ambisjonen med boken er å bidra til en rikere og mer tverrfaglig samtale. Vi har derfor tilstrebet et tilgjengelig språk, og boken har et relativt høyt detaljnivå. Slik håper vi at lesere fra eksempelvis sikkerhetsledelse, militære studier, beredskap og krisehåndtering, statsvitenskap og teknologiske fag kan ha utbytte av boken. Her bygger vi på en god norsk fagtradisjon etablert blant annet av Hans-Inge Langø og Kristin Bergtora Sandvik med flere i fokusnummeret *Cyberspace* (Langø & Sandvik, 2013), Niels Nagelhus Schia med flere i fokusnummeret *Cybersikkerhet* (Schia, 2019), Karsten Friis og Jens Ringsmose (2016) i boken *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*, og Karsten Friis og Håkon Bergsjø (2022) i boken *Digitalisering og internasjonal politikk*. Et annet sentralt bakteppe er det grundige og omfattende utredningsarbeidet vi finner i rapportene til blant annet Digitalt sårbarhetsutvalg (Lysne I) (NOU 2015: 13) og IKT-sikkerhetsutvalget (NOU 2018: 14) – som har vært toneangivende for utviklingen av norsk hendelseshåndtering i cyberdomenet – og dessuten videreføringen av dette i Forsvarskommisjonen av 2021 (NOU 2023: 14) og Totalberedskapskommisjonen (NOU 2023: 17).

Denne boken springer ut av (og er finansiert av) et tverrfaglig miljø ved Forsvarets høgskole, på lik linje med redaktørenes forrige samarbeid «Jakten på Norges militære cyberstrategi» (Wilhelmsen [Berrefjord] et al., 2021).

Bokens struktur

Boken er delt i fire tematiske deler som tar for seg henholdsvis hard og myk makt i cyberdomenet, det normative handlingsrommet for cyberoperasjoner og faktisk hendelseshåndtering.

Den første delen ser på cyberoperasjoner som et verktøy for hard makt. Selv om statsledede destruktive cyberoperasjoner utgjør et relativt lite volum av det totale antallet cyberoperasjoner, vil de likevel utgjøre en definerende side av cybermakt. Det er derfor et naturlig sted å starte. Videre omfatter den harde cybermakten maktmidler for å avskrekke og bekjempe fiendtlige cyberoperasjoner. I kapittel 1 tar Claudia Aanonsen, Eskil Jakobsen og Niels Nagelhus Schia for seg cyberangrepet Operation Olympic Games som USA og Israel utførte mot et iransk urananrikingsanlegg ved hjelp av skadevaren Stuxnet. Dette angrepet blir av mange sett på som det første eksempelet på et *cybervåpen*, og som startskuddet for strategisk og politisk bruk av sabotasje via cyberdomenet. Kapittel 2 og 3 vier Mass Soldal Lund til bruk av offensive cyberoperasjoner i internasjonale konflikter. Som diskutert i kapittel 2 er Operasjon Dempa Melodi et tidlig, men like fullt sjeldent eksempel på et destruktivt cyberangrep med en militær operativ effekt. I kapittel 3 tar han for seg tjenestenektangrepene mot Estland i 2007 og Georgia i 2008, som er blant de første eksemplene på bruk av cybermakt i internasjonal konflikt. I kapittel 4 tar Stig Tore Aannø utgangspunkt i NetPetya-skadevaren for å vurdere muligheten for avskrekking i cyberdomenet fra et småstatsperspektiv. I kapittel 5 ser Geir Olav Dyrkolbotn, Benjamin J. Knox og Roger Johnsen nærmere på defensive cyberoperasjoner i en norsk militær kontekst. I kapittel 6 viser Johanne Jensen Skeie hvordan utnyttelse av iboende sårbarheter i kunstig intelligens kan skape helt nye angrepsflater i fremtidige cyberoperasjoner.

Den andre delen tar utgangspunkt i det som gjerne omtales som myk cybermakt, altså påvirkningsoperasjoner myntet på å forme mottagers verdensanskuelse og strategi. Påvirkningskampanjer regnes ikke alltid som cyberoperasjoner, men påvirkning gjennom cyberdomenet har like fullt blitt et sentralt virkemiddel i moderne konflikter gjennom strategier for historiefortelling og manipulasjon. I kapittel 7 bruker Torbjørn Kveberg og Vårin Alme presidentvalgkampene i USA (2016), Frankrike (2017) og Ukraina (2014) for å vise cyberoperasjoner som en integrert del av påvirkningskampanjer. I kapittel 8 tar Arild Bergh oss gjennom en historisk analyse og viser hvordan sosiale medier har fundamentalt endret mulighetsrommet for påvirkning, propaganda og desinformasjon. Bergh bruker covid-19-pandemien for å belyse cyber-sosial påvirkning som et sosio-teknisk økosystem. I kapittel 9 viser Tobias Sæther frem nyansene gjennom å illustrere hvordan *hva som kommuniseres* digitalt, setter begrensninger og forutsetninger for påvirkningskampanjer.

