FFI Forsvarets forskningsinstitutt

22/01758

FFI-RAPPORT

Økonomisk statshåndverk, teknologisk utvikling og implikasjoner for norsk sikkerhet

– en forstudie

Kristin Waage
Petter Y. Lindgren

Økonomisk statshåndverk, teknologisk utvikling og implikasjoner for norsk sikkerhet – en forstudie

Kristin Waage
Petter Y. Lindgren

Forsvarets forskningsinstitutt (FFI) 7. november 2022

Emneord
Nasjonal sikkerhet
Makt
Teknologisk utvikling
Makroøkonomi
Investering

FFI-rapport
22/01758

Prosjektnummer
5721

Elektronisk ISBN
978-82-464-3439-1

Engelsk tittel
Economic statecraft, technological development and implications for Norwegian security – a preliminary study

Godkjennere
Kari Røren Strand, *forskningsleder*
Sverre N. Kvalvik, *forskningssjef*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Den teknologiske utviklingen vil endre hvordan stater kan benytte økonomiske virkemidler for å fremme sine interesser i internasjonal politikk, men dette er i liten grad behandlet i eksisterende litteratur om økonomisk statshåndverk. Formålet med denne rapporten er å styrke forståelsen av hvordan den teknologiske utviklingen kan påvirke staters evne til å bruke økonomiske virkemidler og å drøfte implikasjoner for norsk sikkerhet. Rapporten fokuserer spesielt på kunstig intelligens og stordata, 5G, skytjenester og tingenes internett. Data er samlet inn fra intervjuer og workshop med forskere ved FFI samt gjennomgang av eksisterende litteratur.

Vi identifiserer først flere måter den teknologiske utviklingen kan påvirke økonomisk aktivitet, inkludert økt betydning av data, mer komplekse og kompetansekrevende produkter, tjenester og verdikjeder, økt markedskonsentrasjon og økt internasjonalisering og/eller automatisering. Dette gjør oss i stand til å drøfte hvordan staters muligheter til å utføre økonomisk statshåndverk potensielt blir endret av teknologiske fremsteg. Vi skiller mellom økonomisk statshåndverk hvor en stat utøver makt og hvor en stat akkumulerer makt som muliggjør fremtidig virkemiddelbruk, også med ikke-økonomiske virkemidler. Innen utøvelse av makt, vurderer vi at den teknologiske utviklingen blant annet vil kunne styrke enkelte staters muligheter til å utnytte avhengigheter til kompetanse, ressurser, komponenter, osv. til (fordekt) å sabotere systemer. Innen akkumulering av makt, vurderer vi at den teknologiske utviklingen særlig vil styrke mulighetene til å utnytte økonomisk aktivitet til å hente inn informasjon og data, til bruk i etterretningsformål og/eller til å forsøke å forme (sær)interesser og oppfatninger i mottakerlandet. Enkelte stater kan i tillegg oppnå økte muligheter til å etablere seg som en sentral leverandør av viktige ressurser, produkter og kompetanse, og slike avhengigheter kan i neste omgang åpne muligheter for strategisk bruk for å fremme disse statenes interesser globalt. Den teknologiske utviklingen driver også stater, særlig USA og Kina, til å implementere innenlandsk næringspolitikk for geopolitiske formål – i litteraturen kalt «det nye økonomiske statshåndverket».

Hva har dette å si for norsk sikkerhet? Vi argumenterer for at det blir stadig viktigere å forvalte data som produseres i det norske samfunnet som en strategisk ressurs. Vi vurderer også at ny teknologi bidrar til at Norge kan bli mer avhengig av visse typer kompetanse, tjenester, råvarer, komponenter og produkter, og at det er behov for å skaffe en bedre oversikt over hvilke typer som er kritiske for norsk sikkerhet, med tilhørende leverandører. Videre tror vi at rivaliseringen mellom USA og Kina i økende grad også vil ha implikasjoner for Norge, blant annet ved økt press fra USA og NATO om å beskytte norsk (og alliert) teknologi og skape større uavhengighet fra kinesiske leverandører i høyteknologiske forsyningskjeder. For å håndtere disse potensielt sikkerhetstruende implikasjonene, vurderer vi at det er behov for å styrke evnen til koordinering på tvers av domener nasjonalt og på tvers av likesinnede land. Det vil også være viktig å spre kunnskap til næringslivsaktører og forbrukere om hvilken rolle økonomisk aktivitet kan spille i å tilrettelegge for datainnsamling, etterretning, påvirkning, undergraving og sabotasje, slik at eventuelle forsøk på sikkerhetstruende virksomhet blir forebygget eller oppdaget. Rapporten identifiserer og anbefaler også videre forskning på en rekke områder som denne studien ikke har hatt mulighet til å gå i dybden på, men som vil bidra til å styrke kunnskapsgrunnlaget for politikkutforming og beslutningstaking.

Summary

Technological progress affects how states may use economic means to pursue strategic, foreign policy goals. Yet, this is an area mostly neglected in existing literature on economic statecraft. The purpose of this report is to strengthen the understanding of how technological developments can affect states' ability to use economic means, and to discuss implications for Norwegian security. The report focuses particularly on artificial intelligence and big data, 5G, cloud services and the Internet of Things. We have collected data from interviews and workshops with researchers at the Norwegian Defence Research establishment (FFI), as well as reviewing the literature.

We first identify several ways in which technological developments can change economic activity. This includes increased importance of data, more complex and skill-intensive products, services and value chains, increased market concentration and increased internationalization and/or automation. These insights enable us to discuss how states' abilities to perform economic statecraft may change due to technological progress. We distinguish between potential attempts at exercising power and accumulating power. The latter enables economic – or other types of – use of force in the future. Our analyses suggest that technological developments may strengthen individual states' opportunities to exercise power, particularly through exploiting dependencies on competence, resources, components, etc. to (covert) sabotage systems. Moreover, technological developments may enhance states' possibilities to accumulate power in several ways, including by utilizing economic activity to collect information and data for intelligence purposes and/or for trying to shape interests and perceptions in the recipient country. Certain states may also experience greater opportunities to establish themselves as key suppliers of important resources, products and expertise – dependencies that may be used strategically in the future to promote these states' interests globally. Technological developments also drive states, especially the U.S. and China, to implement domestic industrial policy for geopolitical purposes – in the literature called "the new economic statecraft".

What are the implications for Norwegian security? We argue that it is becoming increasingly important to manage data produced in the Norwegian society as a strategic resource. We also highlight that development and implementation of new technologies will likely contribute to making Norway more dependent on certain types of expertise, services, raw materials, components and products, and we recommend that studies are conducted to better gauge these dependencies. Furthermore, we believe that the rivalry between the U.S. and China will increasingly have implications for Norway, including increased pressure from the U.S. and NATO to protect Norwegian (and allied) technology and secure greater independence from Chinese suppliers in high-tech supply chains. In order to deal with these potentially security-threatening implications, we recommend strengthening the ability to coordinate across domains nationally and with like-minded countries. It will also be important to continue informing businesses and consumers about the role economic activity can play in facilitating data collection, intelligence, influence, subversion and sabotage, so that any attempts at security-threatening activities are prevented or discovered. The report also identifies and recommends further research in several areas which are beyond the scope of this study, but which will contribute to strengthening policy- and decision-making.

Innhold

Forord

Denne rapporten er skrevet som en del av et oppdrag finansiert av Justis- og beredskaps-departementet. Oppdraget søker å bidra til å sette norske myndigheter bedre i stand til å håndtere sikkerhetsutfordringer fra andre staters bruk av økonomiske virkemidler for å nå strategiske mål (økonomisk statshåndverk).

Vi ønsker spesielt å takke Brynjar Arnfinnsson, Ole Ingar Bentstuen, Bodil Farsund, Maria F. Fauske, Tormod K. Sivertsen og Ronny Windvik for verdifulle diskusjoner og innspill i arbeidet med denne studien. Uten muligheten til å bygge på ekspertkunnskapen og eksisterende forskning hos svært dyktige kollegaer ved FFI, hadde studien vært betydelig mer krevende å gjennomføre. Eventuelle feil og mangler i rapporten står for forfatternes regning.

Kjeller, 7. november 2022

Kristin Waage og Petter Y. Lindgren

1 Innledning

1.1 Bakgrunn

Økonomisk statshåndverk (*economic statecraft*) står høyt på agendaen i sikkerhetsmiljøer verden over. Globalisering av verdens økonomier, økt betydning av internasjonale finansmarkeder, digitalisering og fremvoksende økonomiers, herunder spesielt Kinas, økende sentralitet i verdensøkonomien, har transformert staters evne til å benytte økonomiske virkemidler for å fremme sine interesser i internasjonal politikk. Norge er en liten, åpen økonomi som er tjent med en liberal verdensorden med åpenhet overfor flyt av varer, tjenester, investeringer, finanskapital, kunnskap og teknologi. Tettere sammenveving av verdens land, økonomisk og finansielt, fysisk og digitalt, gjør at mulighetene for å utnytte den økonomiske interaksjonen strategisk vokser. At land utenfor USAs hierarki – både de atlantiske og asiatiske sikkerhetsfelleskapene – vokser frem økonomisk, betyr at Norge stilles overfor nye sikkerhetsutfordringer.

Samtidig står vi midt i den fjerde industrielle revolusjonen (4IR) med teknologisk fremgang innen blant annet kunstig intelligens, robotikk, tingenes internett, autonome kjøretøy, 3D-printing, kvantedatamaskiner og nanoteknologi. Til forskjell fra tidligere industrielle revolusjoner, er ikke 4IR bare karakterisert av ny teknologi, men spesielt av enorme nettverk av kommunikasjon og relasjoner mellom potensielt milliarder av mennesker og produkter (Schwab 2017). Den teknologiske utviklingen finner videre sted innen både maskinvare, programvare og informasjonstilgang. Det er i kombinasjonen av disse tre elementene vi finner mye ny teknologi. For eksempel trekker både kunstig intelligens, tingenes internett og skytjenester veksler på rask og eksponentiell utvikling av mulighetene i maskinvare, programvare og informasjonstilgang.

Den teknologiske utviklingen under 4IR vil endre hvordan stater utfører økonomiske statshåndverk. Mye av den eksisterende litteraturen innen økonomisk statshåndverk fokuserer på tradisjonelle sanksjoner som importrestriksjoner (se f.eks. Drezner 1998; Pape 1997; Peksen 2009; Early og Cilizoglu 2020). Det er også i økende grad fokus på hvordan positive virkemidler som investeringer og lån kan utnyttes av stater for å fremme deres interesser (se f.eks. Norris 2016, 2021; Pepermans 2018; Reilly 2013; Xiaotong og Keith 2017). Med enkelte unntak er det imidlertid ingen oppmerksomhet omkring hvilke implikasjoner ny teknologi og økt digital sammenkobling har for bruken av økonomiske virkemidler, til tross for at moderne økonomier og internasjonal økonomisk aktivitet blir stadig mer digitalisert og automatisert (se også Waage, Kvalvik og Lindgren 2021c).

For å være i stand til å forstå hvordan andre stater kan ta i bruk økonomisk statshåndverk på måter som potensielt er sikkerhetstruende, og iverksette tiltak for å redusere Norges sårbarhet, er det viktig å bygge et bedre kunnskapsgrunnlag om implikasjonene av den teknologiske utviklingen for økonomisk statshåndverk. Denne rapporten er en start på dette arbeidet.

1.2 Rapportens formål, begrepsbruk og problemstillinger

Rapporten er skrevet på oppdrag fra Justis- og beredskapsdepartementet (JD), og finansiert av JD og FFI-prosjektet «Totalforsvaret mot 2040». Oppdraget skal bidra til å sette norske myndigheter bedre i stand til å møte trusler fra andre staters bruk av økonomiske virkemidler. Målgruppen for rapporten er personer som arbeider med sikkerhetspolitiske problemstillinger i JD, andre departementer, forsvarssektoren, næringslivet og i bransjeorganisasjoner.

Formålet med denne rapporten er å styrke forståelsen av hvordan den teknologiske utviklingen kan påvirke staters evne til å ta i bruk økonomiske virkemidler og drøfte implikasjoner for norsk sikkerhet. Vi presiserer at dette er et komplekst og omfattende formål, som det vil kreve mer ressurser å oppnå fullstendig innsikt i enn omfanget av oppdraget som ligger til grunn for denne rapporten. Rapporten er derfor en forstudie, som danner et grunnlag som nye studier kan bygge videre på.

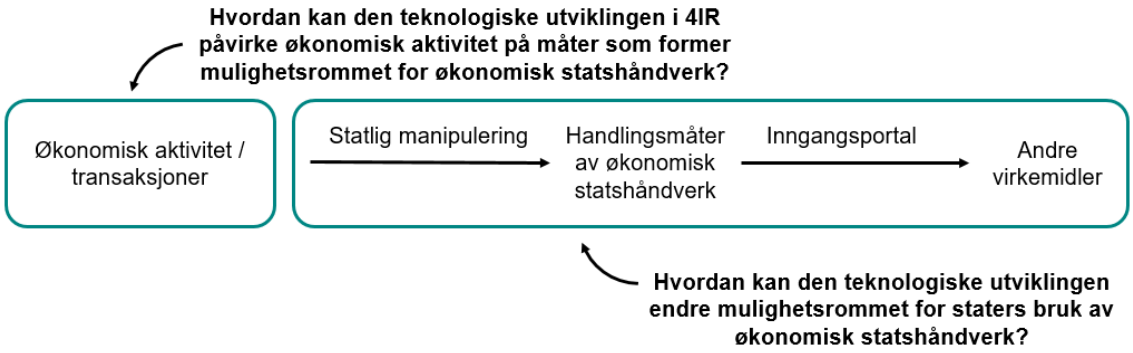
I denne rapporten forstår vi *økonomisk statshåndverk*[1] som en stats samlede bruk av økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål (Baldwin 1985).[2] Inspirert av Norris (2016), definerer vi *økonomiske virkemidler* som statens (intensjonelle) manipulering eller på andre måter utnyttelse av økonomiske transaksjoner. *Økonomiske transaksjoner* er overføringer av økonomiske verdier mellom økonomiske aktører.[3] Siden økonomiske transaksjoner utføres av økonomiske aktører i hovedsak med kommersielle formål, handler økonomisk statshåndverk om å skape insentiver for økonomiske aktører til å agere i tråd med statsledelsens politiske og strategiske formål (Norris 2016). Eksempler på økonomiske virkemidler er sanksjoner, investeringer, handel, lån, donasjon og valuta. Vi omtaler staten og landet som utfører økonomisk statshåndverk som *avsenderstat* og *-land* og *mottakerstat* og *-land* for enhetene som statshåndverket rettes mot. Vi presiserer at vi også har fokus på hvordan økonomiske virkemidler kan benyttes i kombinasjon med andre typer virkemidler, som cyber- og påvirkningsvirkemidler.

For å utarbeide problemstillinger som sikrer at vi oppnår formålet om en styrket forståelse av hvordan ny teknologi påvirker staters evner til å utføre økonomisk statshåndverk, utledet vi en oversikt over forholdet mellom økonomisk aktivitet, økonomiske virkemidler og andre virkemidler. I figur 1.1 vises en nedbryting av de analytiske bestanddelene i formålet vårt, i henhold til definisjonen av økonomisk statshåndverk. Fra figuren kan vi også utlede to håndterbare problemstillinger for denne rapporten:

1. Hvordan kan den teknologiske utviklingen i 4IR påvirke økonomisk aktivitet på måter som former mulighetsrommet for økonomisk statshåndverk?

[1] Vi har oversatt *economic statecraft* til økonomisk statshåndverk (og ikke statskunst som er mer vanlig) fordi håndverk gir lignende konnotasjoner som begrepet tilbyr på engelsk. Vi synes videre at det understreker at begrepet favner noe som minner mer om at politikere, byråkrater og diplomater (og andre myndighetspersoner) må mestre et praktisk fag mer enn å være et vidunder à la Michelangelo eller Beethoven.
[2] Vi henter inspirasjon fra begrepsdefinisjoner i Lindgren, Waage og Boye (2022).
[3] Økonomiske aktører inkluderer stater, statseide foretak, privateide bedrifter, banker og forbrukere.

2. Hvordan kan den teknologiske utviklingen endre mulighetsrommet for staters bruk av økonomisk statshåndverk?



Figur 1.1 Nedbrytning av økonomisk statshåndverk i sine «bestanddeler» med tilhørende problemstillinger.

Økonomisk aktivitet og økonomiske transaksjoner er grunnlaget for staters muligheter til å ta i bruk økonomiske virkemidler. Vi trenger først å forstå hvilke endringer ny teknologi medfører for økonomisk aktivitet (problemstilling 1) før vi kan analysere konsekvenser for mulighetene for å bedrive økonomisk statshåndverk (problemstilling 2). I problemstilling 1 setter vi derfor fokus på hvordan økonomisk aktivitet kan bli påvirket av den teknologiske utviklingen. Dette er et svært og komplekst spørsmål, så vi avgrenser oss til endringer som vi, på bakgrunn av datainnsamlingen (se delkapittel 1.4), vurderer er særlig relevante for å forstå mulighetsrommet for staters bruk av økonomisk statshåndverk i lys av den teknologiske utviklingen.

Med en styrket forståelse av hvordan økonomisk aktivitet endrer seg i takt med fremveksten av nye teknologier, kan vi evaluere hvordan handlingsmåter, eller strategier, av økonomisk statshåndverk blir påvirket. I problemstilling 2 benytter vi derfor svarene fra problemstilling 1 til å drøfte hvilke konsekvenser den endrede økonomiske aktiviteten har for staters muligheter til å benytte økonomisk statshåndverk, inkludert hvordan lovlig økonomisk aktivitet kan utnyttes som inngangsportal for å kunne ta i bruk andre typer virkemidler (f.eks. cybervirkemidler) i fremtiden.[4] Det betyr at vi ikke begynner med å analysere direkte hvordan ny teknologi påvirker hvilke økonomiske virkemidler som er tilgjengelig for stater, men benytter heller endringer i økonomisk aktivitet som utgangspunkt. Det er også relevant å forstå hvordan økonomiske virkemidler kan utnyttes for å posisjonere seg til å kunne utføre annen virkemiddelbruk i fremtiden – altså hvordan økonomiske virkemidler kan fungere som en «inngangsportal». Figur 1.1 viser hvordan dette steget følger etter at stater har benyttet økonomiske virkemidler (ved å manipulere økonomisk aktivitet). En ytterligere nedbryting er å skille på hvordan inngangsportaler kan skapes, styrkes eller svekkes, og på hvordan tilgjengeligheten av andre virkemidler (slik som cyberoperasjoner, (des)informasjon, propaganda, m.m.) kan endre seg som

[4] Merk at vi kan skille på hvordan ulike handlingsmåter av økonomisk statshåndverk (se delkapittel 1.3) kan styrkes eller svekkes, og på hvordan det potensielt kan oppstå nye måter å utføre selve manipuleringen av økonomisk transaksjoner som følge av ny teknologi. Oppdragets omfang har imidlertid ikke gjort det mulig å analysere sistnevnte (se delkapittel 1.5).

følge av den teknologiske utviklingen. Det sistnevnte temaet er imidlertid godt dekket av kollegaer ved FFI (se f.eks. Bentstuen mfl. 2018; Farsund mfl. 2022; Sellevåg mfl. 2020, 2021) og øvrige studier av andre virkemidler. Vi går derfor kun kort inn på temaet i denne rapporten.

Til slutt utleder vi en tredje problemstilling for å knytte problemstilling 1 og 2 til norske nasjonale sikkerhetsinteresser:

3. Hva kan implikasjonene være for norsk sikkerhet?

I den siste problemstillingen 3 drøfter vi implikasjoner for norsk sikkerhet av endringer i staters mulighetsrom for bruk av økonomisk statshåndverk som følge av den teknologiske utviklingen. Basert på dette gir vi også noen innledende anbefalinger til hvilke grep norske myndigheter kan ta for å redusere sårbarheter.

1.3 Typologi for økonomisk statshåndverk

Vi har tidligere utviklet en typologi for å analysere staters mulighetsrom for bruk av økonomiske virkemidler (Lindgren, Waage og Boye 2022; Udal mfl. 2022; Waage mfl. 2022). Typologien beskriver det utvalget av økonomisk statshåndverk som potensielt kan utgjøre en trussel[5] mot norske nasjonale sikkerhetsinteresser.[6] Vi presenterer rammeverket kort i dette delkapittelet, mens drøftingen i kapittel 4 utdyper om hver handlingsmåte samt hvordan den teknologiske utviklingen kan påvirke handlingsmåten.

Typologien består av to maktdimensjoner – maktatferd og maktkanal – med to utfall per dimensjon. For maktatferd skiller vi mellom *utøvelse* og *akkumulasjon* av makt. Makt kan utøves ved å ta i bruk økonomiske virkemidler for å oppnå politiske og strategiske mål, som i å straffe og belønne mottakerstaten eller begrense handlingsrommet til mottakerstaten. Men makt kan også akkumuleres ved å utnytte økonomiske transaksjoner på tvers av landegrenser for å legge til rette for økonomisk – eller annen – maktbruk i fremtiden. For maktkanal skiller vi mellom *bilateral kanal* og *nettverkskanal*. Økonomisk statshåndverk og maktbruk i internasjonal politikk har tradisjonelt blitt forstått i bilaterale relasjoner – mellom to parter. Men makt kan også akkumuleres eller utøves i nettverk. Globaliseringen har bidratt til utviklingen av store nettverk med en topografi av asymmetrisk karakter, der noen av nodene (*nodes*) er knutepunkt (*hub*) med forbindelser til hele eller store deler av nettverket. Slike nettverk tilbyr strukturell makt, hvor noen land – et knippe stormakter som USA og Kina – har evne til å utnytte deres uforholdsmessige gunstige posisjonering i regionale og globale nettverk for å oppnå strategiske mål (Farrell og Newman 2019). Eksempler på slike nettverk inkluderer globale finansnettverk (f.eks. SWIFT), internettplattformer, kommunikasjonsteknologi, nettverk for deling av sensitiv teknologi eller

[5] For litteratur om trusler mer generelt, se f.eks. Brummer (2020), Lindgren (2019), Lindgren og Yennie Lindgren (2019) og Oren og Brummer (2020b, 2020a).

[6] Typologien er tilpasset fra den universelle typologien over økonomisk statshåndverk som utvikles i (Lindgren og Waage 2022), og som inneholder flere handlingsmåter, der kalt strategier, enn typologien som presenteres her. I Lindgren, Waage og Boye (2022) har vi trukket ut de handlingsmåtene som potensielt kan utgjøre en trussel mot norske nasjonale sikkerhetsinteresser (se Sikkerhetsloven 2018: § 1-5). Typologien bygger videre på utfordringskategoriene utledet i Waage, Kvalvik og Lindgren (2021b; se også Waage, Kvalvik og Lindgren 2021a).

utvikling av militære våpensystemer, samt energi- og transportnettverk (Drezner, Farrell og Newman 2021).

Til sammen danner dimensjonene fire kategorier. I hver kategori har vi identifisert mulige handlingsmåter av økonomisk statshåndverk. Med handlingsmåter mener vi her de typene av handlinger stater kan utføre ved bruk av økonomiske virkemidler. Handlingsmåtene kan sees i tabell 1.1. Kategoriene er tildelt hver sin kvadrant i tabellen, som vi beskriver kort i det følgende.

- **Kvadranten for å akkumulere makt i bilaterale kanaler** beskriver handlingsmåter hvor avsenderstaten utnytter den bilaterale økonomiske interaksjonen mellom avsender- og mottakerlandet til å opparbeide seg økt makt. Det er fem handlingsmåter i denne kvadranten: forme (sær)interesser og oppfatninger i befolkningen, øke avhengigheten til ressurser eller innenlandsk marked, etterretningsvirksomhet, styrke militære kapabiliteter og tilrettelegge for (skjult) sabotasje. Merk at vi stiller krav til at handlingen utføres ved bruk av økonomiske virkemidler. Det betyr at etterretningsvirksomhet for eksempel i form av rekruttering av innsidere ikke er økonomisk statshåndverk, mens innhenting av informasjon gjennom utføring av økonomisk aktivitet er det.[7]

- **Kvadranten for å utøve makt i bilaterale kanaler** beskriver handlingsmåter hvor avsenderstaten utnytter den bilaterale økonomiske interaksjonen mellom avsender- og mottakerlandet til å utøve makt. Det er tre handlingsmåter i denne kvadranten: manipulere tilgang til salg til innenlandsk marked, manipulere tilførelsen av ressurser og sabotere infrastruktur (gjennom eierskapskontroll)[8].

- **Kvadranten for å akkumulere makt i nettverkskanaler** beskriver handlingsmåter hvor avsenderstaten utnytter sin gunstige posisjon i regionale eller globale økonomiske nettverk til å opparbeide seg makt. Det er to handlingsmåter i denne kvadranten: trekke ut informasjon eller data fra nettverksstrømmer (*panoptikon*) og øke andre lands avhengighet til eget knutepunkt (*lock-in*). Panoptikon innebærer at avsenderstatens sentrale plassering i et nettverk (for eksempel globale finansnettverk) åpner muligheter for å trekke ut informasjonsfordeler vis-à-vis en annen stat (Farrell og Newman 2019). Ved å øke andre lands avhengighet til eget knutepunkt, kan en avsenderstat legge til rette for bruken av panoptikon eller kvelning (se neste punkt) i fremtiden.

- **Kvadranten for å utøve makt i nettverkskanaler** beskriver handlingsmåter hvor avsenderstaten utnytter sin gunstige posisjon i regionale eller globale økonomiske nettverk til å utøve makt. Det er én handlingsmåte i denne kvadranten: manipulere tilgang til

[7] Et eksempel på sistnevnte er anklagene mot russiske sivile fartøy som i tillegg til å utføre kommersiell økonomisk aktivitet også mistenkes for systematisk å kartlegge norsk sokkel for å få tak i viktig informasjon om kritisk norsk infrastruktur på havbunnen (Kibar 2021).
[8] Dette kan, i teorien, for eksempel forekomme ved sabotasje av oppkjøpte selskaper, eller ved å true med å trekke ut investeringer (Drezner 2008).

nettverksstrømmer (*kvelning*). Kvelning går ut på at avsenderstaten kontrollerer knutepunkt i nettverket som gjør det mulig å styre andre lands tilgang til nettverksstrømmene (Farrell og Newman 2019).

Tabell 1.1 Typologi over handlingsmåter av økonomisk statshåndverk som potensielt kan utgjøre en trussel mot norsk sikkerhet. Kilde: Lindgren, Waage og Boye (2022).

	Akkumulere makt	**Utøve makt**
Bilateral kanal (markeder og leverandører)	**Forme (sær)interesser og oppfatninger i befolkningen** **Øke avhengigheten til ressurser eller innenlandsk marked** **Etterretningsaktivitet** • Overvåking fra geografisk lokasjon • Informasjonsinnhenting fra økonomisk virksomhet **Styrke militære kapabiliteter** • Teknologityveri • Omgå eksportkontroller • Sikre strategisk infrastruktur eller landområder **Tilrettelegge for (skjult) sabotasje**	**Manipulere tilgang til salg til innenlandsk marked** • Import • Muligheter for bedriftsetablering • Utgående turisme **Manipulere tilførselen av ressurser** • Leveranser og kapitalstrømmer • Arbeidstakere og kompetanse **Sabotere infrastruktur**
Nettverks-kanal (knutepunkt)	**Trekke ut informasjon/data fra nettverksstrømmer** (*panoptikon*) **Øke avhengigheten til knutepunkt** (*lock-in*) • Leveranseavhengighet • Promotere egen valuta	**Manipulere tilgang til nettverksstrømmer** *(kvelning)*

1.4 Metoder for datainnsamling

Vi har samlet inn informasjon/data ved å lese eksisterende litteratur og ved å gjennomføre intervjuer og en workshop med forskere ved FFI.

Vi har utført betydelige litteraturgjennomganger ved tidligere oppdrag og forskning om økonomisk statshåndverk i perioden 2020 til 2022 (Lindgren, Hemnes og Waage 2022; Lindgren, Waage og Boye 2022; Udal mfl. 2022; Waage mfl. 2022; Waage, Kvalvik og Lindgren 2021c). Det var allikevel behov for ytterligere søk etter litteratur i arbeidet med denne rapporten, fordi vi i liten grad hadde identifisert studier som koblet utviklingen av ny teknologi med fokus på økonomisk statshåndverk. Vi benyttet derfor samme litteraturidentifikasjonsmetode som ved tidligere arbeider: først søker vi i relevante akademiske søkemotorer med nøkkelord som «*technology*», «*economic statecraft*», «*artificial intelligence*», «5G», «*cloud computing*», «*internet of things*», «*geoeconomics*», «*investments*», «*international relations*», alene eller med to eller flere nøkkelord i kombinasjon. Vi utførte også søk med kombinasjoner av søkeordene sammen med ett eller flere av disse søkeordene: «*economics*», «*business*», «*finance*», «*enterprise*», «*digitalization*» og «*management*». Utover søk etter forskningsartikler i tidsskrifter og litteraturdatabaser, gjennomførte vi også søk på FFIs hjemmesider etter ugraderte FFI-rapporter som omhandler teknologisk utvikling og ulike teknologiområder.

For å samle inn informasjon om teknologier og implikasjoner utover den publiserte, ugraderte litteraturen, har vi også gjennomført intervjuer og en workshop med forskere ved FFI i perioden september 2021 til april 2022. Totalt deltok tolv respondenter på intervjuene og/eller workshopen. Respondentene er eksperter på ulike teknologier og tilhørende risikoer og sårbarheter, cyberdomenet, nasjonal sikkerhet, kompetansebehov som følge av den teknologiske utviklingen og implikasjoner for forsvarssektoren av det grønne skiftet og grønn teknologi.

Workshopen søkte spesielt å avdekke og styrke forståelsen av potensielle koblinger mellom cyberdomenet og økonomisk statshåndverk. I intervjuene har vi komplettert innsikten fra workshopen ved å drøfte nye, fremvoksende teknologier, også utover et spesielt fokus på cyberdomenet. Vi har spurt om hvordan ulike teknologier fungerer, utviklingstrekk, hvilke risikoer og sårbarheter som kan oppstå ved at teknologiene i økende grad blir tatt i bruk i næringslivet, samfunnet generelt og/eller forsvarssektoren, og eventuelle tiltak for å møte ulike utfordringer. Intervjuene har vært en idémyldringsprosess i ukjent farvann. Derfor har intervjuene foregått på et ustrukturert og utforskende format, siden det har vært vanskelig å vite i forkant hvilke temaer som er spesielt viktige for denne studien. Vi mener de ustrukturerte intervjuene har bidratt til å avdekke en større bredde av utfordringer og sårbarheter enn hva strukturerte intervjuer, med forhåndsdefinerte og -avgrensede spørsmål, ville ha lagt til rette for. Temaene som har blitt diskutert, har variert basert på den enkelte forskers spesialkompetanse, men flere av de mest sentrale utfordringene og sårbarhetene som løftes frem i denne rapporten har gått igjen på tvers av intervjuer. I etterkant av intervjuene har vi strukturert temaene som ble tatt opp etter de ulike «bestanddelene» som inngår i økonomisk statshåndverk (se figur 1.1) og, der det har vært relevant, ulike handlingsmåter (se tabell 1.1).

Selv om workshopen og de ustrukturerte intervjuene har bidratt til å skape innsikt og avdekket spesielt relevante temaer, er det likevel flere svakheter ved en slik utforskende fremgangsmåte som det er viktig å være klar over. For det første har diskusjonstemaene blitt avgrenset til de enkelte respondentenes kunnskap, som betyr at et annet utvalg av respondenter potensielt kunne ha belyst og vektlagt andre temaer. Siden vi også har komplettert med innsikt fra litteraturgjennomganger, har vi redusert sannsynligheten for at det finnes store blindsoner som vi ikke har fanget opp i arbeidet med denne studien. For det andre egner kvalitative metoder, som intervjuer, seg best til å tilegne seg dybdekunnskap om temaer, men slike metoder kan gjøre det mer krevende å verifisere og generalisere resultatene. I vårt tilfelle er det særlig en utfordring at temaene som har blitt drøftet på workshopen og intervjuene, er heftet med mye usikkerhet, slik at diskusjonene har handlet om hva som potensielt kan skje uten (mye) empiri som underbygger argumentene tilgjengelig per dags dato (for ytterligere detaljer, se delkapittel 1.5).

Samlet presiserer vi at fremgangsmåten valgt i denne rapporten er best egnet i en forstudie, og at videre arbeid er anbefalt for å studere funnene nærmere og trekke konklusjoner. Vi omtaler følgelig også funnene i kapittel 4 som hypoteser i stedet for konklusjoner.

1.5 Avgrensninger

Det er en utfordring at det eksisterer relativt få empiriske studier og faktiske eksempler av utfordringene og sårbarhetene som løftes frem i denne rapporten. For eksempel har FFI samlet inn informasjon om i underkant av 400 hendelser hvor Kina og Russland potensielt har benyttet økonomisk statshåndverk i perioden 2000–2021 (Udal mfl. 2022; Waage mfl. 2022), men få eller ingen av hendelsene er gode eksempler på utfordringer og sårbarheter som trekkes frem i denne rapporten. Det kan både komme av at utviklingstrekk fremdeles er relativt nye, at eventuelle handlinger hvor stater utnytter ny teknologi i sitt økonomiske statshåndverk kan foregå skjult slik at mottakerstaten ikke forstår at det skjer eller at mottakerstaten ikke er interessert i å dele slike erfaringer med offentligheten.[9] Det gjør at vi i denne studien avgrenser oss til hypoteser og vurderinger basert på hva som kan være teknologisk mulig, uten å vurdere sannsynlighet eller når og hvordan hendelser konkret kan finne sted.

Vi peker på flere hypoteser om mulige utviklingstrekk og konsekvenser i denne rapporten, men diskusjonen er ikke uttømmende. Det er nok flere temaer av relevans vi ikke har inkludert i denne rapporten. Vi avgrenser også rapporten til å handle om spesielt fire teknologier: kunstig intelligens, 5G, skytjenester og tingenes internett. Det er mange andre nye teknologier som kan endre fremmede staters økonomiske statshåndverk, slik som kvantedatamaskiner og blokkjedeteknologi (*blockchain*)[10]. Omfanget av oppdraget begrenset vårt teknologiske nedslagsfelt. Vår ambisjon med denne rapporten er å synliggjøre viktigheten av koblingen mellom økonomisk statshåndverk og teknologisk utvikling, begynne å utforske hypoteser rundt hvordan den teknologiske utviklingen kan påvirke bruken av økonomisk statshåndverk og inspirere videre forskning på temaet.

Definisjonen av økonomisk statshåndverk (se delkapittel 1.2) fremhever at statsledelsen må være i stand til å manipulere og kontrollere kommersielle aktører til å agere i tråd med statsledelsens ønsker. Som vi kort kommer inn på i delkapittel 3.5, kan den teknologiske utviklingen potensielt påvirke denne grunnleggende forutsetningen ved staters bruk av økonomiske virkemidler. Det finnes argumenter for at den teknologiske utviklingen vil bidra til økt grad av sentralisering i bedrifter, mens andre argumenterer for at vi kommer til å se økt grad av desentralisering. Slike organisasjonsendringer kan i neste omgang ha innvirkning på statsledelsens muligheter til å kontrollere de kommersielle aktørene. Oppdragets omfang har ikke gjort det mulig å analysere hvordan staters evne til å kontrollere kommersielle aktører potensielt påvirkes av teknologiutviklingen,[11] men vi fremhever at det er et relevant område for videre studier.

Vi har benyttet intervjuer med FFI-forskere og litteratursøk som metoder for å sammenstille et kunnskapsgrunnlag for å besvare problemstillingene i rapporten. Omfanget av rapporten har

[9] Udal mfl. (2022) og Waage mfl. (2022) tilbyr en mer omfattende diskusjon av skjevheter i hvilke hendelser som kan observeres.
[10] Vi adresserer imidlertid potensielle implikasjoner av fremveksten av digitale valutaer, hvor kryptovalutaer slik som Bitcoin bygger på blokkjedeteknologi (Aggarwal og Marple 2020).
[11] Det er generelt et behov for mer forskning på staters evne til å manipulere kommersielle interesser. Se f.eks. Norris (2021) for relevante forskningsspørsmål om den kinesiske statsledelsens evne til å kontrollere kinesiske kommersielle aktører.

begrenset antallet forskere vi har intervjuet og antallet timer vi har benyttet til å lete frem relevant akademisk litteratur. Det er rom for økt kunnskap ved å utvide listen med respondenter og utføre mer omfattende søk etter ytterligere litteratur.

1.6 Tilgrensende forskning og publikasjoner

FFI har allerede gjennomført studier innen mange temaer som grenser til denne rapportens problemstillinger, og det finnes pågående FFI-prosjekter som forsker på alle teknologiene som er i fokus i denne rapporten.

For eksempel har FFI utgitt en rekke ugraderte publikasjoner om fremvoksende teknologier[12] med fokus på trender, muligheter og/eller utfordringer (Andås 2020; Bentstuen 2022; Farsund mfl. 2022; Farsund, Hegland, og Lillevold 2016; Fauske 2020; Hansen, Halvorsen, og Opland 2022; Klepper mfl. 2021; Kveberg og Johnsen 2014; Lund, Johnsen, og Bergh 2021; Rjaanes mfl. 2020; Stolpe, Hansen, og Halvorsen 2019; Voldhaug mfl. 2021; Waage 2022). Rapportene går i dybden på blant annet 5G og andre mobilteknologier, skytjenester, tingenes internett, stordata, kunstig intelligens og cyberdomenet generelt. FFI har også studert implikasjoner for Forsvaret og/eller samfunnssikkerheten av teknologiutvikling på et overordnet nivå, som én av flere globale utviklingstrekk (Beadle mfl. 2019; Beadle og Diesen 2015; Diesen 2018; Sellevåg mfl. 2020, 2021; Skjelland mfl. 2019, 2022).

Videre har FFI beskrevet viktige trender innen digitale verdikjeder og sikkerhetsmessige konsekvenser for virksomheter og samfunnet (Bentstuen mfl. 2018), utarbeidet metoder for risiko- og sårbarhetsvurderinger av kritiske samfunnsfunksjoner og infrastruktur (Bruvoll, Endregard og Busmundrud 2020; Mancini, Farsund og Lillevold 2017; Maal, Isaachsen og Torget 2017) og evaluert IKT-sikkerhetshendelser i Norge (Bruvoll, Thuv og Enemo 2020). FFI har i tillegg studert påvirkningsoperasjoner som utnytter ny teknologi og digitale plattformer (Bergh 2019, 2020; Sivertsen mfl. 2021, 2022; Strand og Hagen 2015).

Til sammen danner dette kunnskapsgrunnlaget et svært godt utgangspunkt for å studere koblingen mellom fremvoksende teknologier og økonomisk statshåndverk, drøfte implikasjoner for norske myndigheter og identifisere sentrale kunnskapshull. I denne rapporten bringer vi altså ikke til bords ny teknologisk innsikt, men vi søker å koble sammen FFIs eksisterende innsikt om trusler og sårbarheter med staters muligheter for å utnytte økonomisk aktivitet til å oppnå ulike strategiske mål.

Denne rapporten kan leses som et selvstendig arbeid om økonomisk statshåndverk. For interesserte lesere kan vi anbefale andre relevante publikasjoner innen temaet:

[12] I denne rapporten bruker vi begrepene nye teknologier og fremvoksende teknologier synonymt. Vi gjør oppmerksom på at det kan stilles krav, for eksempel basert på teknologiske modenhetsnivå (*technological readiness level* – TRL), for hva som kvalifiserer som en fremvoksende teknologi (se f.eks. Andås 2020: 9), men vi vurderer at slike nyanser ikke er nødvendige for å besvare denne rapportens formål og problemstillinger.

- Waage, Kvalvik og Lindgren (2021c) er en forstudie av hvordan økonomiske virkemidler kan true norsk sikkerhet (se også Waage, Kvalvik, og Lindgren 2021a, 2021b)

- Waage mfl. (2021) gir en omfattende oversikt over ulike økonomiske virkemidler.

- Lindgren og Waage (2021) diskuterer fire nyere bidrag i forståelsen av kinesisk statshåndverk, mens Waage og Lindgren (2021) diskuterer ett av disse mer inngående.

- Lindgren, Hemnes og Waage (2022) analyserer Kinas økonomi og den økonomiske interaksjonen med omverden og Norge mer inngående.

- Lindgren, Waage og Boye (2022) undersøker hvordan kinesisk økonomisk statshåndverk kan true norsk sikkerhet ved å utlede en typologi over potensielt sikkerhetstruende økonomisk statshåndverk og setter typologien opp mot mulige hendelser av kinesisk bruk av økonomiske virkemidler.

- Lindgren og Waage (2022) tilbyr en omfattende konseptuell analyse av økonomisk statshåndverk, utdyper om en universell typologi over økonomisk statshåndverk og drøfter typologiens relevans for beslutningstakere.

- Waage mfl. (2022) analyserer hendelser av potensiell kinesisk bruk av økonomisk statshåndverk i perioden 2000–2021 og implikasjoner for norsk sikkerhet.

- Udal mfl. (2022) analyserer hendelser av potensiell russisk bruk av økonomisk statshåndverk i perioden 2000–2021 og implikasjoner for norsk sikkerhet.

1.7 Rapportens struktur

Først presenterer vi en oppsummering av utvalgte teknologiområder og eksisterende litteratur om sammenhengen mellom økonomisk statshåndverk og teknologisk utvikling i kapittel 2. I kapittel 3 studerer vi problemstilling 1, før vi tar for oss problemstilling 2 i kapittel 4. Kapittel 5 drøfter potensielle implikasjoner for norsk sikkerhet (problemstilling 3). Til slutt oppsummerer vi studiens viktigste funn i kapittel 6 og identifiserer områder for videre studier.

2 Bakgrunn

I delkapittel 2.1 redegjør vi for noen sentrale fremvoksende teknologier som kan føre til endringer i hvordan stater kan utnytte økonomisk aktivitet til å oppnå ulike strategiske mål. I delkapittel 2.2 undersøker vi hva eksisterende litteratur om økonomisk statshåndverk allerede kan bidra med av innsikt om endringer som følger av fremveksten av ny teknologi. I delkapittel 2.3 fremhever vi sentrale gap og utfordringer i denne litteraturen, som motiverer analysene og drøftingen i resten av rapporten.

2.1 Om utvalgte teknologiområder

I denne gjennomgangen inkluderer vi teknologiområder basert på to kriterier. For det første velger vi teknologier som løftes frem som særdeles viktige innen den teknologiske utviklingen (se f.eks. Klepper mfl. 2021; Sellevåg mfl. 2020; Voldhaug mfl. 2021). For det andre har vi valgt teknologier som vi vurderer vil kunne ha størst implikasjoner for staters evne til å bruke økonomiske virkemidler for å forsøke å oppnå utenrikspolitiske, strategiske mål.

Teknologiområdene vi tar for oss i dette delkapittelet, er: kunstig intelligens og stordata (seksjon 2.1.1), femte generasjons mobilnett (5G) (seksjon 2.1.2), skytjenester (seksjon 2.1.3) og tingenes internett (seksjon 2.1.4).[13]

2.1.1 Kunstig intelligens og stordata

Kunstig intelligens (KI) handler om å få maskiner til å utvise det som vanligvis blir ansett som intelligent oppførsel.[14] Kunstig intelligente systemer består av data, programvare og maskinvare, som muliggjør at de kan utføre handlinger, fysisk eller digitalt, i den hensikt å oppnå et gitt mål, og handlingene som blir utført, kjennetegnes av at de normalt krever menneskelig intelligens (Department of Defense 2018; High-Level Expert Group on Artificial Intelligence 2019). Kunstig intelligens brukes blant annet til informasjonshåndtering og -analyse for å øke evnen til datadrevet innsikt og beslutningstaking, automatisere organisasjoners interne prosesser og forbedre ulike produkter og tjenester.

De fleste praktiske anvendelsene av kunstig intelligens i dag baserer seg på maskinlæring (ML).[15] Maskinlæring er et felt under kunstig intelligens hvor systemer blir trent heller enn eksplisitt programmert. Særlig dyp læring er en retning innen maskinlæring som har fått mye oppmerksomhet de siste årene på grunn av dyp lærings store fremskritt og potensial for å prosessere bilde, språk og video samt håndtere ikke-lineære, komplekse problemer.

[13] Vi har utelatt teknologier som kvantedatamaskiner, nanoteknologi, autonome kjøretøy og ulike typer bioteknologier, som genredigering, se f.eks. Schwab (2017).
[14] Selv om det er krevende å definere intelligens, fremhever mange at intelligent oppførsel hos maskiner som regel inkluderer én eller flere av egenskapene sansing, læring, forståelse, resonnering, planlegging og handling (se f.eks. Andås 2020 eller Waage 2022).
[15] Mange bruker av den grunn begrepene kunstig intelligens og maskinlæring om hverandre.

Det er som regel en fordel å trene algoritmene i (maskinlæringsbaserte) KI-systemer på store og gode datasett. Det kommer av at systemene ofte trenger mye data for å «lære seg» å identifisere underliggende mønstre i dataene, som setter systemene i stand til å ta avgjørelser eller utføre prediksjoner (Farsund mfl. 2022). Derfor blir begrepet *stordata* ofte trukket frem i sammenheng med kunstig intelligens. Stordata er data som kjennetegnes av tre V-er (Voldhaug mfl. 2021: 11; se også Stolpe, Hansen og Halvorsen 2019: 8–9): data av forskjelligartet natur (*Variety*), som kommer i store mengder (*Volume*) og/eller har hyppig oppdateringsfrekvens (*Velocity*). Dette gjør at stordata er krevende å håndtere, bearbeide og analysere med tradisjonelle metoder, og at det er nødvendig å anvende KI-teknikker til dette i stedet for tradisjonelle metoder (Voldhaug mfl. 2021). Teknologiske fremskritt innen prosesseringskraft og evnen til å håndtere og anvende stordata har derfor bidratt til at KI-teknikker, særlig dyp læring, har gjort store gjennombrudd det siste tiåret.

ML-algoritmer, særlig innen dyp læring, blir ofte omtalt som en «sort boks» (*black box*), hvor det er krevende å etterprøve resultater. Det kommer av at selv om prosessene er gjennomsiktige og konseptuelt enkle, gjør dimensjonaliteten[16] (*dimensionality*) i dataene det vanskelig å ha full oversikt over oppførselen til systemene. Når flere KI-baserte systemer interagerer med hverandre, hvor resultater fra ett system behandles som inndata i et annet system, kan denne utfordringen forsterkes ytterligere.

For flere detaljer om kunstig intelligens og stordata, se for eksempel Andås (2020), Stolpe, Hansen og Halvorsen (2019) eller Waage (2022).

2.1.2 Femte generasjons mobilnett (5G)

Det hevdes at femte generasjons mobilnett (5G) vil «revolusjonere hverdagen og sentrale funksjoner i samfunnet» og skyte «rakettfart i den teknologiske utviklingen» (Telia 2022b, 2022a). Utviklingen av tidligere generasjons mobilnett (3G og 4G), har handlet om å gi brukerne høyere båndbredde og øke hastigheten i dataoverføring. 5G er derimot helt ny teknologi som skal klare å håndtere mye større datamengder enn tidligere generasjoners mobilnett (Telia 2022a) – og slik understøtte det «hypertilkoblede «smarte» samfunnet og nye industrielle behov» (Sellevåg mfl. 2020: 32).[17]

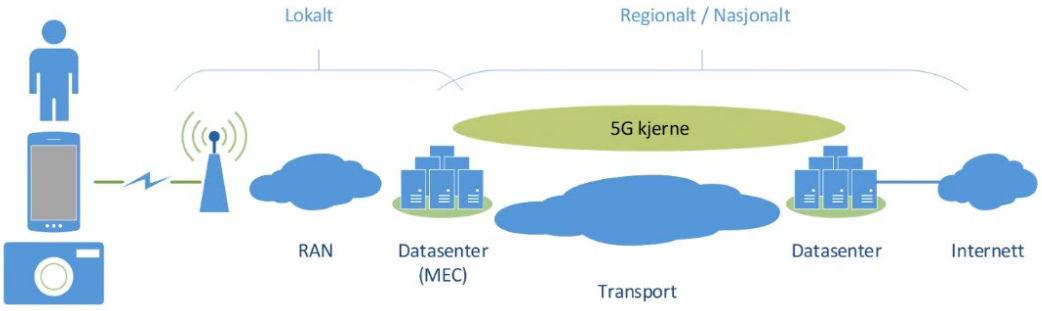
Det er ikke én enkeltstående teknologi som utgjør 5G, men heller en samling av teknologier. Til sammen muliggjør disse teknologiene «datakommunikasjon tilpasset bruk i ulike situasjoner med svært ulike krav til overføringshastighet, pålitelighet og lav forsinkelse for mobile brukere» (Voldhaug mfl. 2021: 16). Et viktig element ved 5G er dessuten at mobilnettet skal kunne håndtere svært mange tilkoblede enheter, selv på mindre geografiske områder, som følge av forventninger om at «alt» i fremtiden vil være tilkoblet internett (Voldhaug mfl. 2021: 16). I de kommersielle

[16] Med dimensjonalitet menes antall attributter, eller egenskaper, som et datasett har. Dersom antallet egenskaper overstiger antallet observasjoner i datasettet, er datasettet høydimensjonalt.

[17] Det innebærer at 5G vil være svært viktig for utviklingen av tingenes internett, hvor et stort antall sensorer kobles sammen. Tingenes internett eksisterer allerede i dag, men med 5G vil bruken av slike teknologier øke kraftig. Se seksjon 2.1.4 for mer om tingenes internett.

mobilnettene er 5G allerede i ferd med å bli implementert, og i årene som kommer vil 5G tas i bruk innen langt flere bruksområder og i langt større skala.