Den tredje delen utforsker det normative handlingsrommet for cyberoperasjoner – altså utøvelsens rammeverk i både juridisk og etisk forstand. I kapittel 10 drøfter Aurora Brændvik Lein, Kaja Reneflot Moe og Oda Marie Bjørvik den folkerettslige gråsonen for cyberoperasjoner under terskelen for væpnede angrep. I kapittel 11 tar Camilla Cooper for seg krigens folkerett og reglene som gjelder for cyberoperasjoner i væpnede konflikter gjennom en casestudie av Operation Glowing Symphony, en amerikansk cyberoperasjon rettet mot Den islamske staten (ISIL). I kapittel 12 viser Vivi Ringnes Berrefjord hvordan cyberdomenet muliggjør maktforskyvning i favør av kommersielle aktører,

kapabilitetsspredning med påfølgende risiko for eskalering og at partnerskap kan undergrave ansvarlighet. I kapittel 13 presenterer Kirsi Helkala og Henrik Syse et etisk rammeverk for bruk av kunstig intelligens i cyberoperasjoner.

Antologiens fjerde del løfter frem noen sentrale erfaringer fra hendelseshåndtering av faktiske hendelser. Slik håper vi å peke på en retning for styrket nasjonal digital motstandskraft. Simen Bakke tar i kapittel 14 utgangspunkt i to sentrale cyberoperasjoner i 2020–2021, og evaluerer norsk og amerikansk håndtering med utgangspunkt i ulike cybersikkerhetsstrategier og politiske rammevilkår. I kapittel 15 diskuterer Aasmund Thuv og Geir Enemo tilsvarende cyberangrepene på Helse Sør-Øst og fylkesmannsembetene i 2017–2018 for å gi et innblikk i hvordan håndtering av cyberangrep mot norske statlige virksomheter fungerer. I kapittel 16, bokens avslutningskapittel, tar Torvald F. Ask, Benjamin J. Knox, Stefan Sütterlin og Ricardo G. Lugo utgangpunkt i kognitiv krigføring og illustrerer kognitive cyberangrep gjennom en fiktiv utvikling av krigen mellom Russland og Ukraina.

Innledningsvis slo vi fast at digitalisering omfatter alle deler av samfunnet. Farer kan være dramatiske angrep, men oftere snikende infiltrasjoner over tid. Terrenget er menneskeskapt, og «tradisjonelle» regler for tid og rom gjelder ikke nødvendigvis. Det skaper et unikt spekter av risiko og mulighet. Det kompliserer også beredskap og hendelseshåndtering. Cyberdomenet forutsetter dermed at fagdisipliner og sektorer makter å snakke sammen og se helheten. De må ikke nødvendigvis anvende det samme språket, men de må ha forståelse for hverandres perspektiv og virkelighet. Denne boken søker ikke å konkludere, men derimot å starte en samtale om hvordan cyberdomenet kan anvendes og beskyttes. Bidragenes detaljrikdom vil legge grunnlaget for å vurdere risiko og mulighet, og forhåpentlig bidra til både økt forståelse for og tverrfaglig samtale om hvordan vi bedre kan møte cyberdomenets utfordringer.

Oslo/Lillehammer, 8. januar 2024.

Vivi Ringnes Berrefjord og Mass Soldal Lund

Referanser

Alnes, E., Skårdalsmo, K., Gundersen, M., Tomter, L. & Thommessen, J. K. (2021, 10. mars 2021). Stortinget er utsett for dataangrep – data skal vere henta ut. *NRK*. https://www.nrk.no/norge/stortinget-utsett-for-nytt-dataangrep-1.15411279

Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141–165.

Friis, K. & Bergsjø, H. (2022). *Digitalisering og internasjonal politikk.* Universitetsforlaget.

Borghard, E. D. & Lonergan, S. W. (2017). The Logic of Coercion in Cyberspace. *Security Studies, 26*(3), 452–481.

Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.

Bulai, E. M. & Haraldsen, S. (2023, 25. juli). Hackerne kan fortsatt være inne i regjeringens systemer. *NRK*. https://www.nrk.no/norge/12-departementer-angrepet_-hackerne-kan-fortsatt-vaere-inne-i-regjeringens-systemer-1.16493620

Cavelty, M. D. & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5–32.

Christl, W. (2017). *Corporate Surveillance in Everyday Life How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*. Cracked Labs. https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Dahl, R. A. (1957). The Concept of Power. *Behavioral science, 2*(3), 201–215.

Echevarria, A. J. (2005). *Fourth-Generation War and Other Myths*. Strategic Studies Institute.

Friis, K. & Ringsmose, J. (red.). (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives.* Routledge.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security, 38*(2), 41–73.