Figur 2.1 illustrerer «komponentene» som inngår i 5G-infrastruktur. Som figuren viser består infrastrukturen av aksenett (basestasjoner) og det såkalte «kjernenettet» som er spredt utover ett eller flere sentrale og lokale datasentre.[18] I kjernenettet finnes funksjoner for å holde styr på abonnementer og fordele datastrømmer til riktig mottaker (Voldhaug mfl. 2021). Mellom bruker-utstyret og basestasjonene er det trådløs forbindelse som bruker ny radioteknologi (Voldhaug mfl. 2021). Deretter er det i hovedsak fiberforbindelser, som kobler sammen basestasjonene med kjernenettet og resten av verden.



Figur 2.1 Oversikt over «komponentene» som inngår i 5G-nettverk. Figuren er hentet fra Bentstuen (2020).

Som Bentstuen mfl. (2018: 15) forklarer, fører 5G-nettverkene med seg en «kompleksitet og skala som gjør det nær umulig å bruke manuelle prosesser i drift og vedlikehold». På grunn av denne kompleksiteten, er det behov for avansert nettverksstyring som utnytter kunstig intelligens til å drifte og vedlikeholde både datasystemene i datasentrene og datanettverkene i og mellom data-sentrene. For militær virksomhet vil automatiserte algoritmer imidlertid medføre potensielle utfordringer for sikkerhetsgodkjenning av systemer, som følge av at det ikke er mulig for systemeier å ha full oversikt over oppførselen til systemene (Bentstuen mfl. 2018). For sivile virksomheter vil det bli vanskeligere å gjennomføre gode risikoanalyser, inkludert analyse av verdikjeder i slike komplekse systemer.

For flere detaljer om 5G, se for eksempel Bentstuen mfl. (2018) eller Voldhaug mfl. (2021).

2.1.3 Skytjenester

Skytjenester (*cloud computing*) bidrar i økende grad til å transformere og digitalisere virksom-heter på tvers av sektorer (Akter mfl. 2020). Skytjenester kan forstås som ulike datatjenester – fra datalagring og -prosessering til ulike former for programvare – som personer og virksomheter kan få tilgang til ved hjelp av internett og eksterne datasentre (Farsund mfl. 2022). Som Farsund mfl. (2022: 15) forklarer, er altså en «sky» egentlig «et stort og sammenkoblet nettverk av kraftfulle servere, plassert i ulike datasentre». Virksomheter kan eie og drifte sine egne datasentre, men den

[18] Sammenliknet med 4G vil enkelte komponenter i 5G-kjernen være spredt ut over flere datasentre.

vanligste løsningen ved bruk av skytjenester er at en ekstern part leverer disse tjenestene (Voldhaug mfl. 2021).

Som for 5G, er det ikke én bestemt teknologi som ligger til grunn for skytjenester, men heller en samling av teknologier som muliggjør skytjenester (Voldhaug mfl. 2021). Videre kjennetegnes skytjenester av flere egenskaper (Lund, Johnsen og Bergh 2021). For det første benyttes tjenestene via nettverkstilgang fremfor at maskinvaren er lokalisert der brukerne er. For det andre setter kunden selv opp og administrerer tilgang til tjenestene de ønsker å bruke. For det tredje samles ressursene (prosessering, lagring, nettverk, m.m.) i ett «punkt». For det fjerde kan man kjøpe tilgang til ressurser basert på behov (fleksible endringer i ressurstilgjengelighet). Og for det femte måles kundens forbruk av ulike ressurser kontinuerlig.

Disse egenskapene ved skytjenester gjør det mulig for kunden å bruke tjenester som beregningskraft, lagringsplass og databaser fortløpende etter behov, i stedet for å gjøre dyre investeringer i infrastrukturen lokalt. Det gir følgelig fordeler i form av dynamisk skalering etter endrede behov hos kunden, uten at kunden trenger å betale for mer enn de bruker (Farsund mfl. 2022).[19] I tillegg gir skytjenester fordeler i form av mobilitet, som følge av at kunden alltid kan få tilgang til skytjenestene så lenge de har internettforbindelse (Farsund mfl. 2022). Kundene slipper også mye av oppgavene knyttet til drift, vedlikehold og oppdatering av systemene siden dette utføres av tjenesteleverandøren (Farsund mfl. 2022). Videre vil økt bruk av virtuelle arbeidsflater redusere mulige angrepsflater og minimal datalagring på lokale datamaskiner vil redusere sårbarheten for datalekkasje (Bentstuen mfl. 2018). De store leverandørene av skytjenester[20] bruker dessuten store ressurser på å sørge for god sikkerhet rundt tjenestene de leverer (Voldhaug mfl. 2021). Samlet har bruken av skytjenester derfor potensial til å øke datasikkerheten hos mange virksomheter, særlig små og mellomstore bedrifter som har mindre ressurser til å ivareta datasikkerhet lokalt. Virksomheter blir imidlertid avhengig av sentrale tjenester hos leverandøren de benytter (Bentstuen mfl. 2018).

For flere detaljer om skytjenester, se for eksempel Lund, Johnsen og Bergh (2021).

2.1.4 Tingenes internett

Tingenes internett (*Internet of Things* – IoT) refererer til fysiske enheter som er koblet til internett (Farsund mfl. 2022). Disse fysiske enhetene, eller «tingene», kan være «alt fra industrielle

[19] Det finnes forskjellige tjenestemodeller for skytjenester (Farsund mfl. 2022), avhengig av om tjenesten tilbyr programvare med underliggende infrastruktur (*Software as a Service* – SaaS), en plattform for å utvikle, teste, levere og vedlikeholde programvareapplikasjoner uten den underliggende infrastrukturen (*Platform as a Service* – PaaS), eller kun IT-infrastruktur som servere, virtuelle maskiner, lagringsmuligheter, nettverk og operativsystem (*Infrastructure as a Service* – IaaS). Man kan også skille mellom forskjellige leveransemodeller som skytjenesteleverandøren kan benytte (Farsund mfl. 2022: 16): i en allmenn sky (*public* cloud) er tjenestene tilgjengelige for alle, i en privat sky (*private cloud*) er tjenestene kun tilgjengelige for en gitt kunde(gruppe), og i en hybrid sky (*hybrid cloud*) kombineres modellene ovenfor for eksempel ved å primært bruke en privat sky, men i perioder med spesielt stor arbeidsmengde også tar i bruk en offentlig sky.

[20] Noen av de største aktørene i verden innen skytjenester i dag, er Amazon Web Services, Microsoft Azure og Google Cloud (Farsund mfl. 2022).

roboter, private og offentlige overvåkningskameraer og biler til barneleker og lyspærer» (Farsund mfl. 2022: 7).

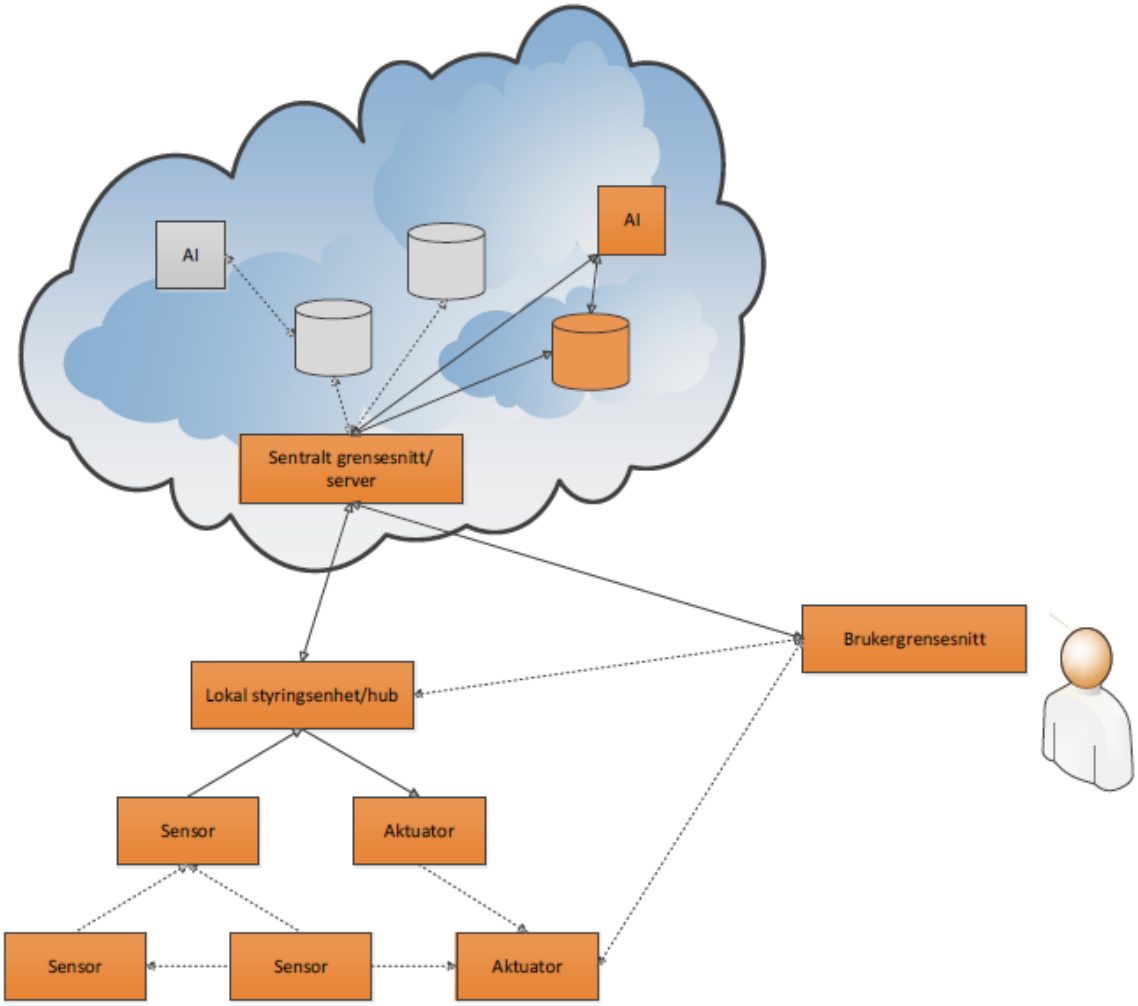
Som Farsund mfl. (2022: 7) beskriver, vil IoT «i økende grad bli brukt til å underholde oss, gjøre hverdagen vår enklere (smarthjem), byer mer ressurseffektive (smartbyer), industribedrifter mer kostnadseffektive (Industri 4.0), og til å gi oss bedre offentlige tjenester som for eksempel helsetjenester (e-helse)». Jo mer IoT-systemer tas i bruk i næringslivet og samfunnet generelt, desto mer vil imidlertid ulike IoT-systemer, og infrastrukturene de danner, også bli sammenkoblet. Det er derfor rimelig å forvente at avhengigheten mellom ulike IoT-systemer – og tilhørende infrastrukturer – øker i årene som kommer.

Det er som regel flere ulike teknologier som inngår i et IoT-system, inkludert trådløs kommunikasjon (5G), skytjenester, kunstig intelligens og stordata (Farsund mfl. 2022). IoT-systemene er derfor ofte komplekse. Videre vil fremskritt innen utviklingen av tilhørende teknologier bidra til å akselerere IoT. For eksempel er det forventet at utvikling og utbygging av 5G-nettverk vil øke bruken av IoT i samfunnet kraftig i årene fremover (Farsund mfl. 2022).

Figur 2.2 er hentet fra Farsund mfl. (2022: 10) og gir en oversikt over komponentene som kan inngå i et IoT-system. Som figuren viser, inkluderer ofte et IoT-system *sensorer* (som temperaturmålere, avstandsmålere eller kameraer), som samler inn informasjon om omgivelsene, og *aktuatorer*[21] (som brytere, døråpnere eller varsellys), som kan utføre handlinger fysisk eller digitalt. Logikken knyttet til sensoren(e) og/eller aktuatoren(e) befinner seg i en *lokal styringsenhet/hub*, som kan være innebygget i sensoren. Det er imidlertid en trend hvor funksjonalitet flyttes fra en lokal styringsenhet til et *sentralt grensesnitt/server* i skyen. Det sentrale grensesnittet styrer kommunikasjonen mellom bruker(e), sensor(er) og/eller aktuator(er) og tilhørende *skytjenester*, som ofte er hvor data samles og lagres og hvor kontrollen til systemet ligger. I tillegg består et IoT-system av et *brukergrensesnitt* som legger til rette for at brukeren kan samhandle med systemet – for eksempel gjennom en app på en mobiltelefon – for å se sensorinformasjon eller og/eller gi kommandoer til aktuatoren(e). Brukergrensesnittet kan kommunisere med den lokale styringsenheten, men det er en trend i retning av økt integrasjon mot sentralt grensesnitt i skyen. *Kommunikasjonsteknologi* understøtter kommunikasjon mellom de ulike komponentene i et IoT-system.

For flere detaljer om tingenes internett, se for eksempel Farsund mfl. (2022).

[21] En aktuator kan defineres som «en teknisk innretning som ved hjelp av styresignaler utfører en mekanisk bevegelse» (Rosvold 2016).



Figur 2.2 Oversikt over IoT-system. Hentet fra Farsund mfl. (2022: 10).

2.2 Tradisjonell og ny litteratur om økonomisk statshåndverk

Det finnes en betydelig litteratur om økonomisk statshåndverk (*economic statecraft*) i studiet av internasjonal politikk. Litteraturen har i stor grad konsentrert seg om (negative) sanksjoner, på tross av at klassikeren i feltet – Baldwin (1985) – forsøkte å spenne opp et bredt lerret av tilgjengelige virkemidler i staters økonomiske statshåndverk. Vi presenterer kort Baldwin og andre diskusjoner om sanksjoner i seksjon 2.2.1. I seksjon 2.2.2 presenterer vi deretter innsikt fra et nytt perspektiv på økonomisk statshåndverk, som anerkjenner at skillet mellom næringspolitikk og økonomisk statshåndverk utfordres av særlig stormaktenes teknologirivalisering.

2.2.1 Økonomisk statshåndverk

Baldwin (1985) er klassikeren innenfor studiet av økonomisk statshåndverk. Her defineres økonomisk statshåndverk som en stats samlede bruk av økonomiske virkemidler for å oppnå utenrikspolitiske mål. Baldwin viser hvordan økonomisk statshåndverk utgjøres av en stor gruppe økonomiske virkemidler som embargo, boikott, dumping, frysing av eiendeler, eksportkontroll, bistand og investeringsgarantier. For Baldwin inneholder økonomisk statshåndverk både positive og negative sanksjoner[22] (se også Baldwin 1971). Han plasserer økonomisk statshåndverk som en del av staters samlede statshåndverk, som utenom økonomiske instrumenter også inkluderer militære, diplomatiske og propagandavirkemidler. Stater velger blant disse typene virkemidler for å håndtere politiske og strategiske utfordringer og muligheter i internasjonal politikk.

På tross av Baldwins forslag om en bred tilnærming til økonomisk statshåndverk, er mye av litteraturen fokusert på sanksjoner. I kjølvannet av Kinas fremvekst som økonomisk og militær stormakt, har det imidlertid blitt større fokus på et rikere sett med økonomiske virkemidler. Studier av kinesiske investeringer, handel, fremstøt for å styrke egen valuta og etableringer av nye internasjonale økonomiske institusjoner har vokst frem som en sentral del av litteraturen om økonomisk statshåndverk (Clarke, Sussex og Bisley 2020; Cohen 2019; Norris 2016b; Roberts, Armijo og Katada 2017; se også Lindgren og Waage 2021; Waage og Lindgren 2021).[23] Det har også provosert frem bidrag om hvordan USA og Vesten skal reagere på utfordringen fra Kinas økonomiske statshåndverk (Blackwill og Harris 2016).

Flere studier fremhever hvordan en stats muligheter til å benytte økonomisk statshåndverk påvirkes av dens evne til å utøve kontroll over kommersielle aktører. Et spesielt relevant bidrag innen denne retningen, er Norris (2016). Han fremhever at økonomiske transaksjoner på tvers av landegrenser i all hovedsak utføres av kommersielt orienterte virksomheter, og at økonomisk statshåndverk derfor i stor grad avhenger av statsledelsens evne til å kontrollere atferden til aktører som helst vil tjene penger i stedet for å adlyde statsledelsen. Også ny teknologi utvikles og tas i bruk i hovedsak blant kommersielle aktører som har som mål å oppnå mest mulig profitt. Båndene til myndighetene hos avsenderstaten kan være tette eller staten kan ha armlengdes avstand til de kommersielle aktørene, men det vil allikevel være slik at økonomiske aktører kan ha insentiver til å agere i uoverensstemmelse med statsledelsen. For flere detaljer om modellen til Norris (2016) henviser vi til Lindgren og Waage (2021a) samt Waage, Kvalvik og Lindgren (2021c).

Til slutt i denne seksjonen vil vi nevne et par bidrag som understøtter hvordan vi forholder oss til økonomisk statshåndverk ved FFI. Foruten Baldwins (1985) brede tilnærming til økonomisk statshåndverk, er vi inspirert av to nye bidrag om hvordan en kan studere maktpolitikk i internasjonal politikk. Goddard og Nexon (2016) argumenterer for et forskningsprogram som setter maktpolitikk i fokus, som kombinerer innsikter fra flere paradigmer innen studiet av internasjonal politikk og som studerer hvordan aktører – stater eller andre aktører – benytter forskjellige

[22] Baldwin (1985) bruker begrepet «sanksjoner» i en bred tolkning, hvor begrepet har samme betydning som begreper slik som «virkemidler», «instrumenter», «teknikker», m.m. – ikke i en smal forstand hvor begrepet primært betyr formelle/juridiske sanksjoner.
[23] Vi henviser til Waage mfl. (2022) for en litteraturgjennomgang av kinesisk økonomisk statshåndverk.

ressurser og typer av makt for å oppnå innflytelse. Inspirert av arbeidene til Charles Tilly og spesielt konseptet om «omstridt politikk» (*contentious politics*)[24], foreslår de å fokusere på «*real-politikk* som politikken til kollektiv mobilisering i konteksten av kampen for innflytelse mellom politiske fellesskap forstått bredt» (Goddard og Nexon 2016: 5). Sett i dette lyset handler økonomisk statshåndverk om staters mobilisering av økonomiske ressurser for å skaffe innflytelse, omforme økonomiske ressurser til andre typer ressurser (informasjon, militærteknologi, osv.) eller forsvare seg mot fremmede staters maktbruk med økonomiske virkemidler. Bidraget deres rammer derfor inn vårt fokus på økonomisk statshåndverk i en større helhet der stater mobiliserer ulike typer virkemidler for å øke innflytelsen og autonomien i internasjonal politikk.

I et annet bidrag argumenterer Goddard, MacDonald og Nexon (2019) for at statshåndverk, som en underkategori av maktpolitikk, gir en fin innfallsvinkel til å forstå internasjonal politikk. Stater har egentlig et nært uendelig sett med virkemidler til disposisjon i verktøykassen, men igjen, inspirert av repertoarbegrepet til McAdam, Tarrow og Tilly (2001; se også Tarrow 1998), argumenterer de for at verktøykassen til stater i et gitt tidsrom er begrenset av hva som er kjent, hva de allerede benytter seg av og hva som er akseptabelt. Stater vil ha ulike repertoarer å spille på, ikke bare på grunn av ulike kapabiliteter, men også av hva som er meningsfulle og sosialt aksepterte strategier og bruk innad i og mellom statene. Tenkningen omkring nye, fremvoksende teknologier er fruktbar i relasjon til disse bidragene: ikke bare vil ny teknologi kunne transformere maktpolitikk og statshåndverk, men hva stater tar i bruk i sitt repertoar av virkemidler vil påvirke den teknologiske utviklingen. Perspektivet løser altså opp en forutsetning om teknologisk determinisme – at en ny teknologi vil bli tatt i bruk på en bestemt måte – og plasserer den teknologiske utviklingen i en politisk, sosial og kulturell kontekst. Dette perspektivet er nyttig å ta med seg i studiet av økonomisk statshåndverk generelt og i en analyse av forholdet mellom nye teknologier og økonomiske virkemidler spesielt. Spesielt relevant blir perspektivet når stater tar i bruk økonomiske virkemidler for å styrke teknologisk utvikling og innovasjon i næringer og bedrifter i egen økonomi, for å styrke evnen til geopolitisk konkurranse og rivalisering. Vi ser på slik bruk av økonomisk statshåndverk i neste seksjon.

2.2.2 Skillet mellom næringspolitikk og økonomisk statshåndverk utviskes

I den tradisjonelle litteraturen om økonomisk statshåndverk i internasjonal politikk, er det kun fokus på hvordan stater bruker økonomiske virkemidler for å oppnå utenrikspolitiske, strategiske mål – à la Baldwin (1985). Her faller altså all politikk og handlingsmåter som har fokus på å styrke økonomiens stilling og konkurransekraft utenfor. Slik politikk og handlingsmåter kan selvsagt også bli omtalt som statshåndverk, men i studiet av internasjonal politikk avgrenses som regel begrepet om økonomisk statshåndverk til staters atferd som er rettet mot å oppnå politisk innflytelse eller autonomi internasjonalt.

Noen bidrag i litteraturen har dog begynt å anerkjenne at det kan være vanskelig å skille ut politikk som er rettet mot styrking av egen økonomis verdiskaping, konkurransekraft, sysselsetting og lignende, fra politikk som er rettet mot strategiske mål i internasjonal politikk, fordi en sterk økonomi vil igjen kunne benyttes til å oppnå mer makt og innflytelse internasjonalt. Selv om

[24] Se McAdam, Tarrow og Tilly (2001).

Japan og Mexico har omtrent like store befolkninger, er Japans bruttonasjonalprodukt (BNP) fem ganger så stort som Mexicos BNP. Det er ikke overraskende at Japan nyter langt større innflytelse i internasjonal politikk enn Mexico. Litteraturen vi gjennomgår i denne seksjonen argumenterer for at særlig teknologirivaliseringen mellom stormaktene visker ut skillelinjene mellom hva som er innenriksøkonomiske/-politiske og utenriksøkonomiske/-politiske mål.

Aggarwal og Reddie (2020) omtaler hva de ser som det «nye» økonomiske statshåndverket; studier som fokuserer på hvordan myndigheter tar politiske grep for å styrke eget næringsliv og teknologiutvikling, ikke bare for økonomisk vinning, men for å møte geopolitisk konkurranse i en stadig mer sammenkoblet økonomi med rask teknologisk utvikling.[25] Ifølge Aggarwal og Reddie (2020: 3) har nye «fundamentalt transformerende teknologier som kvantedatamaskiner, additiv industri, kunstig intelligens, genredigering og cybersikkerhet»[26] potensial til å true sikkerheten til USA og europeiske land. De viser at Kina tar i bruk økonomisk statshåndverk både for å bygge globale vinnere og støtte utenlandske investeringer i teknologibedrifter. Som motsvar har USA og europeiske økonomier tatt i bruk næringspolitikk, promotert nasjonale vinnere og screening av utenlandsinvesteringer for nasjonal sikkerhet. Dette leder til at økonomisk statshåndverk benyttes for å sikre hjemlig teknologisk nivå.

Det nye økonomiske statshåndverket kombinerer nasjonal sikkerhet med et perspektiv på økonomi, teknologi og innovasjon hentet fra nasjonale innovasjonssystemer (Christensen 1997; Kennedy og Lim 2018; Mowery 2009; Nelson 1993; Reppy 2000). Det pekes på hvordan det er nødvendig at teknologier som kan benyttes militært, fungerer både for militært og sivilt bruk – såkalt flerbruksteknologi (*dual use technology)* – for å oppnå skalaen som er nødvendig for innovasjon (Dombrowski og Gholz 2006, 2009; Molas-Gallart 1997). I et slikt perspektiv blir industriell politikk – aktiv politikk for å støtte egne næringer og bedrifter – og reguleringer viktige virkemidler for at nasjonale aktører oppnår og opprettholder teknologifronten (Aggarwal og Reddie 2020).

I artikkelen «Innovasjonsimperativet: teknologi og rivaliseringen mellom USA og Kina i det tjueførste århundret» argumenterer Kennedy og Lim (2018) for at voksende stormakter er nødt til å komme seg til teknologifronten der den ledende stormakten befinner seg – derav innovasjonsimperativ. Den voksende stormakten kan skaffe seg teknologien ved å innovere selv, kjøpe seg teknologien eller stjele den. Slik atferd leder til sikkerhetseksternaliteter for den ledende stormakten. Med det menes at aktiviteten til kommersielle aktører, for eksempel amerikanske teknologiselskaper som overfører teknologi til kinesiske selskaper for å tjene penger, samtidig forverrer USAs sikkerhet i rivaliseringen med Kina.[27] Den ledende stormakten vil da iverksette politikk for å unngå disse sikkerhetseksternalitetene som følger av innovasjonsimperativet. Malkin (2020) analyserer også handels- og teknologikonflikten mellom USA og Kina i et slikt

[25] Se Aggarwal og Reddie (2018; 2021) for fokus på henholdsvis cybersikkerhet og utenlandsinvesteringer.
[26] Ved å inkludere cybersikkerhet, antar vi at forfatterne henviser til behovet for å ha «hjemmelagde kapabiliteter» og «forbli banebrytende innen data- og nettverkssikkerhet» , siden cybersikkerhet i økende grad spiller en «kritisk rolle for nasjonal sikkerhet» (Aggarwal og Reddie 2018: 453). Cybersikkerhet kan da handle om teknologier og kapabiliteter for forebyggende sikkerhet, deteksjon og hendelseshåndtering, som bidrar til å beskytte ressurser og aktiviteter.
[27] Se Norris (2016) for en ytterligere utdyping om sikkerhetseksternaliteter av økonomisk aktivitet. En eksternalitet er et begrep fra samfunnsøkonomifaget om konsekvenser av atferd som ikke internaliseres av aktørene som utfører den økonomiske aktiviteten, for eksempel forurensing.

lys, og viser at kinesisk åndsverksbeskyttelse, oppgradering i globale verdikjeder og konkurransepolitikk må forståes i et sikkerhetsperspektiv. Weiss (2021) argumenterer for at USAs politikk for å sikre teknologisk overlegenhet har opplevd et comeback siden den kalde krigen ved å støtte gjennombrudd i militærteknologi, avansert industri og sikre industrielle verdikjeder.

Mens litteraturen har stort fokus på USA og Kina, finnes det her også flere studier om andre økonomiske stormakter, som Japan. Igata og Glosserman (2021: 26) redegjør for Japans nye økonomiske statshåndverk, som er en konsekvens blant annet av «den endrede kvaliteten ved avanserte teknologier» og Kinas geoøkonomiske og geopolitiske trussel. Her står hindring av teknologioverføring, reduksjon i avhengigheten av den kinesiske økonomien, begrense fremmede aktørers oppkjøp av landområder og få næringslivet til å tenke sikkerhet i høysetet (Igata og Glosserman 2021). I Japan er det lange tradisjoner både for at myndighetene styrer næringslivet mot økonomisk vekst og en diversifisert økonomi (Johnson 1982) og for at private aktører samarbeider med myndighetene på militær-sivil teknologi og produksjon (Samuels 1994). Men fremveksten av Kina som gigantøkonomi, med geopolitiske virkninger for Japans nabolag, og sino-amerikansk rivalisering, har ledet til ytterligere fokus på militær bruk av flerbruksteknologi (Govella 2021).

Det er altså mer krevende å utdefinere næringspolitikk, markedsregulering og handels- og investeringspolitikk i hjemlig økonomi fra økonomisk statshåndverk. Når stater har klare mål om å sikre overlegenhet innen militær- og flerbruksteknologi og iverksetter politikk for slike mål, gir det mening å inkludere slikt i den konseptuelle forståelsen av økonomisk statshåndverk. Vi setter imidlertid grensen ved politikk som har som mål å sikre sitt eget lands økonomiske konkurransekraft.[28]

2.3 Gap og utfordringer i eksisterende litteratur

Det er betydelige gap i eksisterende litteratur om hvordan ny teknologi kan endre staters muligheter til å benytte økonomisk statshåndverk.

For det første finnes det generelt få studier som studerer implikasjoner av den teknologiske utviklingen for økonomisk statshåndverk. Vi finner en interesse for ny teknologi i det nye økonomiske statshåndverket, men i hovedsak kun i form av å studere hvordan konkurransen mellom USA og Kina bidrar til politikk for å fremme og beskytte egne industrier og innovasjon. Vi finner kun et fåtall studier i den øvrige litteraturen om økonomisk statshåndverk som drøfter hvordan for eksempel internettplattformer, digitale valutaer og 5G-utbygging inngår i, eller påvirker muligheter for, økonomisk statshåndverk. Vi trekker disse studiene inn i drøftingen i kapittel 4. Det finnes imidlertid forskning ved FFI som drøfter konsekvenser av den teknologiske utviklingen og hvor også økonomiske forhold (som verdikjeder og ressursavhengigheter) løftes

[28] For eksempel foreslår Thurbon og Weiss (2021: 111) å anse Sør-Koreas politikk for å fremme egen industris produksjon av intelligente robotsystemer for å møte den (geo)økonomiske trusselen fra «et økende teknologisk konkurransedyktig Kina og svært kostnadsmessig konkurransedyktig Japan». Vi mener dette ligner for mye på tradisjonell økonomisk politikk for å fremme egen industriell og økonomisk utvikling til at det bør tas med i økonomisk statshåndverksbegrepet, men anerkjenner likevel at en sterk økonomi kan øke staters muligheter for å ta i bruk økonomiske virkemidler.

frem. Det åpner muligheter for å koble sammen innsikt fra studier av utfordringer, sårbarheter og risikoer ved ny teknologi med økonomisk statshåndverkperspektivet, inkludert hvordan økonomiske virkemidler kan legge til rette for annen virkemiddelbruk i fremtiden. I denne rapporten søker vi å begynne på nettopp denne koblingen.

For det andre finnes det, så vidt oss bekjent, heller ingen helhetlig evaluering av hvordan den teknologiske utviklingen potensielt påvirker og endrer ulike former for økonomisk statshåndverk. Det finnes studier som belyser hvordan enkelte forhold ved den teknologiske utviklingen kan ha konsekvenser for staters bruk av økonomiske virkemidler, som for eksempel seksjon 2.2.2 redegjør for. Men det mangler en omforent evaluering av hvordan den teknologiske utviklingen kan påvirke både staters muligheter til å utøve makt og til å akkumulere makt gjennom økonomisk statshåndverk. Ved å ta for oss hver av handlingsmåtene av økonomisk statshåndverk, presentert i tabell 1.1, søker vi å forstå om og hvordan den teknologiske utviklingen kan medføre endringer innen hver av disse handlingsmåtene.

For det tredje har eksisterende litteratur en skjevhet i retning av et fokus på stormakter, hvor det først og fremst er konsekvensene av den teknologiske utviklingen på stormakters muligheter til å utføre økonomisk statshåndverk som er gitt oppmerksomhet. Den samme skjevheten observerer vi i litteraturen om økonomisk statshåndverk mer generelt, hvor det særlig er stormaktene USA og Kina som er i fokus (se også Waage, Kvalvik og Lindgren 2021c). Denne skjevheten resulterer i at diskusjonene og hypotesene presentert i kapittel 4 også preges av et fokus på særlig stormakters muligheter til å utøve økonomisk statshåndverk i lys av den teknologiske utviklingen.

For det fjerde mangler det oversikter over staters teknologikapabiliteter og kobling til hvordan slike kapabiliteter kan utnyttes i form av økonomisk statshåndverk samt andre lands avhengighet av disse kapabilitetene. Kan dominans innenfor noen av de nye teknologiene bidra til makt innenfor ulike subdomener av økonomien, som handel, finans og FoU? Hvilke land vil i så fall besitte og være i stand til å utnytte dette maktpotensialet? Vi berører slike spørsmål uten at vi besvarer dem i denne rapporten, spesielt når vi diskuterer hvordan konkurransen mellom USA og Kina også vil ha implikasjoner for allierte land i kapittel 4. Vi tar også med oss denne mangelen i konklusjonen av rapporten i kapittel 6 der vi drøfter mulige retninger for fremtidig forskning innenfor krysningen av nye teknologier og økonomisk statshåndverk.

3 Hvordan påvirker ny teknologi økonomisk aktivitet?

Økonomiske virkemidler er staters manipulering, eller på andre måter utnyttelse av, økonomiske transaksjoner til strategiske formål (se delkapittel 1.2). Det betyr altså at statsledelsen søker å utøve kontroll eller innflytelse over aktiviteten til økonomiske aktører for derigjennom å oppnå sine utenrikspolitiske, strategiske mål. Før vi drøfter konsekvenser av ny teknologi for staters bruk av økonomisk statshåndverk, mener vi derfor at det er nyttig å styrke forståelsen av hvordan ny teknologi påvirker nasjonal og internasjonal økonomisk aktivitet. Dette danner et grunnlag for å evaluere hvordan stater kan utnytte økonomiske transaksjoner på nye eller endrede måter for å utføre økonomisk statshåndverk.

I dette kapittelet søker vi altså å besvare problemstilling 1 om hvordan nasjonal og internasjonal økonomisk aktivitet blir påvirket av den teknologiske utviklingen i 4IR på måter som former mulighetsrommet for økonomisk statshåndverk. Vi identifiserer, og utdyper om, følgende endringer og utviklingstrekk: betydningen av data (delkapittel 3.1), økt kompleksitet (delkapittel 3.2), økt kunnskapsbehov og tjenesteutsetting (delkapittel 3.3), økt markedskonsentrasjon (delkapittel 3.4), organisasjonsendringer og internasjonalisering (delkapittel 3.5), automatisering av arbeidsoppgaver og beslutningstaking (delkapittel 3.6) og betydningen av fremvoksende markeder (delkapittel 3.7). Der det er relevant, trekker vi inn økonomisk teori for å styrke forståelsen av hva som driver utviklingstrekkene. Vi oppsummerer de viktigste poengene i delkapittel 3.8.

3.1 Betydningen av data

Allerede for femten år siden understreket Ayres (2007) mulighetene som ligger i bruken av store datasett til prediksjon og beslutningsstøtte, og siden da har data blitt en stadig viktigere innsatsfaktor i både økonomisk og strategisk aktivitet. Vi innledet rapporten med en kort presentasjon av hvordan den teknologiske utviklingen i 4IR ikke bare bestod av ny teknologi, men også sammenkoblingen av nettverk av kommunikasjon og relasjoner mellom milliarder av mennesker og elektroniske produkter. Mye ny teknologi finnes nettopp i krysningspunktet mellom rask og eksponentiell utvikling av maskinvare, programvare og informasjonstilgang. Stordata krever både kraftig maskinvare og smart programvare for å bli utnyttet fornuftig. Samtidig er verdien av teknologier, som kunstig intelligens, skytjenester og tingenes internett prisgitt tilgangen til data.

The Economist (2017a, 2017b) omtaler derfor data som «oljen for den digitale tidsalderen», både fordi data, som olje, fraktes i «rørledninger» (*pipelines*) og fordi begge er sentrale «råstoffer» (*feedstock*) i verdensøkonomien.[29] Maskinlæringsalgoritmer trenger som regel store datasett for å trenes opp. Tilgang til data, av god kvalitet, legger til rette for å kunne produsere og tilby nye, og bedre, produkter og tjenester basert på KI-teknologi. Data er også verdifullt for statistiske

[29] Som en respondent påpekte under intervjuet, kan imidlertid hvem som helst i prinsippet etablere seg som en sentral aktør innen IKT – i motsetning til naturressurser som olje.

analyser uten bruk av kunstig intelligens (se f.eks. Ayres 2007). Datadrevet innsikt og beslutningstaking kan videre forbedre og optimalisere virksomheter og gjøre dem mer konkurransedyktige.

Den teknologiske utviklingen bidrar også til å skape nye muligheter for å få tilgang til, og ta i bruk, data. Som Farsund mfl. (2022: 26) påpeker, «har utviklingen av teknologier som internett, økt prosesseringskraft i datamaskiner og reduserte kostnader for datalagring gjort at det har blitt enklere for virksomheter å overføre, samle, lagre og analysere data». De nye teknologiene kjennetegnes av at de omgir oss «overalt», og både næringslivet, samfunnet og Forsvaret vil i økende grad bli avhengig av digitale løsninger. Det medfører også at data og informasjon vil bli samlet inn «overalt», og det vil bli vanskelig å beskytte seg mot datainnsamlingen – til forskjell fra tidligere hvor en løsning hadde vært «å legge fra seg telefonen» (Farsund mfl. 2022: 42).

Som følge av at data stadig blir viktigere, blir også tilgang og eierskap til data viktigere. Farsund mfl. (2022: 27) trekker frem flere eksempler på oppkjøp hvor det har vært «informasjonen eller informasjonsinfrastrukturen» i det oppkjøpte selskapet som har motivert investeringen, inkludert Facebooks oppkjøp av Instagram (2012) og WhatsApp (2014) og IBMs oppkjøp av The Weather Company (2015) og Truven Health Analytics (2016). I tillegg har dataforhandlere (*data brokers*) vokst frem som en ny «industri» (Farsund mfl. 2022: 26), som spiller en sentral rolle i dataøkosystemet (Yeh 2018). Disse forhandlerne «sammenstiller personlig data fra mange kilder» og selger de sammenstilte dataene til selskaper over hele verden (Yeh 2018: 282; se også Ayres 2007: 134–135).

Land har imidlertid forskjellige reguleringer rundt mulighetene til datainnsamling, særlig på grunn av ulik vekting av å ivareta personvern. Personvern beskytter enkeltindividers data, men kan samtidig redusere aktørers muligheter til å samle inn, sammenstille og analysere store datasett. Datas betydning for kunstig intelligens skulle tilsi at land med mildere lovgivning for innsamling og bruk av data, har et fortrinn i den globale konkurransen. I den forbindelse sammenligner Aho og Duffield (2020) EUs og Kinas politikk og regulering rundt stordata og personvern. Mens EUs GDPR kan bli sett på som en reaktiv respons, som begrenser selskapers bruk av persondata, er Kinas sosiale kredittsystem en proaktiv respons, hvor overvåking og innsamling av persondata i kombinasjon med kunstig intelligens blir aktivt utnyttet. De påpeker at det kinesiske systemet, i teorien, legger til rette for «massedatainnsamling, maskinlæringsalgoritmer og, etter hvert, sanntid kybernetisk tilbakemelding og justering» (Aho og Duffield 2020: 205), mens de anerkjenner at det har blitt advart om at EUs system kan ha en «kjølende effekt på forskning og utvikling av nye stordata- og KI-teknologier» (Aho og Duffield 2020: 206). Det gjenstår likevel å se hvilken økonomisk effekt EUs GDPR vil ha, siden systemet også bidrar til å harmonisere dataregulering på tvers av unionen og fordi domstoler og GDPR-institusjoner i årene som kommer vil avgjøre hvordan regelverket faktisk blir implementert (Aho og Duffield 2020).

I tillegg til forskjeller i reguleringer rundt muligheter til å samle inn og benytte data, er det også forskjeller i hvordan ulike land og aktører behandler og bearbeider sine data, for eksempel innen «merking» (*labeling*). Det betyr at de aktørene som over tid blir i stand til å tilby de beste produktene og tjenestene, kan være de som har best muligheter og ferdigheter til å jobbe med

data. Ved å kunne tilby de beste produktene og tjenestene, vil disse aktørene også skaffe seg større markedsandeler enn konkurrenter.

3.2 Økt kompleksitet

Det er mange årsaker til at kompleksiteten øker ved bruk av nye teknologier som kunstig intelligens, 5G, skytjenester og tingenes internett. I dette delkapittelet tar vi kort for oss noen av årsakene som løftes frem i forskning på disse teknologiene ved FFI, mens vi henviser til andre FFI-publikasjoner for ytterligere detaljer (se f.eks. Farsund mfl. 2022). I tillegg utdyper boks 3.1 om ulike former for kompleksitet knyttet til tekniske systemer: samspillskompleksitet, koblings-kompleksitet, organisatorisk kompleksitet, verdikompleksitet og dynamisk kompleksitet.

Boks 3.1 – Kompleksitet

Farsund mfl. (2022: 23–25) og Birkemo, Kristiansen og Farsund (2021: 59) redegjør for ulike egenskaper ved et system som er relevante å vurdere for å forstå kompleksitet:

Samspillskompleksitet: Hvordan avhengigheter er mellom og innad i de tekniske systemene. Interne avhengigheter kan forståes som et sett med aktiviteter mellom elementer eller funksjoner i et system eller en infrastruktur. Eksterne avhengigheter kan forståes som avhengigheter til andre (komplekse) systemer/infrastrukturer, for tilgang til ressurser og tjenester (som ekom, kraft eller skytjenester), data (som værdata), maskin-vare (som antenner og sensorer) og/eller programvare fra samme programvare-bibliotek.

Koblingskompleksitet: I hvilken grad koblinger mellom tekniske systemer og organisatoriske elementer er tidskritiske. Sammenkoblinger mellom elementer og funksjoner i systemer/infrastrukturer kan være tette eller løse. Tette koblinger innebærer at en handling ett sted har umiddelbare effekter et annet sted, og slike koblinger tolererer dermed ikke forsinkelser eller slakk. Løse koblinger responderer derimot saktere og er mer robuste med tanke på feilhåndtering. Tette koblinger er derfor mer komplekse enn løse koblinger.

Organisatorisk kompleksitet: Hvordan avhengigheter er mellom de involverte organisasjonene og mellom organisasjonene og de tekniske systemene. Det kan være mange aktører involvert i leveransen av en tjeneste – private virksomheter, offentlige instanser og/eller utenlandske virksomheter. Egenskaper ved aktørene kan også endre seg, for eksempel ved oppsplitting av virksomhet eller sammenslåinger og oppkjøp. Jo flere aktører som er involvert, desto større vil den organisatorisk kompleksiteten være.

Verdikompleksitet: Graden av oversikt over hvordan et teknisk system eller et organisatorisk element bidrar oppover i verdikjeden. Verdikompleksiteten er lav dersom man har god oversikt over hvilke verdier systemet/infrastrukturen bidrar til, mens den er høy dersom man har liten oversikt. Sistnevnte kan for eksempel være tilfellet fordi mange bruker (både indirekte og direkte) systemet/infrastrukturen.

Dynamisk kompleksitet: Hvordan tekniske systemer, organisatoriske elementer og koblinger endrer seg over tid. Dynamisk kompleksitet er for eksempel knyttet til hvor ofte det skjer programvareoppdateringer, hvor ofte det skjer endringer i den fysiske infrastrukturen eller hva infrastrukturen brukes til, og/eller hvor ofte det skjer organisatoriske endringer.

En årsak til at kompleksiteten øker med den teknologiske utviklingen, er at produkter og tjenester i seg selv blir mer komplekse. Det kan for eksempel komme av bruken av automatiserte algoritmer, som er krevende å etterprøve, både til å utføre oppgaver og drifte og vedlikeholde systemer, fordi store datamengder og kompleksiteten i oppgaveløsning gjør at flere og flere systemer avhenger av kunstig intelligens for å fungere (se delkapittel 2.1). Denne typen kompleksitet er en form for samspillskompleksitet.

I tillegg blir systemer i økende grad sammenkoblet, hvor blant annet kritiske infrastrukturer vil ha «et intrikat nettverk av vekselvirkninger mellom de ulike komponentene eller delsystemene som utgjør infrastrukturen» (Farsund mfl. 2022: 23).[30] For eksempel vil 5G ha avhengigheter både innad i infrastrukturen og til andre infrastrukturer som skytjenester, og andre kritiske infrastrukturer som kraftforsyning vil bli kjennetegnet av lignende komplekse sammenkoblinger (Farsund mfl. 2022). Tette koblinger og avhengigheter kan bidra til å øke koblingskompleksiteten. Bruken av kunstig intelligens vil dessuten gjøre det mer krevende å skaffe seg oversikt over disse sammenkoblingene og avhengighetene.

Videre vil produkter som bygger på de nye teknologiene kjennetegnes av at de ikke er ferdige når de blir solgt, men videreutvikles og oppdateres gjennom hele levetiden. Leverandørene av produktene vil derfor ha mange muligheter til å endre produktet etter salg, ofte digitalt gjennom programvareoppdateringer. Kontinuerlige oppdateringer og endringer bidrar også til å øke kompleksiteten. Dette er en form for dynamisk kompleksitet.

Det er forventet at (digitale) verdikjeder[31] vil bli lengre, mer komplekse og mer uoversiktlige, som følge av at mange flere aktører blir involvert i verdikjeden for nye teknologier enn hva som har vært tilfellet for mer tradisjonelle teknologier. Maskinvare og programvare som inngår i produkter og tjenester kan dessuten befinne seg i ulike geografiske områder – potensielt over hele verden (Farsund mfl. 2022). Det vil også være utfordrende å ha fullstendig kontroll på verdikjedene til enhver tid, særlig fordi det kan skje hyppig utskiftning i leverandører blant annet basert på hvem som tilbyr den beste programvaren, mens kunstig intelligens blir benyttet for å håndtere det store antallet underleverandører (Bentstuen mfl. 2018). Det vil også være krevende å ha full

[30] Farsund mfl. (2022: 22) forklarer hvordan infrastruktur både kan bli beskrevet som «et nett av faste anlegg som er grunnlaget for en virksomhet», slik som «systemet av veier, havner, flyplasser, ledningsnett med mer, som betjener næringslivet og husholdningene i et land eller område». Samtidig påpeker Farsund mfl. (2022: 23) hvordan infrastruktur også kan «betraktes som et konsept som formes av teknologiene som samfunnet har tilgjengelig og som følgelig er i konstant endring», slik som «skiftet fra romerske akvedukter til dagens vann- og avløpssystemer».

[31] Med henvisning til Lysne-utvalgets rapport (NOU 2015:13 2017) forklarer Bentstuen mfl. (2018: 7) digitale verdikjeder som: verdikjeder som «dekker alle de enkeltelementene som til sammen bygger opp en digital tjeneste som benyttes av en bruker, og strekker seg fra transport- og transmisjonsnett, via aksessnett til tale- og datatjenester».

oversikt over alle brukere av en tjeneste, samt verdien til tjenesten for brukerne. For eksempel vil økt bruk av tingenes internett i samfunnet gjøre det vanskeligere å vurdere verdien til 5G-nettet (Farsund mfl. 2022). Dessuten forventer Bentstuen mfl. (2018) at brukere i økende grad tar i bruk digitale tjenester fra store internasjonale selskaper, uten full kontroll over verdikjedene og hvor personlige data havner. Samlet bidrar disse forholdene til å øke den organisatoriske kompleksiteten og verdikompleksiteten.

Med fremveksten av avanserte smartbyer, vil alle egenskapene ved kompleksitet omtalt i boks 3.1 gjøre seg gjeldende (Farsund mfl. 2022: 35). For det første vil det være mange avhengigheter, både internt mellom de IoT-baserte infrastrukturene som inngår i smartbyen og til andre infrastrukturer som ekom og kraft, som skaper en høy samspillskompleksitet. For det andre vil koblingskompleksiteten være høy som følge av at det er tette koblinger og ofte behov for kort responstid. For det tredje vil det være krevende å vurdere verdien av noen systemer for brukere og samfunnet, som gjør at verdikompleksiteten øker. For det fjerde vil mange forskjellige aktører være involvert i drift, vedlikehold og videreutvikling av infrastrukturene, som øker den organisatoriske kompleksiteten. Og for det femte vil den dynamiske kompleksiteten være høy, siden systemene jevnlig blir oppdatert i tillegg til at blant annet eierforhold og datautveksling mellom systemer jevnlig kan bli endret.

Det er imidlertid krevende å konkludere hva den samlede effekten på sikkerhet av økt kompleksitet vil være. Mens bruken av kunstig intelligens til drift, vedlikehold og forvaltning medfører potensielt negative effekter i form av svekket kontroll og oversikt over informasjon og verdikjeder, kan det også resultere i positive effekter. Særlig trekker Bentstuen mfl. (2018) frem at KI-systemer har muligheten til å agere og tilpasse seg gjeldende forhold, for eksempel ved å bytte underleverandører hyppig, som øker uavhengigheten til enkelte leverandører og teknologier.[32] Videre poengterer Bentstuen mfl. (2018) at den økte kompleksiteten, med manglende muligheter for oversikt og kontroll av verdikjeder, også vil være en utfordring en eventuell trusselaktør vil stå overfor. Vi noterer oss altså at kompleksiteten kan bidra til at mottakerstater blir mer sårbare overfor økonomisk statshåndverk, men også at økonomisk statshåndverk kan bli vanskeligere å utføre for avsenderstater.

3.3 Økt kunnskapsbehov og tjenesteutsetting

Mange av de nye teknologiene er kunnskapskrevende, og kunnskap spiller en viktigere rolle for evnen til å anskaffe, utvikle, drifte og vedlikeholde – samt kontrollere sikkerheten til – disse teknologiene enn hva som har vært tilfellet for mer tradisjonelle teknologier. For eksempel krever utvikling av KI-algoritmer høy kompetanse. Gjennom intervjuene avdekker vi flere ulike typer kompetanse som antas å bli stadig viktigere fremover: kompetanse på programvare, bestillerkompetanse, teknologisk forståelse hos beslutningstakere, kompetanse om sikkerhet, juss og etikk knyttet til ny teknologi, kompetanse på å integrere systemer og legge til rette for datautveksling og dataforvaltningskompetanse.

[32] Merk likevel at det gjelder håndtering av hendelser som forekommer hyppig. Håndtering av kritiske hendelser som oppstår sjeldent kan imidlertid skape utfordringer for algoritmene. For en illustrativ figur, se Esposito mfl. (2018).