Greenberg, A. (2023, 12. september). China-Linked Hackers Breached a Power Grid – Again. *Wired*. https://www.wired.com/story/china-redfly-power-grid-cyberattack-asia/

Halpin, E. F., Trevorrow, P., Webb, D. & Wright, S. (red.). (2006). *Cyberwar, netwar and the revolution in military affairs.* Palgrave Macmillan

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Langø, H.-I. & Sandvik, K. B. (red.) (2013). Fokus: Cyberspace. *Internasjonal Politikk, 71*(2).

Lukes, S. (1974). *Power: A Radical View.* Macmillan.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity Press.

Maness, R. C. &Valeriano, B. (2016). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society, 42*(2), 301–323.

Microsoft. (2022). *Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine*. https://aka.ms/ukrainespecialreport

Microsoft. (2023). *A year of Russian hybrid warfare in Ukraine. What we have learned about nation state tactics so far and what may be on the horizon*. https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

Newman, L. H. & Burgess, M. (2023, 9. oktober). Activist Hackers Are Racing Into the Israel-Hamas War – for Both Sides. *Wired*. https://www.wired.com/story/israel-hamas-war-hacktivism/

NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

NOU 2018: 14. (2018). *IKT-sikkerhet i alle ledd. Organisering og regulering av nasjonal IKT-sikkerhet*. Justis- og beredskapsdepartementet.

NOU 2023: 14. (2023). *Forsvarskommisjonen av 2021. Forsvar for fred og frihet*. Forsvarsdepartementet.

NOU 2023: 17. (2023). *Nå er det alvor. Rustet for en usikker fremtid*. Justis- og beredskapsdepartementet.

Nye, J. S., jr. (2010). *Cyber power*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf

Nye, J. S., jr. (2011). *The future of power*. PublicAffairs.

Nye, J. S., jr. (2017). Soft power: the origins and political progress of a concept. *Palgrave Communications*, 3(1), 17008.

Oslua, A.-M. & Rõigas, H. (red.). (2016). *International Cyber Norms Legal, Policy & Industry Perspectives*. NATO CCD COE Publications.

Rid, T. (2012). Cyber War Will Not Take Place. *The Journal of Strategic Studies, 35*(1), 5–32.

Rid, T. (2013). *Cyberwar will not take place*. Oxford University Press.

Rid, T. (2020). *Active measures: the secret history of disinformation and political warfare*. Farrar, Straus og Giroux.

Sambuli, N. (2023, 12. september). When the Rubber Meets the Road: Cybersecurity and Kenya's Digital Superhighway. *Carnigie Endowment for International Peace. https://carnegieendowment.org/2023/10/12/when-rubber-meets-road-cybersecurity-and-kenya-s-digital-superhighway-pub-90766https:/carnegieendowment.org/2023/10/12/when-rubber-meets-road-cybersecurity-and-kenya-s-digital-superhighway-pub-90766*

Schia, N. N. (red.). (2019). Fokus: Cybersikkerhet. *Internasjonal Politikk, 77*(3).

Schmitt, M. N. (2017). *Tallin Manual 2.0 on international law applicable to cyber operations*. Cambridge University Press.

Sloan, E. C. (2002). *Revolution in Military Affairs. Implications for Canada and NATO*. McGill-Queen's University Press.

Staff, A. K. B. (2020, 8. desember). Datainnbruddet mot Stortinget er ferdig etterforsket. *Politiets sikkerhetstjeneste*. https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

Strachan, H. & Scheipers, S. (red.). (2011). *The changing character of war*. Oxford University Press.

Twetman, H. & Bergmanis-Korats, G. (2021). *Data Brokers and Security. Risks and vulnerabilities related to commercially available data.* NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/data-brokers-and-security/17

Voo, J., Hemani, I. & Cassidy, D. (2022). *National Cyber Power Index 2022*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/national-cyber-power-index-2022

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D. & Schwarzenbach, A. (2020a). *Reconceptualizing Cyber Power*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/reconceptualizing-cyber-power

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D. & Schwarzenbach, A. (2020b). *National Cyber Power Index 2020*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/national-cyber-power-index-2020

Wilhelmsen, V., Larsen, T., Lund, M., Svenungsen, B. & Aannø, S. (2021). Jakten på Norges militære cyberstrategi. I T. Heier (red.), *Militærmakt i nord* (s. 242–262). Universitetsforlaget.

Wilson, E. J. I. (2008). Hard power, soft power, smart power. *The Annals of the American Academy of Political and Social Science, 616*(1), 110–124.

Zuboff, S. (2019). *The Age of Surveillance Capitalism. The fight for a Human Future at the New Forntier of Power*. Public Affairs.

Zuiderveen Borgesius, F. J., Möller, J., Kruikemeier, S., Ó Fathaigh, R., Irion, K., Dobber, T., Bodo, B. & de Vreese, C. (2018). Online Political Microtargeting: Promises and Threats for Democracy. *Utrecht Law Review, 14*(1), 82–96.