Behovet for, og konkurransen om, kunnskap medfører også at det er vanskeligere for selskaper å rekruttere og beholde talenter og eksperter som er nødvendige for å utvikle og produsere løsninger som bygger på teknologiene. Samlet kan dette motivere selskaper til å søke å få tak i kunnskap, som med data, ved å kjøpe opp eller kjøpe seg inn i andre selskaper. Det vil nok imidlertid være mer vanlig at selskaper søker å kjøpe utvalgte tjenester fra andre selskaper, nasjonalt eller internasjonalt, som besitter nødvendig kunnskap og kompetanse på området. Tjenesteutsetting bidrar til at «virksomheten holder følge med teknologiutviklingen og får tilgang på personell med relevant kompetanse og verktøy» i tillegg til å «redusere (drifts)kostnader og gi mulighet til å fokusere på kjerneoppgaver» (Birkemo, Kristiansen og Farsund 2021: 16).

Bentstuen mfl. (2018) fremhever også hvordan kunnskap om personvern og krav til oppbevaring av personopplysninger kan være en kompetanse som selskaper ikke vil klare å besitte i tilstrekkelig grad. I forbindelse med drift og forvaltning av selskapers datasikkerhet, forventer Bentstuen mfl. (2018: 18) at det spesielt er små og mellomstore bedrifter som vil velge å sette ut tjenestene til «tredjeparts spesialister». Det kan på sikt øke personvern og datasikkerhet, med mindre utilsiktet spredning av personinformasjon (Bentstuen mfl. 2018).

Den samfunnsøkonomiske litteraturen diskuterer også kompetansebehovene for kunstig intelligens og andre teknologier. Benzell og Brynjolfsson (2019) mener at det finnes noe i økonomien som har en uelastisk tilbudskurve og som ikke kan digitaliseres. Dette «noe» kan være visse typer kompetanse og ferdigheter som begrenser implementeringen av kunstig intelligens, automatisering, digitalisering og andre nye teknologier – hva de kaller «genier» eller «superindivider». Hvis det er slik at det er vanskelig å få tak i nok arbeidskraft som kan implementere nye teknologier i næringslivet og det offentlige, underbygger det argumentene fra både FFI-forskningen og våre respondenter om at det er økt kunnskapsbehov med nye teknologier og at disse teknologiene da bidrar til økt tjenesteutsetting.

Litteraturen peker dessuten på at teknologisk fremgang er forbundet med en ytterligere akkumulering av kunnskap. Det innebærer at den menneskelige «brønnen» med kunnskap utvides. For å bidra i fronten av menneskelig kunnskap, må forskere, teknologer og andre bidragsytere lære mer enn tidligere. Jones (2009) finner at alder ved første oppfinnelse, spesialisering og teamarbeid øker med den teknologiske utviklingen. I tillegg finner han at spesialisering og teamarbeid har større betydning i områder med «dypere kunnskap». Selv med et mindre ambisiøst mål som at noen skal forstå hva som skjer i den teknologiske fronten – og ikke nødvendigvis bidra med ny kunnskap, krever det altså mer og mer tid og krefter enn tidligere. Samtidig øker utdanningsnivået i moderne økonomier og de vier en større og større andel av arbeidskraften til forskning og utvikling. Dette motvirker effekten Jones (2009) identifiserer, men det er allikevel begrensninger på hvor mange år folk kan bruke i utdanning og hvor stor andel av arbeidsstokken som kan vies til forskning og utvikling. I et bidrag om at produktiviteten per forsker reduseres med den teknologiske utviklingen – fordi mer og mer av det mulige er allerede identifisert og oppfunnet – viser Bloom mfl. (2020) at antallet forskere som skulle til for å doble tettheten av transistorer på et areal hvert andre år er 18 ganger så stort som på 1970-tallet. Det skal altså langt mer innsats til for å få til samme teknologiske utvikling som tidligere.

3.4 Økt markedskonsentrasjon

I takt med den teknologiske utviklingen, har det skjedd en markant endring i den industrielle organiseringen i mange næringer i moderne økonomier – markedskonsentrasjonen har økt. Fra samfunnsøkonomisk litteratur kan vi finne argumenter for hvorfor dette er tilfellet. Økt konsentrasjon kan skyldes enten at konkurransen har falt (De Loecker, Eeckhout og Unger 2020; Gutiérrez og Philippon 2017) eller at forskjeller i produktivitet bidrar til at høyproduktive bedrifter tar større markedsandeler (Autor mfl. 2020). Cremér, de Montjoye og Schweitzer (2019) argumenterer for at tilgangen til og evnen til å lagre og benytte massive data, ekstremt skalautbytte og sterke nettverkseffekter, gir store fordeler til eksisterende bedrifter og leder til en høyere markedskonsentrasjon med et fåtall tilbydere.

Autor mfl. (2020) mener at økt markedskonsentrasjon skyldes underliggende teknologiske endringer som favoriserer de mest produktive[33] bedriftene – såkalte superbedrifter.[34] De nevner at høyere forbrukersensitivitet overfor priser på varer og tjenester og økt konkurranse som følge av globalisering eller bedre leteteknologier (som på internett, se Akerman, Leuven, og Mogstad 2022) vil kunne bidra til slik økt favorisering. Det vil også plattformkonkurranse eller økt skala-utbytte av immateriell kapital eller forbedringer i IKT.

Crouzet og Eberly (2018) undersøker detaljhandelen (*retail*) i USA og finner at den økte konsentrasjonen skyldes underliggende produktivitetsendringer som følge av «teknologidrevne forbedringer i forretningspraksiser» som logistikk og organisering. Økt viktighet av immaterielle verdier kan forklare høy produktivitetsvekst, lav grad av fysiske investeringer, høy verdsettelse og økt konsentrasjon.

I intervjuene med FFI-forskere ble det påpekt hvordan det ofte kun er få, men store leverandører i verden innen teknologiområdene. For eksempel er det kun noen få globale leverandører innen 5G og skytjenester, og det samme gjelder også for operativsystemer. Som vi kommer tilbake til i kapittel 4, kan mottakerlands tilgang til alternative leverandører, produkter og tjenester påvirke mulighetene til å utføre økonomisk statshåndverk.

3.5 Organisasjonsendringer og internasjonalisering

Det er også argumentert for at bedrifter gjennomgår organisasjonsendringer som følge av lavere letekostnader[35] (*search costs*) i kjølvannet av den pågående, teknologiske utviklingen (Goldfarb

[33] Med produktive menes bedrifter med høyt prispåslag (pris minus kostnader) og relativt lav arbeidsinnsats.

[34] Autor mfl. (2020) tester teorien og finner at i) det har skjedd en økning i konsentrasjonen, med flere større bedrifter og økt grad av spesialisering, ii) industrier med økt konsentrasjon har sett større nedgang i arbeidskraftsandelen, iii) nedgangen skyldes reallokering av salg til bedrifter med lav arbeidskraftsandel, iv) denne reallokeringen er størst i næringer med høyest økning i konsentrasjonen, v) næringer med høyest konsentrasjon har også høyest vekst i produktivitet og innovasjon, vi) større bedrifter har høyere prispåslag, og vii) trenden sees ikke bare i USA, men også i andre OECD-land.

[35] Med letekostnader menes kostnader ved å søke etter informasjon (Goldfarb og Tucker 2019).

og Tucker 2019). Litteraturen om lavere letekostnader i det digitale rom er inspirert av samfunnsøkonomisk lete- og *matching*-litteratur (Diamond 1971; Stigler 1961; Varian 1980).[36] Lete- og matchinglitteraturen viser at det er knyttet kostnader – spesielt tid, men også andre ressurser – til å lete etter informasjon om varer, tjenester og jobber. Digitalisering bidrar til at leting blir mer effektiv og målrettet. Digitaliseringen har også bidratt til fremveksten av plattformtjenester (inklusive såkalt deletjenester) som kobler sammen forbrukere og produsenter, arbeidstakere og arbeidsgivere, gründere og investorer, osv., både nasjonalt og på tvers av landegrenser. Lavere letekostnader endrer også organiseringen innad i bedrifter: bedre informasjonsflyt kan øke sentraliseringen ved at ledere får bedre oversikt over bedriftens aktiviteter og virksomhetsområder, mens lavere kommunikasjonskostnader kan bidra til desentralisering ved at ansatte får bedre informasjon som tidligere var forbeholdt ledere på toppen av bedriften (Bloom mfl. 2014; Garicano 2000). Fremtidige bedrifters organisering kan derfor gå i retning av mer sentralisering. I så fall vil det tjene utenlandske bedrifters virksomheter å ha mer kontroll fra hovedkontoret i utlandet. Men organiseringen kan også bli mer desentralisert. Da vil datterselskaper oppleve mer frihet og autonomi i sin daglige drift. Økonomisk statshåndverk handler om avsenderstatens evne til å kontrollere og manipulere kommersielle aktørers atferd. Hvordan ny teknologi endrer multinasjonale bedrifters gevinster og kostnader knyttet til kontroll og autonomi kan igjen påvirke staters evne til økonomisk statshåndverk.

Litteraturen om lavere letekostnader kan videre bidra til å forklare hvordan digitalisering legger til rette for økt internasjonalisering. Digitaliseringen har også ledet til lavere transaksjonskostnader utenfor bedriften, og således til internasjonalisering av mange arbeidsoppgaver som bedrifter tidligere utførte lokalt (Agrawal, Lacetera og Lyons 2016). Kostnaden av å transportere informasjon i bits er dessuten nær null. Denne egenskapen er i sterk kontrast til transport av fysiske varer. Kommunikasjon og digitale produkter og varer er derfor nesten likegyldig overfor fysisk distanse. Men også transport av fysiske varer har blitt billigere av digitale bestillinger, fordi digitaliseringen bidrar til bedre koordinering og optimalisering av transporten.

Bentstuen mfl. (2018: 16) hevder også at selskaper «vil samle all sin overordnete drift og forvaltning på regionalt (verdensdel) eller globalt nivå», og at de vil velge å utføre drift «fra lokasjoner med billig og stabil datakraft, som ikke nødvendigvis befinner seg i Norge» – med mindre det skapes insentiver som tilrettelegger for å beholde virksomhet nasjonalt.

3.6 Automatisering av arbeidsoppgaver og beslutningstaking

Samfunnsøkonomifaget er spesielt opptatt av hvordan ny teknologi vil kunne automatisere menneskelige arbeidsoppgaver og beslutningstaking. I boks 3.2 utdyper vi om sammenhengen mellom ny teknologi – særlig kunstig intelligens og automatisering – og økonomisk vekst.

[36] For oppsummering om leteteorien på norsk, se Lindgren og Presterud (2020, 2021c, 2021a, 2021b).

Boks 3.2 – Ny teknologi og økonomisk vekst

Lindgren og Brummer (2022) gjennomgår litteraturen om teknologisk utvikling og økonomisk vekst i samfunnsøkonomifaget, med spesielt fokus på kunstig intelligens. De finner både pessimister og optimister i forskningsfronten. Pessimistene argumenterer for at kunstig intelligens er en *hype* og at teknologien i beste fall vil ha en liten effekt på økonomisk vekst i modne økonomier (Gordon 2012). Et nøkkelargument mot nye teknologiers påvirkning på vekstraten er at innovasjon og nye ideer blir vanskeligere og vanskeligere å oppdage og utnytte (Bloom mfl. 2020; B. F. Jones 2009; C. I. Jones 1995, 2002). Det er også viktig å huske på at eksponentialiteten i vekstrater tilsier at produktivitet, innovasjon og teknologisk utvikling må forbedres mer og mer for å holde samme vekstrate over tid (Triplett 1999).

Optimistene argumenterer for at kunstig intelligens har potensial til å være en såkalt allsidig teknologi (*general purpose technology* – GPT). En GPT er karakterisert av «utbredthet, iboende potensial for teknologisk forbedring, og 'innovasjons-komplementariteter', som gir opphav til økende skalautbytte» (Bresnahan og Trajtenberg 1995). GPT-er som dampmaskinen, fabrikksystemet, den elektriske motoren og halvledere har hatt en dramatisk effekt over en lengre tidsperiode på den økonomiske vekstraten fordi de er implementert i mange sektorer i samfunnet (Bresnahan og Trajtenberg 1995). Sammen med kraftigere maskinvare og sterk økning i data, vil maskinlæring og annen relatert kunstig intelligens kunne påvirke vekstraten betydelig (Mayer-Schönberger og Ramge 2018). Kunstig intelligens vil også kunne være en «oppfinnelse av en metode for å oppfinne» (*invention of method of inventing* – IMI) (Cockburn, Henderson, og Stern 2018; Griliches 1957), med muligheter for å forbedre innovasjons- og nyskapingsprosesser i økonomien (Cockburn, Henderson og Stern 2018).

Et modererende element i effekten av kunstig intelligens selv for optimistene, er illustrert ved Baumols (1967) økonomiske teori om «kostnadssykdom». Akkurat slik næringer med høy produktivitetsvekst (industrinæringer) opplevde fallende andeler av BNP og sektorer med lav produktivitetsvekst (tjenestenæringer) opplevde økende andeler av BNP, vil muligens fremtidig økonomisk vekst bli hindret av reduserte andeler verdiskapning i KI-automatiserte næringer (Aghion, Jones og Jones 2019).

Hvis ny teknologi betyr automatisering av arbeidsoppgaver som tidligere var monopolisert av menneskelig arbeidskraft, for eksempel på grunn av behov for menneskets kognitive evner, vil økonomien se svært annerledes ut over tid. Autonome roboter, systemer og algoritmer vil lede til at innholdet i arbeidsoppgaver utført av mennesker vil endres, og nye arbeidsoppgaver vil komme til (Acemoglu og Restrepo 2018). Det betyr samtidig at stater, bedrifter og eksperter mister oversikt over hva de autonome systemene utfører. Kompetansen om utførelsen av de automatiserte arbeidsoppgavene vil også forvitre eller bli for kompliserte å forstå. Det er vanskelig å si per i dag i hvilken grad kunstig intelligens vil overta for menneskelig intelligens på ulike arbeidsområder.

Boks 3.2 fremhever at det er stor debatt om dette i samfunnsøkonomifaget, og at det på ingen måte er konsensus om fremtiden.

Domingos (2015) mener at kombinasjonen av kunstig intelligens og digitalisering gjør at vi vil bruke programvare til å ta langt flere beslutninger om kjøp av produkter og tjenester, bytte av jobb og til og med kanskje venner og partnere. Harari (2016) spekulerer i en fremtid der datamaskinene kjenner menneskene bedre enn de selv gjør. Det vil kunne lede til at mennesker frivillig oppgir mange valg de står overfor til intelligent programvare. På bedriftssiden er det også forventet at digital tilgang til informasjon muliggjør at bedrifter lar datamaskinene ta beslutninger i større grad (Iansiti og Lakhani 2020). Selv en nøktern vurdering vil forvente en forsterkende effekt av at mer informasjon vil tilgjengeliggjøres digitalt, som sammen med mer presis programvare (KI), vil gjøre at forbrukere, investorer, bedrifter og andre økonomiske aktører vil bruke algoritmer for å ta beslutninger.[37] Slik vil det skapes enda mer digital informasjon, til bruk i å forbedre maskinenes intelligens.

3.7 Betydningen av fremvoksende markeder

Fremvoksende markeder blir nok viktigere i fremtiden. For det første bidrar ny teknologi til nettverkseffekter i den forstand at flere brukere øker verdien av tjenestene for brukerne, i tillegg til at flere brukere genererer mer bruksdata som kan utnyttes til å forbedre og videreutvikle tjenestene. For det andre er fremvoksende markeder karakterisert av store befolkninger som gir statsledelsen evne til å stille krav til vestlige lands inntreden i markedene. På den annen side vil ny teknologi kunne redusere muligheten for fremvoksende økonomier til å benytte vekststrategi nummer 1 for lavinntektsland de siste 50 årene, nemlig å tilby en stor befolkning med lave lønninger til disposisjon for vestlige bedrifter. Vi utdyper kort om disse tre forholdene i dette delkapittelet.

Mange produkter og tjenester produsert med nye og/eller moderne teknologier, har nettverkseffekter (også kalt nettverkseksternaliteter eller skalautbytte i etterspørselen). Intuisjonen bak nettverkseffekter er at verdien av produkter og tjenester øker med antallet brukere. Tjenestene blir derfor mer verdt og attraktive for alle eksisterende og potensielle kunder, hvis bedriften er i stand til å utvide kunderepertoaret. Plattformtjenester som Ebay, finn.no og Airbnb blir bedre også av å utvide antallet tilbydere. Verdien av tjenestene fra sosiale medier som Facebook, Twitter og WeChat henger tett sammen med at andre i ditt sosiale nettverk deltar. Mange andre typer produkter og tjenester – fra Googles søke- og karttjenester til selvkjøringsegenskapene til Tesla – blir bedre av at mange bruker dem. Siden fremvoksende markeder er blant de mest folkerike økonomiene i verden (Kina, India, Brasil, osv.), vil betydningen deres øke. Det gir også selskaper utviklet internt i disse landene store fordeler overfor selskaper som er utviklet i mindre økonomier. Kinesiske selskaper som Alibaba, Tencent og Baidu kan samle inn data, trene algoritmer og til-

[37] Merk likevel at kunstig intelligens antakelig først blir brukt for analyse, deretter beslutningsstøtte og til slutt, dersom systemene oppnår nok tillit, til å ta beslutninger (Bentstuen 2022). På kort sikt vurderer vi derfor at KI-modeller primært benyttes til analyse og beslutningsstøtte, men på lengre sikt kan beslutningstaking utgjøre en større andel av aktivitetene KI-modeller blir brukt til.

passe teknologien med mange hundre millioner potensielle kunder før de eventuelt internasjonaliseres. Når landet samtidig hindrer vestlige selskapers tilgang til det enorme kinesiske markedet, får disse selskapene en fordel i den internasjonale konkurransen.

Også vestlige bedrifter som tilbyr andre typer produkter og tjenester (som ikke nødvendigvis er karakterisert av nettverkseffekter), vil være avhengige av å etablere seg i land som Kina, India og Brasil, for å sikre tilgang til disse landenes store forbrukermarkeder. Det gir disse landene makt til å definere spillereglene for vestlige selskapers etablering i markedene deres. I den forbindelse kan det være nødvendig for selskaper å samarbeide med lokale aktører, både for å få tilgang til markedene av myndighetene og for å kunne hevde seg i konkurransen med andre aktører. Det har spesielt vært oppmerksomhet rundt krav stilt av kinesiske myndigheter for at utenlandske virksomheter skal få tilgang til det kinesiske markedet, slik som å oppgi bedriftshemmeligheter, immaterielle rettigheter og/eller inngå i fellesforetak (*joint venture*) med kinesiske selskaper (O'Connor 2019). I intervjuene har det også blitt påpekt hvordan spesielt kinesiske selskaper lettere har markedstilgang i sine store, innenlandske markeder, og at det kan være en måte disse selskapene blir ledende på innen ulike produkter og tjenester globalt.

Det er samtidig viktig å være klar over at den teknologiske utviklingen kan ha negativ påvirkning på fremtidsutsiktene til fremvoksende økonomier. Sachs (2019) argumenterer for at mulighetene for å kopiere de østasiatiske vekstmiraklene – der økonomiene startet med arbeidsintensive industrier for deretter å utvikle mer kunnskapsintensive industrier – kan være i ferd med å lukkes med automatisering (se også delkapittel 3.6). Det vil i så fall ha konsekvenser både for lavinntektsland og for fremvoksende økonomier som Kina og India, der deler av befolkningen fortsatt er ansatte i lavt betalte, arbeidsintensive næringer. Korinek og Stiglitz (2021) deler også denne bekymringen for mindre utviklede land, men mener at Kina allerede har gjennomgått «tilstrekkelig dyp økonomisk transformasjon» og faktisk kan bli en av den kunstige intelligensrevolusjonens vinnere.

Store fremvoksende økonomier, spesielt Kina og India, vil altså kunne bygge opp store internasjonale bedrifter med nettverkseffekter og være viktige forbrukermarkeder for vestlige selskaper i årene fremover (se også Lindgren, Hemnes og Waage 2022). Deres økonomiske fremtid vil imidlertid kunne bli forstyrret ved at den teknologiske utviklingen reduserer mulighetene for å utnytte deres komparative fortrinn innenfor arbeidsintensive industrier.

3.8 Oppsummering av kapittelet

I dette kapittelet har vi undersøkt og besvart problemstilling 1 – hvordan påvirker den teknologiske utviklingen i 4IR økonomisk aktivitet på måter som former mulighetsrommet for økonomisk statshåndverk? – ved å samle innsikt fra respondenter og litteratur. Vi har pekt ut noen trender som vi argumenterer er av relevans for å forstå implikasjonene av den teknologiske utviklingen på staters bruk av økonomisk statshåndverk.

Nye teknologier både øker betydningen av data for (videre)utvikling av produkter og tjenester, gjør data mer tilgjengelig og bidrar til at data samles inn «overalt». Som følge av at data blir

viktigere, blir også tilgang og eierskap til data viktigere. Det kan blant annet resultere i at investeringer og oppkjøp av selskaper med god tilgang til data blir en stadig mer aktuell måte å sikre seg kontroll over dataene selskapene besitter.

Den teknologiske utviklingen bringer med seg økt kompleksitet. Det er flere grunner til dette. For det første blir systemer i seg selv mer komplekse, og drift og vedlikehold kan basere seg på automatiserte algoritmer, som er krevende å etterprøve. For det andre blir produkter og tjenester også i økende grad sammenkoblet, og det blir vanskelig å få oversikt over avhengigheter og verdiskapning. For det tredje kjennetegnes produkter og systemer i økende grad av at de ikke er ferdigprodusert når de blir solgt, men heller oppdateres kontinuerlig gjennom levetiden. For det fjerde øker kompleksiteten i verdikjeder, blant annet fordi leverandører og brukere befinner seg i ulike geografiske områder, leverandører byttes ut hyppig og kunstig intelligens blir tatt i bruk for å håndtere det store antallet underleverandører. Vi noterer oss imidlertid at selv om kompleksiteten ved ny teknologi kan bidra til at mottakerstater blir mer sårbare overfor økonomisk statshåndverk, kan også økonomisk statshåndverk bli vanskeligere å utføre for avsenderstater på grunn av den økte kompleksiteten.

Nye teknologier er kunnskapskrevende, og det vil bli økt etterspørsel etter talenter og arbeidstakere med kompetanse som gjør det mulig å anskaffe, utvikle, drifte og vedlikeholde produkter, tjenester og systemer som bygger på avanserte teknologier. Høy konkurranse om, og knapphet på, denne typen kompetanse fører til at stadig flere selskaper velger å sette ut utvalgte tjenester til andre selskaper som besitter nødvendig kunnskap og kompetanse på området. I likhet med behovet for tilgang til data, kan tilgang til kompetanse også motivere investeringer og oppkjøp.

Den teknologiske utviklingen bidrar til økt markedskonsentrasjon, ved at de produktive bedriftene fremmes, globalisering og lavere letekostnader fører til økt konkurranse, og mange nye næringer karakteriseres av nettverkseffekter og skjevfordeling av produktivitet innad i markeder. Eksisterende bedrifter med evne til å lagre og benytte massive data, stort skalautbytte, sterke nettverkseffekter og viktige immaterielle verdier kan oppnå store fordeler og hindre nye selskaper fra å etablere seg i markedet.

Den teknologiske utviklingen kan også påvirke organisasjonsformer i næringslivet og det offentlige. Plattformtjenester og lavere letekostnader bidrar til å forbedre informasjonsflyten i organisasjoner, som igjen kan resultere enten i økt sentralisering eller desentralisering. Graden av sentralisering kan igjen påvirke staters evne til å benytte økonomisk statshåndverk, som fordrer kontroll over kommersielle aktører. Lavere lete- og transaksjonskostnader gjør det videre enklere å internasjonalisere mange arbeidsoppgaver som bedrifter tidligere utførte lokalt.

Den teknologiske utviklingen øker graden av automatisering i utføring av arbeidsoppgaver og beslutningstaking. Dette har potensielt store implikasjoner for fremtidens arbeidsliv. I tillegg til å endre hvilke jobber – og kompetanse – menneskelig ansatte kommer til å inneha i fremtiden, blir både offentlige og private virksomheter samt enkeltindivider i økende grad avhengig av maskiner i hverdagen. Denne utviklingstrenden bidrar også til at det skapes og lagres enda mer digital informasjon og data enn hva som tidligere var tilfellet.

Den økonomiske og demografiske utviklingen globalt, kombinert med det økende behovet for tilgang til data og nettverkseffekter ved ny teknologi, kan også medføre at markedstilgang i fremvoksende økonomier blir stadig viktigere for selskapers evne til å utvikle de beste produktene og tjenestene samt hevde seg i internasjonal konkurranse. Det styrker makten til store økonomier som Kina og India. Samtidig kan den teknologiske utviklingen med økt automatisering redusere mulighetene for slike mindre utviklede, befolkningsrike økonomier å kapitalisere på tilgang til en stor og rimelig arbeidsstokk.

4 Hva er konsekvensene for økonomisk statshåndverk?

I dette kapittelet besvarer vi problemstilling 2 om hvordan den teknologiske utviklingen kan endre mulighetsrommet for staters bruk av økonomisk statshåndverk. Vi gjør dette ved å ta for oss hver handlingsmåte i typologien for økonomisk statshåndverk (tabell 1.1) i tur, delt inn etter dimensjonen som skiller på om makt blir utøvd (delkapittel 4.1) eller akkumulert (delkapittel 4.2) ved bruk av handlingsmåtene med oppsummering i delkapittel 4.3. Vi presiserer at både oppdragets omfang, teknologiutviklingens uforutsigbarhet og manglende eksisterende forskning på tematikken innen økonomisk statshåndverkslitteratur gjør det krevende å fastslå konsekvenser. Derfor bør ideene presentert i dette kapittelet bli betraktet som hypoteser i stedet for konklusjoner.

4.1 Utøve makt

Hvordan økonomiske virkemidler kan bli tatt i bruk for å utøve makt og innflytelse, er viet stor oppmerksomhet innen både den tradisjonelle litteraturen og nyere litteratur om økonomisk statshåndverk. Innen dimensjonen utøvelse av makt, består rammeverket presentert i delkapittel 1.3 av fire handlingsmåter: manipulere tilgang til salg til innenlandsk marked, manipulere tilførselen av ressurser, sabotere infrastruktur og manipulere tilgang til nettverksstrømmer. I det følgende drøfter vi hvordan den teknologiske utviklingen potensielt kan påvirke hvordan hver av handlingsmåtene kan tas i bruk som del av staters økonomiske statshåndverk.

4.1.1 Manipulere tilgang til salg til innenlandsk marked

Bruken av økonomiske virkemidler for å manipulere utenlandske selskaper sin tilgang til å selge varer og tjenester til avsenderlandets innenlandske marked kan være en potent handlingsmåte for å utøve makt, dersom de innenlandske markedene er viktige for mottakerlandets industrier og selskaper. Fra datasettene over hvordan Russland og Kina potensielt har tatt i bruk økonomiske virkemidler, finner vi at virkemidlene som går mest igjen innen denne handlingsmåten er ulike former for importrestriksjoner i tillegg til restriksjoner i turisme til mottakerlandet (Udal mfl. 2022; Waage mfl. 2022).

Når det gjelder implikasjoner av den teknologiske utviklingen, vurderer vi at virkemidlene som en avsenderstat har til rådighet, fremstår å være de samme som tidligere (importrestriksjoner, turismerestriksjoner, og lignende). Vi vurderer med andre ord at de tilgjengelige virkemidlene til å utøve makt ved denne handlingsmåten ikke endrer seg som følge av den teknologiske utviklingen. Likevel noterer vi oss noen forhold som kan være av relevans, og som potensielt kan resultere i at (enkelte) stater får økte muligheter til å utnytte handlingsmåten.

Kunstig intelligens og stordata kan potensielt benyttes som verktøy for å utforme mer effektiv bruk av økonomiske virkemidler. For eksempel eksisterer det store, åpne datasett over handelsstrømmer mellom land. I tillegg besitter mange lands myndigheter store og detaljerte datasett over innenriksforhold så vel som økonomiske relasjoner med andre land. Disse dataene, i kombinasjon med kraftige dataprosesserings- og analyseverktøy (inkludert KI), kan potensielt utnyttes av avsenderstaten til å forsøke å identifisere hvilke områder som vil påføre mottakerlandet størst kostnad, til lavest mulig kostnad for avsenderlandet.

Utover mulighetene for mer effektiv virkemiddelbruk ved støtte av kunstig intelligens og stordata, vil fremvoksende markeder, med store innenlandske befolkninger, kunne få økte muligheter til å utnytte utenlandske selskapers behov for markedstilgang, slik vi drøftet i delkapittel 3.7. Produkter og tjenester med nettverkseffekter blir mer sentrale med fremveksten av ny teknologi samt at betydningen av data for å utvikle og forbedre produkter og tjenester øker. Det blir følgelig viktigere enn tidligere å få innpass i disse markedene på grunn av befolkningens størrelse og kjøpekraft. Det øker makten til å manipulere tilgang til salg til innenlandsk marked.

Fremvoksende markeders økonomiske fremtid ser også lysere ut enn de mer modne økonomiene i Vest-Europa og Nord-Amerika. Grunnen er at det er enklere å lære eksisterende kunnskap og teknologi, enn å måtte forske og utvikle ny kunnskap og teknologi. Lav- og mellominntektslands andel av verdens BNP er derfor forventet å øke fremover. En større økonomi og bedre kjøpekraft i egen befolkning, styrker fremvoksende økonomiers evne til å utnytte denne handlingsmåten. Derimot taler argumenter om at arbeidsintensiv industri vil bli rammet hardere av ny teknologi enn kunnskapsintensiv industri for at fremvoksende markeders viktighet reduseres. Disse antakelsene bør undersøkes nærmere enn hva som har vært mulig innenfor rammene av denne studien.

Samlet vurderer vi at den teknologiske utviklingen potensielt kan styrke enkelte staters muligheter til å utøve makt gjennom å benytte økonomiske virkemidler til å manipulere tilgangen til salg til sine innenlandske markeder. Det er imidlertid behov for mer forskning omkring konsekvensene av den teknologiske utviklingen for fremvoksende markeders økonomiske fremtid.

4.1.2 Manipulere tilførselen av ressurser

En annen handlingsmåte for utøvelse av makt, er å manipulere mottakerlandets tilførsel av ressurser. De fleste økonomier er avhengige av flere typer ressurser utenfra, inkludert råvarer, halvfabrikata, komponenter, ferdigvarer, kapital, teknologi, immaterielle rettigheter, arbeidskraft og kompetanse. Muligheten til å (gi løfter om å) øke tilførselen av ressurser eller (true med å) redusere tilførselen av ressurser, for eksempel ved eksportrestriksjoner, åpner opp for maktbruk.

Vi vurderer at den teknologiske utviklingen kan bidra til å styrke staters muligheter til å utnytte mottakerlandets avhengighet til ressurser for å utøve makt.

Fra intervjuene og workshopen påpeker flere respondenter hvordan særlig avhengighet av kompetanse (kompetanseverdikjeder) kan åpne nye muligheter for stater til å utøve makt. Nye, avanserte teknologier stiller (betydelig) høyere krav til kompetanse enn gamle teknologier, og man forventer fortsatt (og økende) mangel på arbeidskraft som kan møte disse kompetansekravene (se delkapittel 3.3). Utfordringer med å sikre tilstrekkelig intern kompetanse til drift, vedlikehold, forvaltning og videreutvikling av løsninger som utnytter avanserte teknologier slik som kunstig intelligens og skytjenester, vil trolig medføre at selskaper i økende grad velger å sette ut slike oppgaver til eksterne leverandører nasjonalt og internasjonalt. Avhengigheter til ekstern kompetanse kan åpne muligheter for utøvelse av makt. For eksempel påpeker respondenter i intervjuene hvordan selskaper i avsenderlandet kan gi beskjed om at vedlikeholdstjenester, av ulike årsaker, ikke kan bli utført før om seks måneder. Denne formen for maktutøvelse kan foregå fordekt og være vanskelig å attribuere til en avsenderstat, siden det tilsynelatende er organisatoriske forhold hos en leverandør som forårsaker forstyrrelsene.

I tillegg til kompetanse er det flere andre typer ressursavhengigheter som skapes av den teknologiske utviklingen, og som potensielt kan åpne for å utøve makt ved å manipulere mottakerlandets tilgang til disse ressursene. Noen eksempler kan være reservedeler, komponenter, programvareoppdateringer (for både funksjonalitet og sikkerhet) og vedlikeholdstjenester som befinner seg hos selskaper i avsenderlandet. Ved at det blir forsinkelser eller andre forstyrrelser i tilgangen til slike ressurser, kan systemer i mottakerlandet slutte å fungere. Dette er også en måte hvor aktører i en verdikjede potensielt kan utnyttes av avsenderstaten til å presse eller svekke mottakerstaten fordekt. Selv om det kan finnes andre leverandører av ulike produkter og tjenester som kan gjøre det mulig å bytte leverandør på lengre sikt, kan det være tidkrevende og kostbart slik at man på kort sikt i praksis er låst til én leverandør – av Voldhaug mfl. (2021: 45) omtalt som risikoen ved «*vendor lock-in*».

Videre ser vi allerede tendenser til økt knapphet på innsatsfaktorer og komponenter som inngår i avanserte teknologiske produkter og løsninger, slik som halvledere og sjeldne jordarter[38] (*rare earth elements* – REE). Knapphet globalt på slike ressurser kan bidra til at det er mer krevende å finne substitutter (på kort sikt) dersom leveranser av innsatsfaktorene bortfaller. Det kan både ha konsekvenser for landet som produserer produkter som trenger innsatsfaktorene, og tredjeland (eller allierte) som er avhengig av å kjøpe produktene fra produsentlandet. Dersom avsenderstaten klarer å utøve kontroll over selskaper i eget eller andre land, som er viktige produsenter og leverandører av innsatsfaktorene, kan det følgelig gi styrkede muligheter for maktutøvelse i takt med at den teknologiske utviklingen øker etterspørselen etter innsatsfaktorene. Dersom enkelte aktører oppnår en dominerende posisjon innen forsyningen av REE, kan det dessuten være aktuelt å analysere mulighetene for en avsenderstat til å utøve makt gjennom handlingsmåten *manipulere tilgang til nettverksstrømmer* (se seksjon 4.1.4).

[38] REE består av de 15 lantanoidene i periodesystemet samt metallene scandium og yttrium (Fjellvåg 2022).

Samtidig viser Kinas tilsynelatende utnyttelse av Japans avhengighet av REE hvordan de langsiktige effektene av å forstyrre forsyningen av viktige eller kritiske innsatsfaktorer kan være negative for avsenderstaten. I dette tilfellet diversifiserte Japan og andre (vestlige) land sin forsyning av REE, inkludert ved å skape insentiver for produksjon i vestlige land, da det ble tydelig hvordan Kina kunne utnytte sin dominerende markedsandel[39] til å utøve makt (Nye 2020; Wilson 2018). I den grad det er mulig å utnytte andre lands avhengigheter til kompetanse og andre ressurser, kan det være at disse mulighetene, som eksisterer i dag eller som vil bli etablert i fremtiden, er midlertidige. Det kan i så fall tale for at slike virkemidler vil bli tatt i bruk kun i en internasjonal konflikt som er alvorlig nok til at avsenderstaten aksepterer de potensielt langsiktige negative konsekvensene.

Samlet vurderer vi at den teknologiske utviklingen kan styrke enkelte staters muligheter til å utøve makt ved å manipulere tilførselen av ressurser, fordi både kompetanse og innsatsfaktorer kan bli viktigere og mer knappe i tillegg til at enkeltselskaper kan sitte på reservedeler, komponenter, programvareoppdateringer, vedlikeholdstjenester og lignende som systemer avhenger av for å fungere. Som for handlingsmåten *manipulere tilgang til salg til innenlandsk marked*, kan dessuten avsenderstatens bruk av kunstig intelligens og stordata (handelsdata m.m.) potensielt bidra til å identifisere hvilke økonomiske virkemidler som har størst potensial til å påføre mottakerlandet en kostnad, til lavest mulig kostnad for avsenderlandet.

4.1.3 Sabotere infrastruktur gjennom eierskapskontroll

Handlingsmåten *sabotere infrastruktur* inkluderer sabotasje muliggjort av eierskapskontroll over infrastruktur eller underleverandører, slik som forstyrrelser eller endringer i driften av selskaper som infrastrukturer avhenger av. Det kan også være forsøk på å svekke selskaper utført ved (å true med) å trekke ut investeringer (Drezner 2008). Til sammenligning dekker handlingsmåten *tilrettelegge for (skjult) sabotasje* (seksjon 4.2.5) forsøk på å utnytte økonomiske virkemidler til å komme i posisjon til å kunne utføre sabotasje i fremtiden, også med andre virkemidler enn økonomiske virkemidler (for eksempel cyberrelaterte virkemidler).

Fra forskningen utført ved FFI finner vi flere forklaringer til hvorfor sårbarheten for sabotasje generelt kan øke i takt med den teknologiske utviklingen. Vi begrenser vi oss derfor til å trekke frem noen eksempler i denne rapporten. Særlig gir Farsund mfl. (2022) en rekke eksempler på utfordringer for nasjonal sikkerhet med økt bruk av IoT-systemer. De påpeker hvordan sammenkoblede IoT-systemer – ofte kombinert med skytjenester og kunstig intelligens – «gir mange angrepspunkter, hvor mange kan nås fra internett, og da også i praksis fra hele verden» (Farsund mfl. 2022: 42). Videre er det ikke tilstrekkelig å sikre ett enkelt system, så lenge dette systemet har avhengigheter til andre systemer som ikke er like sikre – eller at sammenkoblingene i seg selv ikke er sikre. Dessuten kan konsekvensene i den fysiske verden av eventuelle angrep øke, som følge av at aktuatorer blir koblet til systemene. Samlet øker dette faren «for sabotasjehandlinger mot virksomheter, kritiske infrastrukturer, viktige samfunnsfunksjoner og Forsvaret» (Farsund mfl. 2022: 43).

[39] På den tiden (dvs. 2010) sto Kina for rundt 90 prosent av forsyningen globalt.

Fokuset i denne rapporten er ikke hvilke sabotasjemuligheter som generelt kan oppstå fra ny teknologi, men hvordan økonomiske virkemidler kan inngå i sabotasjeforsøk. Som det fiktive scenarioet om tjenesteutsetting av kritisk infrastruktur presentert av Farsund mfl. (2022) – og gjengitt i boks 4.1 – viser, kan økonomiske transaksjoner spille en viktig rolle i å øke sårbarheter for sabotasje.

Boks 4.1 – Scenario om tjenesteutsetting av kritisk infrastruktur.

Det følgende fiktive scenarioet om tjenesteutsetting av kritisk infrastruktur er presentert i Farsund mfl. (2022: 35–36) og har tidligere blitt brukt ved FFI. Som scenarioet viser, kan økonomisk aktivitet, sammen med høy kompleksitet, spille en viktig rolle i å øke sårbarheter for sabotasje (bortfall av tjenester).

«Scenarioet går ut på at et veiselskap i Norge legger ut anskaffelse og drift av ladeinfrastruktur for elektriske kjøretøyer i Østerdalen ut på anbud. Et tysk firma, AutoEl Gmbh, vinner anbudsrunden og blir kontraktør. De leverer avanserte ladere, og ett av de viktigste kriteriene ved valg av kontraktør var å minimere kostnadene.

AutoEl Gmbh er et selskap som er eid av flere aktører i Asia og Midtøsten, og det benytter mange aktører for å produsere tjenestene de leverer. Når det gjelder ekom har de kontrakter med seks internasjonale ekom-selskaper, mens skytjenester kjøper de av to ulike leverandører. Operasjon av ladestasjonene utføres av fem aktører fordelt over Ukraina, Bulgaria, India og Vietnam, mens den tekniske operasjonen av ladestasjonene foretas av lokale aktører i Østerdalen. Strømleveranser får de fra en latvisk bedrift med sammensatt eierskap, mens den fysiske strømleveransen kommer fra en lokal nettleverandør.

En slik infrastruktur vil ha høy kompleksitet. Når det gjelder samspillkompleksitet, vil denne infrastrukturen av ladestasjoner ha avhengigheter til mange datasentre, driftssentre, kommunikasjonsnoder og kommunikasjonsveier i form av kjernenett, spredd over hele verden. Det vil være deling av data med andre tjenester og infrastrukturer. Samspillkompleksiteten vil derfor være høy, og koblingene vil i stor grad være tette. Verdikompleksiteten vil være noe høy, fordi det vil være vanskelig å ha oversikt over hvilke verdikjeder disse elkjøretøyene, som bruker ladestasjonene, inngår i. Den organisatoriske kompleksiteten vil også være høy. En kan tenke seg at firmaet bygger ut nye ladestasjoner andre steder i verden, at selskaper blir kjøpt opp, og deler blir solgt ut. Infrastrukturen vil derfor også kunne inneha høy dynamisk kompleksitet.

Dette er som nevnt et fiktivt scenario, men vil ikke kunne være utenkelig slik virksomheter opererer i dag. Det er også å anta at ladeinfrastrukturer langs Norges hovedfartsveier vil være av betydning for nasjonal sikkerhet, siden bortfall av disse vil påvirke transportsektoren i alle fall på sikt.»

De økonomiske virkemidlene som gir eierskapskontroll vil fremdeles være de samme – investeringer, oppkjøp og potensielt også å benytte underleverandører som oppnår fysisk tilgang til infrastrukturer. Den teknologiske utviklingen kan imidlertid øke mulighetene for, og effekten av, å utnytte eierskap eller underleverandører til å utøve makt gjennom sabotasje av infrastruktur, både fordi stadig større deler av samfunnet avhenger av tjenester og fordi systemer i stadig større grad blir sammenkoblet. Videre øker mulighetene for å utføre sabotasje fra utlandet, hvor eierskap er utenfor mottakerstatens kontroll, mens det tidligere i større grad var nødvendig med tilgang i mottakerlandet for å kunne ramme dette landets infrastruktur.

I tillegg til investeringer i enkeltselskaper, påpeker Farsund mfl. (2022: 42) hvordan innsamling av data på tvers av enheter og selskaper om «personer, virksomheter, kritiske infrastrukturer, samfunnsfunksjoner samt Forsvaret» potensielt kan benyttes som utgangspunkt for å «utføre ulike angrep mot kritiske infrastrukturer og Forsvarets systemer». Når det gjelder underleverandører, kan fysisk tilgang (og eventuelt andre kontaktpunkter) til IoT-basert infrastruktur gi sabotasje-muligheter for eksempel gjennom å manipulere, eller besudle, data eller å kjøre egne kommandoer på systemene. Fysisk tilgang kan også åpne muligheter for å modifisere *firmware* og installere egne bakdører på systemet (Farsund mfl. 2022). For mer om potensielle sabotasjemuligheter i sammensatte systemer, henviser vi til Farsund mfl. (2022).

Samtidig blir sannsynligheten for sabotasjeforsøk generelt vurdert til å være lav av våre respondenter, blant annet fordi slike forsøk sannsynligvis vil ha betydelige negative konsekvenser for avsenderstaten og eventuelle involverte kommersielle aktører. Dersom den sikkerhetspolitiske situasjonen er alvorlig nok, kan det likevel være aktuelt for avsenderstaten å forsøke å utnytte muligheter for å utføre sabotasje av infrastruktur.

Samlet vurderer vi at mulighetene for å utføre sabotasje av infrastruktur vil øke med den teknologiske utviklingen, og at det er viktig å være bevisst på hvordan økonomiske transaksjoner spiller en sentral rolle i å skape sårbarheter som kan utnyttes samt hvordan flere økonomiske transaksjoner enn tidligere potensielt kan gi slike muligheter.

4.1.4 Manipulere tilgang til nettverksstrømmer

Manipulering av tilgang til nettverksstrømmer innebærer at en avsenderstat er i stand til å utnytte sin maktposisjon i regionale eller globale nettverk til å kontrollere andre lands tilgang til nett-verksstrømmene. Eksempler på slike nettverk inkluderer globale finansnettverk, internettplatt-former, kommunikasjonsteknologi, nettverk for deling av sensitiv teknologi eller utvikling av militære våpensystemer, samt energi- og transportnettverk (Drezner, Farrell og Newman 2021).

Litteraturen om teknologiutviklingens betydning for økonomisk statshåndverk drøfter hvordan den teknologiske utviklingen potensielt kan påvirke muligheten for å utøve makt i internasjonale finansnettverk. USA og andre vestlige land har særlig nytt godt av sin sentrale rolle i disse nett-verkene siden andre verdenskrig. I dag gir vestlig kontroll over det internasjonale betalings-systemet SWIFT muligheter til å utestenge andre land fra dette nettverket, slik det har blitt gjort mot Iran (2012) og Russland (2022). Den amerikanske dollaren (USD) sin dominerende posisjon som global valuta gir også makt og innflytelse til USA. Det er imidlertid allerede tegn til en

utvikling hvor Kina, i samarbeid med likesinnede land, søker å etablere alternative institusjoner og systemer, inkludert innen internasjonale betalingssystem og promotering av andre valutaer, spesielt kinesisk renminbi (RMB), til bruk i internasjonale transaksjoner (se f.eks. Roberts, Armijo og Katada 2017). Kina har også introdusert en digital valuta – e-CNY. Det kan styrke den kinesiske statens evne til å overvåke og kontrollere egne innbyggere, men også styrke Kinas internasjonale valutaposisjon (Duffie 2022). Slike initiativer kan bidra til å redusere vestlig/ amerikansk dominans i globale finansnettverk. Eksisterende litteratur forklarer også hvordan den teknologiske utviklingen kan svekke posisjonen til etablerte valutaer (særlig USD) og betalingssystemer (SWIFT) ytterligere. Det kommer i mindre grad av fremveksten av teknologiområdene omtalt i delkapittel 2.1, men knytter seg i stedet til den økende bruken av digitale valutaer. Vi inkluderer likevel noen hypoteser om hvilke endringer dette kan medføre.

Aggarwal og Marple (2020) diskuterer betydningen av fremveksten av digitale valutaer i et økonomisk statshåndverkperspektiv, hvor de også har fokus på trusler mot amerikansk nasjonal sikkerhet. Aggarwal og Marple (2020) fremhever hvordan digitale valutaer har sine egne nettverk for å prosessere transaksjoner og følgelig ikke blir prosessert gjennom SWIFT-nettverket. De mener at det kan svekke USA sine muligheter til å implementere finansielle sanksjoner. I tillegg fokuserer de på hvordan digitale valutaer kan komme til å spille en viktig rolle som reservevaluta, noe som kan true posisjonen til USD i det internasjonale finansielle systemet. Samtidig argumenterer Rosenberg mfl. (2019: 3) for at «det er usannsynlig at nye digitale betalingsteknologier eller kryptovaluta vil vise seg å være en meningsfull metode for å unngå amerikanske økonomiske tvangstiltak på kort sikt».

På den annen side kan den teknologiske utviklingen bidra til å styrke mulighetene for enkelte mektige stater til å utnytte maktposisjoner i globale eller internasjonale nettverk, også på kort sikt. For eksempel utforsker Tusikov (2021: 134–135) hvordan internettplattformer[40] kan åpne muligheter for å utøve makt ved å «kontrollere eller blokkere informasjonsstrømmer», inkludert å gjøre nettsider «kommersielt ikke-levedyktige, ved å essensielt stenge dem ute fra den globale økonomien». Hun påpeker at det primært er «domenet til mektige stater slik som USA og Kina, som kan presse deres innenlandske industrier» (Tusikov 2021: 134). Eksempler som trekkes frem på hvordan internettplattformer blir utnyttet til «kvelning» inkluderer USAs kampanje mot WikiLeaks etter sistnevntes publisering av et stort antall klassifiserte amerikanske diplomatiske dokumenter, og Kinas utestengelse av basketballteamet Houston Rockets – sammen med resten av National Basketball Association (NBA) – fra kinesiske TV- og internettplattformer etter at Houston Rockets' daglige leder uttrykte støtte for demokratiforkjemperne i Hong Kong. Når det gjelder Kina, påpeker Tusikov (2021) hvordan statsledelsen i dag primært har muligheter til å stenge aktører ute fra Kina, men det kan endre seg med utvidelsen av kinesiske plattformer til andre land.

Selv om bidraget til Tusikov (2021) setter fokus på internettplattformer, avslutter hun med å trekke inn skytjenester. I den forbindelsen fremhever hun hvordan det med «et økende antall kommersielle og offentlige tjenester som avhenger av skyen, inkludert utdanning, helsetjenester

[40] Plattformer blir forstått som «enheter, ofte fra privat sektor, som leverer viktige kommersielle og tekniske tjenester som muliggjør at internett fungerer effektivt, slik som betaling eller domenenavnsystem» (Tusikov 2021: 134).

og militærtjenester» kan få alvorlige konsekvenser dersom en stat er i stand til å forstyrre leveransene av disse tjenestene (Tusikov 2021: 143).

Tusikov (2021) fremhever også hvordan det er behov for å forstå bedre «kvelningspotensialet» knyttet til den fysiske infrastrukturen til internett, og trekker frem «eierskap og drift av kjerne-elementer i den globale internettinfrastrukturen» inkludert «fiberoptiske undervannskabler, autonome systemtall og internettutvekslingspunkter som utgjør internetts 'rørledninger' [('*pipes*')]» (Tusikov 2021: 143). Det skjer en utvikling hvor eierskap over disse elementene i økende grad flyttes fra USA mot særlig Europa, Brasil, Russland, India, Kina og Sør-Afrika (Tusikov 2021). Respondenter ved FFI uttrykker imidlertid skepsis til i hvilken grad eierskap til underliggende fysisk infrastruktur, og spesielt undersjøiske fiberkabler, i seg selv kan utnyttes som del av kvelningsstrategier rettet mot enkelte mottakerstater. Internett er veldig distribuert av natur, og store selskaper som Google, Facebook og Microsoft har tilstedeværelse i mange land og kontinenter. Det er i tillegg et stort antall fiberkabler over for eksempel Atlanterhavet. Kontroll på én enkelt fiberstrekning vil gi få muligheter til å kvele trafikken til enkeltland, med det unntaket at det fortsatt er noen små land, særlig i Stillehavet, som har kun én eller to fiberkabler tilgjengelig.

Til sist stiller Tusikov (2021: 144) spørsmålet om hvordan Kina kan utnytte kvelning i nettverk til «å oppnå teknologisk dominans i områder av strategisk betydning for seg selv og USA, spesielt innen robotikk, autonome kjøretøy, og kunstig intelligens», men uten å gå nærmere inn på konkrete eksempler knyttet opp til spørsmålet. Segal (2021) presenterer imidlertid en rekke eksempler på hvordan USA har utnyttet sine gunstige nettverksposisjoner, inkludert innen produksjon og transport av halvledere, til å forsøke å svekke det kinesiske selskapet Huawei ved å stenge det ute av nettverkene. 5G er også et eksempel på et nettverk hvor særlig amerikanske myndighetspersoner og etterretningsmiljøer har fremhevet hvordan det er potensielle kvelnings-muligheter til stede (Segal 2021), for eksempel dersom tjenestene blir forstyrret slik at viktige samfunnsfunksjoner blir slått ut.

Bodamer og Schilde (2021) setter også fokus på hvordan stater kan manipulere andre lands tilgang til teknologi. De forklarer hvordan både det amerikanske F-35-nettverket og det europeiske Eurofighter-nettverket kan forstås som nettverk hvor enkelte stater kan utøve kontroll over hvem som får tilgang til «teknologistrømmene» i nettverkene. Bodamer og Schilde (2021) gir eksempler på hvordan USA og Tyskland stengte ute henholdsvis Tyrkia (F-35) og Saudi-Arabia (Eurofighter) fra nettverkene.[41] I sistnevnte tilfelle rammet Tysklands beslutning om å stenge ute Saudi-Arabia også andre europeiske land som forhandlet om salg av våpensystemer til Saudi-Arabia, slik som BAE i Storbritannia, på grunn av Tysklands sentrale rolle i europeisk våpenproduksjon. Slike «teknologinettverk» kan, i tillegg til våpensystemer, også inkludere flerbruksteknologi. I den forbindelse drøfter Mastanduno (2021) hvordan USA under den kalde krigen var et sentralt knute-punkt i nettverket av sivil og militær teknologi med flerbrukspotensial, som søkte å stenge Sovjet-unionen ute av nettverket, og hvordan en lignende utestengelse i dag er relevant med hensyn til Kina. Videre kan global kontroll over viktige eller kritiske råvarer (som REE) og komponenter som inngår i produksjonen av avanserte teknologiske systemer gi muligheter til å utestenge

[41] Bodamer og Schilde (2021) påpeker imidlertid at det er usikkert hvilken rolle den tyske staten spilte i utestengelsen, eller om den skjedde som et resultat av offentlig press mot den tyske våpenindustrien.

enkelte land fra forsyningen, og følgelig potensielt hemme evnen til å opprettholde og videreutvikle egen teknologi (se også seksjon 4.1.2).

Samlet vurderer vi at den teknologiske utviklingen har potensial til både å styrke og svekke staters muligheter til å utøve makt gjennom å manipulere tilgangen til nettverksstrømmer, avhengig av typen nettverk. På kort sikt fremstår det som mulighetene primært blir styrket, men for internasjonale finansnettverk kan mulighetene bli svekket over tid dersom digitale valutaer i økende grad blir tatt i bruk i internasjonale transaksjoner som alternativ til betalingstjenester som SWIFT.[42] Den teknologiske utviklingen kan også øke viktigheten av ekskluderende «teknologinettverk» mellom likesinnede stater, som kan medføre at teknologi, kunnskap og ekspertise ikke flyter like fritt globalt som har vært tilfelle siden den kalde krigens slutt – i tillegg til at tilgang eller utestengelse av nettverk kan brukes både som et maktmiddel og for å svekke den teknologiske utviklingen til geopolitiske konkurrenter.

4.2 Akkumulere makt

Økonomiske virkemidler kan bli brukt ikke bare til å utøve makt, men også til å legge til rette for fremtidig økonomisk – eller annen – maktbruk. Det er slik bruk av økonomiske virkemidler vi omtaler som akkumulering av makt. Innen maktdimensjonen akkumulering av makt, består rammeverket presentert i delkapittel 1.3 av totalt syv handlingsmåter: forme (sær)interesser og oppfatninger i mottakerlandet, øke avhengigheten til ressurser og innenlandsk marked, etterretningsvirksomhet (gjennom økonomisk aktivitet), styrke materielle/militære kapabiliteter, tilrettelegge for fremtidig sabotasje, panoptikon og øke avhengigheten til knutepunkt. I det følgende drøfter vi hvordan den teknologiske utviklingen potensielt kan påvirke hvordan hver av handlingsmåtene kan tas i bruk som del av staters økonomiske statshåndverk.

4.2.1 Forme (sær)interesser og oppfatninger i mottakerlandet

Økonomisk statshåndverk kan brukes for å forsøke å påvirke hvordan statsledelsen, elitene og befolkningen i mottakerlandet oppfatter avsenderstaten og hvordan de responderer på dens initiativ i internasjonal politikk. Innen den tradisjonelle litteraturen av økonomisk statshåndverk, samt nyere studier som særlig fokuserer på Kinas bruk av økonomiske virkemidler, er det fokus på hvordan positive økonomiske insitamenter som investeringer, lån og økninger i handel kan bli forsøkt brukt til å forme (sær)interesser og oppfatninger. Flere peker på hvordan avsenderstaten kan forsøke å skape interessegrupper i mottakerlandet som i neste omgang har mulighet til å påvirke landets politikk og beslutningstaking (se f.eks. Hasegawa 2018; Kastner og Pearson 2021; Keng, Tseng og Yu 2017; Wei 2013; Wong og Wu 2016).

For å forstå implikasjoner av den teknologiske utviklingen på staters muligheter til å forme (sær)interesser og oppfatninger i et mottakerland, vurderer vi at det er relevant å trekke inn perspektiver fra litteratur om påvirkning, inkludert propaganda og spredning av (des)informasjon. Waage mfl. (2022) drøfter hvordan økonomiske virkemidler som investeringer og lån i mediehus kan være en

[42] Det kan potensielt også redusere muligheten til å utnytte internettplattformer ved å avstenge dem fra betalingstjenester.

metode Kina potensielt kan ha benytte for å forsøke å påvirke det offentlige ordskiftet i et mottakerland, for eksempel i Tsjekkia (se også Karásková mfl. 2018; Karásková 2019). Den teknologiske utviklingen kan åpne nye muligheter – utover investeringer i medieselskaper – for å påvirke det offentlige ordskiftet og oppfatninger hos interessegrupper eller befolkningen som helhet. Forskning både internasjonalt og ved FFI drøfter godt og grundig hvordan dette kan foregå. For eksempel kan stordata og kunstig intelligens utnyttes for å kunne «skreddersy nyhetsmeldinger til ulike befolkningsgrupper for å endre opinionen i samfunnet» (Bentstuen mfl. 2018: 21).[43] De seneste årene, og spesielt etter presidentvalget i USA i 2016, har det også vært økende oppmerksomhet rundt hvordan folks digitale fotavtrykk kan åpne muligheter for å utnytte «psykologisk målretting» (*psychological targeting*) til å gjennomføre storskala påvirkningskampanjer for å påvirke holdninger, følelser og oppførsel (Matz, Appel og Kosinski 2020). KI-modeller kan dessuten utnyttes til å generere sammenhengende og meningsfull – men også falsk – tekst så vel som «*deepfakes*», altså KI-genererte falske bilder og videoer (Sellevåg mfl. 2020). Sivertsen mfl. (2021) går ytterligere i detalj på ulike påvirkningsmetoder som kan være relevante å se i sammenheng med bruken av økonomiske virkemidler, inkludert falske responser[44], falsk informasjon[45] (f.eks. falske nyheter) og pseudonymitet[46].

Vi nøyer oss med å henvise til disse eksemplene og å understreke at det finnes relevant forskning ved FFI og internasjonalt om hvordan påvirkning kan foregå. I stedet søker vi, i denne rapporten, å fremheve hvordan økonomisk aktivitet kan være en måte å komme i posisjon til i neste omgang å kunne påvirke (sær)interesser og oppfatninger i mottakerlandet. Det kan foregå gjennom investeringer og lån til aktører med mulighet til å utøve innflytelse i mottakerlandet, på samme måte som investeringer i tradisjonelle mediehus for å forsøke å påvirke hvordan ulike nyhetssaker omtales. Som følge av den teknologiske utviklingen, vurderer vi imidlertid at mengden av potensielle inngangsportaler for å nå frem til ulike interesse- og befolkningsgrupper øker, i tillegg til at det kan bli lettere å gjøre det fra lokasjoner i utlandet. Som Farsund mfl. (2022: 42) påpeker, kan dessuten de store datamengdene, som blir tilgjengeliggjort og understøttet av nye teknologier som 5G, skytjenester og tingenes internett, «brukes som utgangspunkt ved ulike påvirkningsoperasjoner».[47] Det betyr at investeringer og oppkjøp i selskaper som muliggjør datainnsamling, også kan legge til rette for påvirkningsoperasjoner.

[43] I den forbindelse er det verdt å huske på at «kompleksiteten gjør det … vanskeligere å ha kontroll med hvilken informasjon vi gir fra oss» (Bentstuen mfl. 2018: 21).

[44] Som Sivertsen mfl. (2021: 25–26) forklarer, kan man overordnet si at «falske responser enten promoterer informasjon og synspunkter som gagner påvirker eller sverter informasjon og synspunkter som strider mot påvirkers mål».

[45] Som Sivertsen mfl. (2021: 26) forklarer, er kjernen i påvirkning «informasjon som på forskjellige måter fordreier eller ignorerer fakta, for å promotere noe som gagner den som står bak påvirkningen. Et viktig element er at den falske informasjonen 'pakkes inn' i formater som fremstår som troverdig».

[46] Som Sivertsen mfl. (2021: 25) forklarer, dreier dette seg om «å skjule hvem som egentlig står bak innlegg, narrativ og budskap. Anonymitet er en variant av pseudonymitet, men det er mer formålstjenlig for påvirkning om personen/gruppen som en profil referer fremstår som a) ekte og b) med innsikt som er troverdig, gjerne med spesiell innsikt». Et eksempel er astroturfing, som går ut på «å skjule den egentlige aktøren bak et budskap eller organisasjon slik at engasjementet ser ut til å komme fra, eller være støttet av, grasrotbevegelser».

[47] For eksempel kan kunstig intelligens benyttes for å filtrere og personalisere informasjon basert på analyser av trender og mønstre (Waage 2022; se også Daugherty og Wilson 2018; Wirtz, Weyerer og Geyer 2019). Slike systemer er for eksempel utbredt innen e-handel, strømmetjenester og sosiale medier.

Mens vi tror at virkemidlene stater har til rådighet i stort vil være de samme – spesielt investeringer og lån – vurderer vi oppsummert at denne handlingsmåten av økonomisk statshåndverk kommer til å bli mer potent med den teknologiske utviklingen. Og selv om virkemidlene er de samme, kan datainnsamling og kraftige analyseverktøy (særlig KI) potensielt bidra til å spisse innrettingen av dem, slik at de mest effektivt påvirker viktige særinteresser, lokalsamfunn og lignende på måter som gagner avsenderstaten.

4.2.2 Øke avhengigheten til ressurser eller innenlandsk marked

Denne handlingsmåten omhandler økonomiske transaksjoner som kan bidra til å øke mottakerlandets avhengighet til ressurser, inkludert kompetanse. Handlingsmåten inkluderer også bruken av økonomiske virkemidler på måter som øker mottakerlandets selskaper sin avhengighet til å selge produkter og tjenester til avsenderlandets markeder, slik som for eksempel inngåelsen av en bilateral handelsavtale. For at en avsenderstat skal være i stand til å benytte seg av denne handlingsmåten, må den besitte kontroll over ressurser som er viktige for mottakerlandet, eller ha forbrukermarkeder som er attraktive – eventuelt nødvendige – for mottakerlandets selskaper å være til stede i. Avhengigheter kan i neste omgang potensielt utnyttes i et forsøk på å utøve makt over mottakerstaten, som forklart i seksjon 4.1.1 (markedstilgang) og seksjon 4.1.2 (ressurser).

I vurderingen av hvordan den teknologiske utviklingen påvirker slike staters muligheter til å benytte handlingsmåten, noterer vi oss at markedskonsentrasjonen øker i flere markeder som følge av ny teknologi (se delkapittel 3.4). Det kan øke mulighetene for å etablere eller styrke avhengigheter, da tilgangen på substitutter globalt blir redusert og/eller det er høy terskel for å bytte systemer («*vendor lock-in*»). Dersom konsentrasjonen blir så høy at det kun er én eller et fåtall tilbydere globalt, som typisk er tilfellet for leverandører innen flere av teknologiområdene beskrevet i delkapittel 2.1, er det relevant å studere mulighetene dette gir for å ta i bruk økonomisk statshåndverk langs nettverksdimensjonen. Vi utdyper derfor om dette i seksjon 4.2.7.

Mer generelt vil det være slik at den teknologiske utviklingen skaper nye avhengigheter mellom land i fremtiden på grunn av behovet for ulike typer ressurser – f.eks. råvarer, halvfabrikata, komponenter, ferdigvarer, kapital, tjenester, teknologi, immaterielle rettigheter, arbeidskraft og kompetanse. Som ved maktbruken knyttet til struping av ressurser (se seksjon 4.1.2) vil en stat kunne akkumulere makt ved å gjøre andre land avhengige (på kort eller også lang sikt) av dens ressurser. Den teknologiske utviklingen bidrar til at innsatsfaktorer og komponenter som halvledere og råvarer, som litium, nikkel og kobolt, blir mer nødvendige. Produkter, tjenester og kompetanse knyttet til fremvoksende teknologier, som 5G, kunstig intelligens og tingenes internett, vil også kunne bidra til maktakkumulering for land som besitter dominerende posisjoner i form av produksjon eller kunnskap. I noe som minner det «nye» økonomiske statshåndverket (se seksjon 2.2.2), argumenterer Beckley (2022) for eksempel for at Kina har «massivt subsidiert strategiske industrier for å skaffe monopol innenfor hundrevis av vitale produkter» som en del av et økonomisk offensiv (*economic offensive*).

En av respondentene påpeker dessuten hvordan det grønne skiftet vil legge press på flere knappe innsatsfaktorer, som for eksempel er viktig i batteriproduksjon. I den forbindelse blir det fremhevet at Kina er en aktør som satser stort på grønn energi (se f.eks. også Chiu 2017; Lewis 2012),

som solenergi. Det kan medføre at Norge og andre land potensielt blir avhengige av kinesisk produksjon for å lykkes med det grønne skiftet.

Samlet vurderer vi at enkelte stater, som besitter knappe ressurser eller svære innenlandske markeder, kan oppnå økte muligheter til å etablere avhengigheter som følge av den teknologiske utviklingen.

4.2.3 Etterretningsvirksomhet

Økonomisk aktivitet kan åpne muligheter for å bedrive etterretningsvirksomhet i mottakerlandet. For eksempel identifiserer Udal mfl. (2022) flere hendelser som kan være russiske forsøk på å utføre etterretning forkledd som økonomisk aktivitet, inkludert eiendomsinvesteringer på strategisk viktige lokasjoner og økonomisk virksomhet i nærheten av viktig infrastruktur. I denne seksjonen drøfter vi hvordan den teknologiske utviklingen kan gjøre det både mer aktuelt å forsøke å utnytte økonomisk aktivitet til etterretningsformål og åpne flere muligheter for å gjøre det.

I delkapittel 3.1 vektla vi betydningen av data i moderne, digitale økonomier. Data er også viktig i etterretningsøyemed, inkludert som del av «åpne kilder etterretning». Vi vurderer at den teknologiske utviklingen øker mulighetene til å utnytte økonomisk aktivitet for å innhente sensitiv informasjon eller data. Tingenes internett bidrar til at data samles inn «overalt» og i større mengder enn tidligere, på tvers av enheter, og med avanserte analyseverktøy, inkludert kunstig intelligens, åpnes nye muligheter for å analysere og trekke ut innsikt fra dataene. Farsund mfl. (2022) har testet noen tilfeldige IoT-produkter rettet mot forbrukermarkedet, og finner at produktene ofte samler inn detaljerte data om brukere og/eller miljøet, og at disse dataene havner i utlandet. De påpeker også at det er utfordrende å beskytte seg mot denne datainnsamlingen.

Det kan også være rimelig å forvente investeringer og oppkjøp i selskaper i mottakerlandet motivert av tilgang til data ikke bare i et kommersielt perspektiv, men også i etterretningsøyemed. Som følge av at (digitale) verdikjeder blir lengre og mer geografisk spredt (se delkapittel 3.3), vurderer Farsund mfl. (2022) at det også vil eksistere flere muligheter for aktører til å komme seg inn i verdikjeder, og at det kan være mer krevende for «mottakeren» å oppdage trusselaktøren. Det betyr at det kan eksistere en risiko for at investeringer og oppkjøp i selskaper i verdikjeder også kan være inngangsportaler for å få tilgang til data og informasjon i andre selskaper i verdikjeden. Det samme kan gjelde for byggeprosjekter, og Waage mfl. (2022) gjengir en hendelse hvor Kina er blitt anklaget for å ha tilegnet seg konfidensiell data fra det kinesiskbygde hovedkvarteret til den afrikanske union (se også Fidler 2018).

Videre kan etterretningsorganisasjoner i prinsippet også forsøke å få produsenten av utstyr til å legge inn bakdører under produksjon, eller å forsøke å gjøre det selv etter at utstyret er produsert, før det blir levert til sluttbruker (Birkemo, Kristiansen og Farsund 2021). Salg av produkter eller tjenester kan følgelig også være en form for økonomisk aktivitet som kan utnyttes for informasjonsinnhenting og etterretning. I seksjon 4.2.5 utdyper vi om hvordan også stater som oppnår en sentral posisjon i nettverk – for eksempel 5G – potensielt kan trekke ut informasjon fra nettverket.

Kunstig intelligente systemer og øvrige omtalte teknologiområder kan dessuten i seg selv være (svært) komplekse. Denne kompleksiteten kombinert med knapp tilgang til personell med kompetanse til å forstå alle avhengigheter og eventuelle sårbarheter kan medføre en risiko for at informasjon om personell, materiell, kapabiliteter, sårbarheter og annet kan fanges opp av fremmede stater. Samtidig er det viktig å huske på at kompleksiteten tilknyttet nye teknologier også kan gjøre det utfordrende for en trusselaktør å forsøke å få tilgang til informasjonen og dataene av interesse (nål-i-høystakk-problematikk). I tillegg kan trenden med økt utsetting av drift og forvaltning av selskapers datasikkerhet til tredjeparts spesialister (se delkapittel 3.2.3) medføre bedre beskyttelse av data.

Samlet vurderer vi likevel at den teknologiske utviklingen vil øke staters muligheter til, og utbytte av, å forsøke å utføre etterretningsvirksomhet gjennom økonomisk statshåndverk.

4.2.4 Styrke materielle/militære kapabiliteter

Gjennom økonomiske virkemidler kan en stat tilegne seg teknologi, ekspertise og andre ressurser som kan brukes for å styrke og modernisere statens militære kapabiliteter. Vi inkluderer denne handlingsmåten som en form for akkumulering av makt siden staten øker sine muligheter for å true med, eller eventuelt å ta i bruk, militære maktmidler på et senere tidspunkt.

FFI har tidligere studert hvordan Russland og Kina tilsynelatende har forsøkt å utnytte økonomiske virkemidler for å få tilgang til teknologi, kunnskap og ekspertise, ved å forsøke å identifisere hendelser hvor dette potensielt har forekommet (Udal mfl. 2022; Waage mfl. 2022). De identifiserte hendelsene retter seg mot handlinger utført internasjonalt, slik som teknologityveri, investeringer i selskaper i utlandet eller andre forsøk på å omgå eksportkontroll i mottakerlandet. I Norge ble for eksempel salget av Bergen Engines til det russiskregistrerte Transmashholding Group stanset på bakgrunn av bekymringer om at teknologien Bergen Engines besitter, ville kunne ha styrket Russlands militære kapabiliteter (Flaaten 2021). I tillegg fremhever eksisterende litteratur hvordan stater også kan bruke økonomiske virkemidler slik som lån og investeringer til andre land for å forsøke å styrke alliertes kapabiliteter (Hasegawa 2018), som blant annet Marshallhjelpen kan bli sett som et eksempel på.

I lys av den teknologiske utviklingen, kan det bli mer aktuelt for stater å forsøke å utnytte økonomiske virkemidler til å utføre teknologityveri eller omgåelse av eksportkontroll for å få tak i avansert teknologi. I tillegg til handlinger med et utenlandsk fokus – tilegne seg teknologi, kunnskap og ekspertise fra utenlandske selskaper og ekspertmiljøer – utvider bidragene som setter fokus på politikk for å fremme og styrke nasjonal teknologiutvikling, forståelsen av hvordan stater kan utnytte økonomiske virkemidler til å styrke sine materielle/militære kapabiliteter. Som forklart i seksjon 2.2.2 har slik politikk et innenlandsk fokus, men er drevet av geopolitiske hensyn (Weiss 2021).

I seksjon 2.2.2 redegjorde vi for «det nye økonomiske statshåndverket» der litteraturen argumenterer for at skillet mellom økonomisk statshåndverk og næringspolitikk i større grad enn tidligere blir visket ut. En mer multipolar verden, rivaliseringen mellom USA og Kina og konkurransen innenfor forskning, utvikling og innovasjon vestlige land (inklusive USAs allierte

i Øst-Asia) opplever fra fremvoksende økonomier, bidrar til at virkemidler for å styrke materielle og militære kapabiliteter blir viktigere fremover. Det blir sentralt både å lede an i utviklingen av ny teknologi og å beskytte fremskrittene. Spesielt gjelder dette militær teknologi, men i og med at mye teknologi rettet mot sivil bruk også kan og vil benyttes av militære organisasjoner – såkalt flerbruk (*dual use*) – vil selv sivil teknologi kunne utfordre samfunns- og statssikkerheten. Slik blir forsknings-, handels- og investeringspolitikk rettet mot å opprettholde eller frembringe teknologisk overlegenhet en del av det økonomiske statshåndverket. Her er det altså den teknologiske utviklingen som er formålet med det økonomiske statshåndverket, og ikke den teknologiske utviklingen som styrker eller svekker staters muligheter til å benytte slikt håndverk. Det resulterer imidlertid i at virkemidlene som statene benytter i det «nye» økonomiske statshåndverket endres, ved å inkludere virkemidler som tidligere var forbeholdt næringspolitikk. Næringspolitikk er jo rettet mot innenlandsk økonomi, mens «tradisjonelt» økonomisk statshåndverk i hovedsak er rettet mot utenrikspolitiske mål.

Fra intervjuene og eksisterende litteratur identifiserer vi flere virkemidler stater potensielt kan ta i bruk for å styrke egen industri. For eksempel kan stater bevisst søke å legge til rette for at produkter og tjenester levert av egne selskaper er billigst og best, slik at de kaprer markedsandeler som kan gi fordeler ved konflikt, sabotasje, etterretning, med mer. Subsidiering av spesifikke næringer og selskaper og handelshindringer som ikke er toll[48], slik som sanitære begrensninger, kvoter eller krav om bruk av hjemlige økonomiske aktører, er typiske virkemidler (Beckley 2022). Slike virkemidler kan bidra til økt hjemlig verdiskapning, men også bidra til at landets økonomiske aktører kan dominere verdensmarkedet, gjøre andre land avhengig av produkter, tjenester, kompetanse og teknologi, og øke innsamlingen av data. Videre kan avsenderstaten, gjennom kontroll over hjemlige bedrifter, investorer eller statlige investeringsfond, kjøpe opp eller kjøpe seg inn i oppstartsselskaper og andre bedrifter i teknologisektoren i mottakerlandet med formål om å hente hjem teknologi eller sabotere selskapenes utvikling.[49] Det kan også bidra til å styrke avsenderstatens kapabiliteter relativt til konkurrenters kapabiliteter. Mens oppkjøp av selskaper kan være en måte å sikre tilgang til teknologi, kunnskap og ekspertise – og data – på kort sikt, kan stater i et langsiktig perspektiv også søke å benytte oppkjøpene til å (videre)utvikle eget, nasjonalt teknologi- og kompetansenivå.

Samlet vurderer vi at dette «nye» økonomiske statshåndverket vil bli viktigere i årene som kommer. Dette gjelder ikke bare i USA og Kina. For eksempel må allierte av USA også regne med å bidra i utviklingen av teknologi og beskyttelsen av den overfor stater utenfor det amerikanske alliansenettverket. Ifølge Beckley (2022) ser vi konturene av en ny verdensorden der G7-landene leder an i etableringen av en økonomisk blokk som holder autoritære stater utenfor og en militær forskansning mot Kina. Den økonomiske blokken adresserer utfordringen fra Kina ved å «forme eksklusive handels- og investeringsnettverk designet for å øke hastigheten på fremgang i kritiske sektorer og senke Kinas fart» (Beckley 2022).[50] Hvis Beckley har rett, vil

[48] Se https://www.instituteforgovernment.org.uk/explainers/non-tariff-barriers.
[49] Se for eksempel Drezner (2008) for en kort diskusjon om dette i forbindelse med statlige investeringsfond.
[50] Utestengelse av Kina fra nettverkene er også et eksempel på handlingsmåten *manipulere tilgang til nettverksstrømmer*, se seksjon 4.1.4.

interessen for å redusere avhengigheter av Kina øke og fokuset på å hindre Kinas tilgang til avansert teknologi øke i årene fremover i USA og blant dets allierte.

4.2.5 Tilrettelegge for (skjult) sabotasje

Mens seksjon 4.1.3 fokuserte på hvordan eierskapskontroll potensielt kan utnyttes for å utøve makt gjennom sabotasje av infrastruktur, tar vi i denne seksjonen for oss hvordan økonomiske virkemidler kan benyttes til å komme i posisjon til å utføre sabotasje i fremtiden, eventuelt også ved å muliggjøre bruken av andre virkemidler som cyberrelaterte virkemidler.

Forskning ved FFI beskriver flere årsaker til at risikoen for sabotasje kan øke med de nye teknologiene, og vi har i seksjon 4.1.3 allerede pekt på flere slike årsaker. For eksempel er det flere potensielle sårbarheter i IoT-systemer som kan utnyttes av en trusselaktør til å utføre ulike former for angrep.[51] Dersom en angriper får fysisk tilgang til IoT-enheter (sensorer og aktuatorer) og/eller hubene som de benytter for kommunikasjon, kan angriperen «koble seg til … for å overstyre hva som foregår på enheten» (Farsund mfl. 2022: 20). Ved å få tilgang til ukryptert informasjon om identiteten til kommuniserende parter, kan en angriper også komme i posisjon til å forsøke å utgi seg for å være en annen part (Farsund mfl. 2022). Med aktuatorer som muliggjør handling i den fysiske verden, kan dessuten konsekvensene av slike angrep øke.

I denne rapporten er vi interessert i hvordan økonomiske virkemidler kan utnyttes for å komme i posisjon til å gjennomføre slike eller andre angrep i fremtiden. Som drøftet i seksjon 4.1.3 kan økonomiske virkemidler – slik som investeringer, oppkjøp, salg av utstyr og inngåelse av drifts- og vedlikeholdsavtaler – åpne muligheter for at uønskede aktører får tilgang og kan utføre sabotasje i fremtiden, inkludert ved bruk av cyberrelaterte virkemidler. Samtidig kan behovet for tjenesteutsetting og ekstern støtte øke, som følge av mangel på kompetent arbeidskraft til å forstå, drifte og vedlikeholde avanserte teknologiske systemer. Selv store stater og multinasjonale selskaper vil måtte lene seg på ekspertise og kunnskap utenfor egen organisasjon. Det er også aktuelt å huske på at teknologiske løsninger kjennetegnes av kontinuerlige oppdateringer, heller enn at produktet selges «ferdig». Det kan åpne muligheter for å utføre sabotasje på et senere tidspunkt dersom en avsenderstat er i stand til å utnytte leverandørene av systemene til dette formålet. Ny teknologi som 5G, tingenes internett og kunstig intelligens bidrar til å gjøre systemer og verdikjeder mer kompliserte og uoversiktlige, og det gjør også attribusjon vanskeligere. Andre typer teknologier som vi har utelatt i denne rapporten vil også kunne bidra til økt sårbarhet overfor sabotasje i form av drenering av oppdateringer, tjenesteleveranser, og lignende (se også seksjon 4.1.2). Økt automatisering av arbeidsoppgaver og beslutningstaking i både offentlige og private selskaper, samt økt bruk av autonome systemer som autonome kjøretøy, kan også bidra til å styrke staters muligheter til å utføre sabotasjeoperasjoner tilrettelagt av økonomiske virkemidler.

Samtidig har flere respondenter argumentert for at det er krevende å utføre sabotasje i cyberdomenet, og at kostnaden kan være relativt høy sammenlignet med gevinsten. Det er tendenser til at IT-systemer relativt raskt stables på beina igjen. I tillegg er ofte cybervåpen engangsvåpen. Det

[51] Det kan for eksempel være Man in the Middle (MitM)-angrep, injisering av egen nettverkstrafikk i systemet via brukergrensesnittet, DoS- og DDoS-angrep, SQL-injection, cross-site scripting, modifisere firmware, installere egne bakdører og å gjøre produktene utilgjengelige via jamming (Farsund mfl. 2022).

er også i økende grad bekymringer for uintenderte konsekvenser og «utilsiktet skade» (*collateral damage*) ved cyberangrep. Av disse grunnene kan det være rimelig å anta at det er mer sannsynlig med forekomster av forsøk på sabotasje i form av forsinkelser eller andre forstyrrelser i leveranser av for eksempel reservedeler, programvareoppdateringer og vedlikeholdstjenester (se seksjon 4.1.2), heller enn at økonomisk aktivitet utnyttes for å posisjonere seg for fremtidige sabotasje-operasjoner i cyberdomenet. Dessuten kan trenden med tjenesteutsetting av datasikkerhet og beskyttelse av personvern (se delkapittel 3.3) til «tredjeparts spesialister» gjøre det mer krevende for en trusselaktør å angripe systemene enn da de ble driftet internt i selskaper.[52] Likevel kan det oppstå konfliktsituasjoner som er så alvorlige at det vil bli vurdert lønnsomt av en avsenderstat å utnytte eventuelle etablerte sårbarheter – blant annet gjennom lovlige økonomiske transaksjoner – også til å utføre angrep i cyberdomenet.

Samlet vurderer vi at den teknologiske utviklingen gir stater bedre muligheter til å legge til rette for fremtidige sabotasjemuligheter, spesielt i cyberdomenet. Samtidig understreker vi at sabotasjeoperasjoner i cyberdomenet også kan medføre høye kostnader for avsenderstaten, både politisk, økonomisk og omdømmemessig, samtidig som effekten er tvilsom. Derfor tror vi at det er mer sannsynlig med maktutøvelse i form av drenering, utsettelse av oppdateringer, og andre former for press og sabotasje som diskutert i seksjon 4.1.2 og 4.1.3.

4.2.6 Panoptikon

Panoptikon – definert av Farrell og Newman (2019) som uttrekk av informasjon og data fra nett-verksstrømmer gjennom kontroll over regionale eller globale knutepunkt – er en handlingsmåte som vi, i likhet med handlingsmåten *etterretningsvirksomhet*, vurderer kan øke i betydning med den teknologiske utviklingen.

For eksempel diskuterer både Segal (2021) og Goddard (2021) hvordan Kinas beherskelse av 5G-teknologi kan gi Beijing muligheter til å utnytte panoptikon. Dersom kinesiske aktører dominerer 5G-nettverk, kan den kinesiske staten oppnå «en knutepunktposisjon i kommunikasjon» med muligheter for å trekke ut informasjon fra nettverksstrømmene (Goddard 2021: 94). Segal (2021) henviser også til hvordan amerikanske myndigheter har fremhevet trusselen om kinesisk etter-retning som begrunnelse for å ekskludere Huawei fra utbyggingen av 5G-infrastruktur, med spesiell vekt på de omfattende verktøyene det kinesiske kommunistpartiet har til rådighet for å kreve samarbeid fra privat næringsliv i Kina. Beckley (2022) mener at Kina har «installert maskinvare for digitale nettverk i dusinvis land» for å oppnå strategiske fordeler. Mulighetene for informasjonsinnhenting kan dessuten være store etter hvert som 5G-teknologi blir tatt i bruk for å understøtte smarte byer. Samtidig blir det påpekt at bruken av kryptering og autentisering vil bidra til å redusere disse risikoene for datainnsamling. Det er også relevant å vurdere hvilke deler av 5G-infrastrukturen som en gitt aktør er leverandør av. Som forklart i seksjon 2.1.2 er det først i kjernenettet data kan kobles til enkeltstående brukerutstyr. Forsøk på avlytting av basestasjoner og øvrig infrastruktur er dermed utfordrende, fordi det er svært vanskelig å vite hvem som er hvem. Det er med andre ord viktig å få tilgang til datasentrene og 5G-kjernen.

[52] Dette gjelder spesielt for små og mellomstore bedrifter.

I tillegg til 5G-teknologi, fremhever Tusikov (2021) hvordan internettplattformer overvåker brukernes aktiviteter og transaksjoner, og hvordan denne «masseakkumuleringen av data presenterer et fristende mål for stater». Tusikov (2021) trekker særlig frem dette i konteksten av overvåking og kontroll av egne borgere, men det kan også tenkes at data kan være interessante for stater også i etterretningsøyemed, på samme måte som datainnsamling for etterretningsformål via bilaterale kanaler (seksjon 4.2.3). Forsøk på å manipulere og omdirigere flyten av informasjon på internett kan potensielt også være en måte å samle inn data (temporært) via kontroll over knutepunkt i nettverk, og det er eksempler på at data har blitt omdirigert via Kina (se f.eks. Hillman 2021: 129–166).

Samlet vurderer vi at mulighetene for å utføre økonomisk statshåndverk i form av panoptikon vil øke som følge av den teknologiske utviklingen.

4.2.7 Øke avhengigheten til knutepunkt

I tillegg til økonomiske transaksjoner som øker den bilaterale avhengigheten mellom mottakerlandet og avsenderlandet, kan en avsenderstat også akkumulere makt gjennom forsøk på å øke avhengigheten til et knutepunkt avsenderstaten har kontroll over i nettverk.

Som Tusikov (2021: 141; se også Moran 2013) belyser, vil mulighetene for å etablere og utnytte knutepunkt avhenge av «graden av konsentrasjon i en gitt industri og tilgjengeligheten av erstatningstjenesteytere», inkludert hvor enkelt det er for nye aktører å starte opp i industrien. I delkapittel 3.4 diskuterte vi hvordan økt markedskonsentrasjon potensielt er en konsekvens av den teknologiske utviklingen. Det kan resultere i at land blir mer avhengige av enkelte regionale eller globale knutepunkt. Tusikov (2021: 143) fremhever spesifikt skyinfrastruktur som en «høyt konsentrert industri», dominert av amerikanske aktører – som Amazon Web Services, Microsoft Azure, IBM og Google Cloud Platform – og noen kinesiske aktører – som Alibaba Cloud og Tencent Cloud. Også online betalingstjenester blir trukket frem som et eksempel på en konsentrert industri med få alternativer til de store, dominerende aktørene som PayPal, Visa, MasterCard, WeChat Pay og Alibaba's AliPay (Tusikov 2021). Beckley (2022) mener at Kina eksplisitt ønsker seg 'kvelningspunkt' (*chokeopints*), definert som «varer og tjenester som andre land ikke kan leve uten». Det vil gi kinesiske myndigheter muligheter til å presse frem innrømmelser. Å bli monopolist på sentrale varer og tjenester er derfor en form for akkumulering av makt ved å skape avhengigheter til knutepunkt. Også Hillman (2021) setter fokus på hvordan kinesiske leverandører for mange land etablerer seg som den billigste og/eller i realiteten eneste tilgjengelige leverandøren av produkter og tjenester som for eksempel 5G, internettilgang og satellittsystemer. Utover muligheter for datainnsamling og potensielt kvelning/sabotasje kan slik aktivitet bidra til å øke landenes avhengighet til Kina og styrke Kinas politiske innflytelse i landene.

Under intervjuene løfter respondenter særlig frem bekymringer om at Norge eller vesten mister egen kompetanse og egne leverandører av avansert teknologi, som mobilnett (5G), slik at ikke-vestlige (særlig Kina) i neste omgang kan bli eneste leverandør av 6G. Dette kan også skje med andre typer teknologier, som kunstig intelligens og komponenter og programvare knyttet til tingenes internett. Hvis det er slik at det er superbedriftseffekter (se delkapittel 3.4) – for eksempel nettverkseffekter – knyttet til utvikling og produksjon av ny teknologi, er slike scenarioer mer

sannsynlige. Hvis fremvoksende økonomier, som Kina, subsidierer egne bedrifter for å vinne frem i nye teknologier, vil kinesiske bedrifter kunne dominere sentrale, høyteknologiske industrier i fremtiden.

Innen denne handlingsmåten vurderer vi at det også er relevant å synliggjøre hvordan teknologisk standardisering, eller standardsetting, kan være et virkemiddel for å akkumulere makt. Som Malkin (2020; se også Ernst og Kim 2002) forklarer, kan global produksjon forstås som et hierarkisk system, som strekker seg fra «lavnivåmontering» (*low-end assembly*) til komplekse FoU- og designaktiviteter – til standardsetting på toppen av pyramiden. Selskapene som setter globale teknologistandarder «definerer ikke bare hvordan varer blir produsert, men også hvordan fremtidige generasjoner av teknologiske oppfinnelser er kommersialisert» og utgjør slik «prosessen med eiendelsskapning» (*process of asset creation*) (Malkin 2020: 19).

Særlig amerikansk/vestlig industri har definert teknologiske standarder i bruk i dag. Litteraturen fremhever hvordan Kina i økende grad forsøker å ta plass innen teknologisk standardisering globalt, blant annet innen kommunikasjonsteknologi og jernbane (Hungerland og Chan 2021; Malkin 2020; Yan 2022; se også Hillman 2021: 13–14). Standardsetting kan i prinsippet utnyttes som et maktmiddel ved at standardisering gir makt til å bestemme hvordan teknologi skal «se ut» – og kan følgelig bidra til å «låse inne» (*lock in*) produsenter lengre nede i «hierarkiet» samt forbrukere – men hittil har standardisering primært vært drevet av kommersielle interesser. Det er likevel viktig å være klar over makten som potensielt ligger i å promotere egne selskapers rolle innen standardiseringsarbeid, og som er årsaken til at flere omtaler standardisering som en form for (økonomisk) statshåndverk (Malkin 2020; Yan 2022).

Et annet poeng er at nye teknologier, spesielt kunstig intelligens, vil kunne være såkalte allsidige teknologier (se boks 3.2 i kapittel 3). I så fall vil bruksområdene til slike teknologier spre seg utover økonomien og bli en viktig innsatsfaktor i produksjonen av mange ulike produkter og tjenester. Å dominere produksjonen av maskinvare og programvare for slike teknologier vil gi muligheter for maktbruk og representerer derfor akkumulering av makt. Hvis kunstig intelligens også er en oppfinnermetode (Cockburn, Henderson, og Stern 2018; Griliches 1957), forsterkes virkningene for maktakkumulering av dominans av produkter og tjenester knyttet til disse teknologiene.

Samlet vurderer vi at den teknologiske utviklingen kan øke enkelte stater, i hovedsak stater med store økonomier som USA, Kina, EU og Japan, sin evne til å utnytte sentraliteten i nettverkene av global produksjon, distribusjon og salg av varer og tjenester. Det gjelder både fordi ny teknologi ser ut til å endre den globale økonomiens virkemåte, med høyere markedskonsentrasjon med færre og større tilbydere, men også fordi noen få, store land som USA og Kina dominerer utvikling og produksjon av produkter og tjenester knyttet til nye teknologier.

4.3 Oppsummering av kapittelet

I dette kapittelet har vi undersøkt og besvart problemstilling (2) – hvordan kan den teknologiske utviklingen endre mulighetsrommet for staters bruk av økonomisk statshåndverk? – ved å synliggjøre potensielle implikasjoner av den teknologiske utviklingen, strukturert etter handlingsmåtene av økonomisk statshåndverk (tabell 1.1). Vi presiserer at diskusjonene i kapittelet er et første steg på veien mot å styrke koblingen mellom innsikt om utfordringer og sårbarheter ved ulike nye teknologier og forståelsen av staters muligheter for økonomisk statshåndverk. Det er et komplekst tema som bør utforskes videre og grundigere i fremtidige studier enn hva som har vært mulig innenfor rammene av dette oppdraget.

Vi har identifisert flere potensielle implikasjoner av ny teknologi for økonomisk statshåndverk som nye studier kan bygge videre på. I tabell 4.1 oppsummerer vi noen sentrale observasjoner per handlingsmåte.

Tabell 4.1 Oppsummerende vurderinger per handlingsmåte av hvordan den teknologiske utviklingen kan endre mulighetsrommet for økonomisk statshåndverk.

Handlingsmåte	Vurdering av implikasjoner av teknologiutviklingen
Utøve makt	
Manipulere tilgang til salg til innenlandsk marked	Økt potensial gjennom bruk av KI og stordata til å utforme virkemidler. Aktuelle økonomiske virkemidler er fremdeles importrestriksjoner, turismerestriksjoner og lignende. For enkelte stater også økt potensial pga. store innenlandske forbrukergrupper, som blir viktigere med den teknologiske utviklingen.
Manipulere tilførselen av ressurser	Økt potensial gjennom nye avhengigheter til ressurser, som kompetanse, varer, tjenester og råvarer, som får større betydning med den teknologiske utviklingen. KI kan bidra til mer effektiv utforming av virkemidler. Manipulering av kompetanse kan spesielt bli et mer potent økonomisk virkemiddel for enkelte stater.
Sabotere infrastruktur (gjennom eierskaps-kontroll)	Økt potensial for sabotasje ved at samfunnet avhenger av tjenester og systemer blir sammenkoblet i større grad. Det oppstår flere angrepspunkter, inkludert større muligheter for sabotasje utført gjennom eierskap i utlandet. Aktuelle økonomiske virkemidler er fremdeles investeringer og oppkjøp.
Manipulere tilgang til nettverks-strømmer	Digitale og andre fysiske valutaer kan svekke USDs dominans i det internasjonale finanssystemet, og digitale valutaer kan på sikt svekke mulighetene til å utnytte internasjonale finansnettverk til å utøve makt. På den annen side økt potensial for økonomisk statshåndverk ved at internettplattformer kan bli benyttet som virkemiddel til å presse og lokke med hhv. utestengelse fra, eller tilgang til, plattformene. Også potensial for å utnytte muligheter til å utestenge stater fra «nettverk» av høyteknologiske produkter, tjenester og kritiske innsatsfaktorer.

Akkumulere makt	
Forme (sær)-interesser og oppfatninger i mottakerlandet	Økonomiske virkemidler er fremdeles lån, oppkjøp, investeringer, osv., men de kan bli mer potente. Økt potensial pga. at antallet mulige inngangsportaler for å bedrive for eksempel påvirkningsoperasjoner øker betraktelig med nye teknologier som skytjenester, 5G og tingenes internett. Det blir også lettere å bedrive denne handlingsmåten fra utlandet og lettere å spre positiv (des)informasjon om avsenderstaten.
Øke avhengighet til ressurser og innenlandsk marked	Potensialet kan øke for enkelte land som besitter knappe ressurser, teknologisk kompetanse, viktig produksjon og/eller attraktive innenlandske markeder. Næringspolitikk, med geopolitisk motivasjon, kan utnyttes som økonomisk virkemiddel for å styrke egen økonomi og ressurskontroll (se derfor også handlingsmåten *styrke materielle/militære kapabiliteter*).
Etterretningsvirksomhet (gjennom økonomisk aktivitet)	De økonomiske virkemidlene er de samme, men mulighetene for innhenting av informasjon og data øker betydelig med bl.a. tingenes internett og 5G. Også økt potensial pga. at (digitale) verdikjeder blir lengre, mer geografisk spredt og mer uoversiktlige, samt pga. muligheter til å legge inn bakdører via kontinuerlige programvareoppdateringer. Samtidig kan den økte kompleksiteten også vanskeliggjøre utnyttelsen av økonomisk aktivitet til etterretningsformål.
Styrke materielle/ militære kapabiliteter	Den teknologiske utviklingen har bidratt til å aktualisere næringspolitikk med geopolitisk motivasjon som et økonomisk virkemiddel. Forståelsen av økonomisk statshåndverk som «utadrettet» bør revideres i lys av den teknologiske utviklingen. Flere inngangsportaler som følge av økt (digital) sammenkobling kan dessuten øke muligheten til å tilegne seg sensitiv/beskyttet teknologi, programvare, patenter og andre immaterielle rettigheter, for eksempel gjennom teknologityveri og omgåelse av eksportkontroll.
Tilrettelegge for (skjult) sabotasje	Økt potensial, spesielt for å utnytte økonomisk aktivitet til å legge til rette for operasjoner i cyberdomenet, blant annet pga. mer kompliserte og sammenkoblede systemer, økt automatisering av arbeidsoppgaver og økt behov for tjenesteutsetting. Samtidig fremstår terskelen for å utføre sabotasje ved bruk av cybervirkemidler som høy, med potensielt store, negative konsekvenser for avsenderstaten og involverte kommersielle aktører.
Panoptikon	Virkemidlene er de samme, men mulighetene for overvåking og innhenting av informasjon og data øker betydelig. Det økte potensialet kommer både av mer sammenkoblede nettverk og økt generering av data.
Øke avhengighet til knutepunkt	Økt potensial, i hovedsak for store økonomier, til å utnytte sentralitet i nettverk for global produksjon, distribusjon og salg av varer og tjenester. Årsaker til dette er blant annet økt markedskonsentrasjon, muligheter til å oppnå en monopolistposisjon innen global forsyning av teknologisk viktige ressurser,

	innsatsfaktorer og kompetanse (som sjeldne jordarter eller kompetanse på hvordan kommunikasjonsteknologi fungerer). Den teknologiske utviklingen påvirker hvilke økonomiske virkemidler stater har tilgjengelig, og vi noterer særlig at standard-setting og næringspolitikk med geopolitisk motivasjon er relevante, men tidligere lite vektlagte, virkemidler.

Som tabell 4.1 viser, kan den teknologiske utviklingen påvirke staters muligheter til å utføre økonomisk statshåndverk på flere måter. Innen utøvelse av makt fremstår det spesielt som at den teknologiske utviklingen vil medføre styrkede muligheter for å utnytte avhengigheter til kompetanse, ressurser, komponenter, osv. til (fordekt) å sabotere systemer. Vi forventer også at det vil oppstå styrkede muligheter til å utnytte eierskapskontroll til å utføre sabotasje mot systemer og infrastruktur, men fordekt sabotasje gjennom forstyrrelser i tilførselen av ressurser – som forsinkelse i vedlikeholdstjenester – fremstår som en mer aktuell handlingsmåte dersom den er tilgjengelig. For flere – kanskje til og med alle – av handlingsmåtene, kan tilgang på store datasett (for eksempel handelsdata) kombinert med KI-teknologi potensielt bidra til å identifisere hvilke økonomiske virkemidler som kan ha størst potensial til å oppnå avsenderstatens mål, til lavest mulig kostnad for avsenderstaten.

Innen akkumulering av makt – det vil si, tilrettelegging for fremtidig økonomisk, eller annen, maktbruk – vurderer vi at den teknologiske utviklingen særlig vil styrke mulighetene til å utnytte økonomisk aktivitet til å hente inn informasjon og data. Det kan foregå bilateralt, for eksempel gjennom investeringer i målselskaper eller underleverandører som yter tjenester for målselskapet, eller gjennom nettverk, slik som 5G og internettplattformer. Vi vurderer også at enkelte stater kan oppnå bedre muligheter for å skape avhengigheter hos mottakerland som følge av den teknologiske utviklingen. Årsaker til dette kan både være kompetansemangel, økt konkurranse om knappe ressurser og innsatsfaktorer som halvlederteknologi og sjeldne metaller, økt markeds-konsentrasjon med færre alternative leverandører samt økt (digital) sammenkobling. Vi tar også med oss at det kan oppstå styrkede muligheter for å utnytte økonomiske virkemidler som legger til rette for fremtidig sabotasje, særlig ved bruk av cybervirkemidler, men at terskelen for å utføre sabotasjeoperasjoner i cyberdomenet fremstår som relativt høy. Derimot ser vi det som mer sannsynlig at økonomisk aktivitet, som investeringer og oppkjøp av selskaper, kan inngå i staters forsøk på å forme (sær)interesser og oppfatninger i mottakerlandet, for eksempel ved at avsender-staten kommer i posisjon til å utføre påvirkningsoperasjoner – i tillegg til å samle inn data som kan gjøre slike operasjoner mer effektive og spissede mot enkelte målgrupper.

Innen akkumulering av makt, tar vi også særlig med oss perspektivet til det «nye» økonomiske statshåndverket, som – i motsetning til den tradisjonelle tilnærmingen til fagfeltet – plasserer næringspolitikk (i bred forstand) med geopolitisk motivasjon som en sentral del av staters repertoar av økonomiske virkemidler. Kombinert med «kvelningspunkter» i form av eksklusive teknologinettverk mellom likesinnede stater eller allierte og forstyrrelser i ressurstilgangen til geopolitiske konkurrenter, gir slik bruk av økonomiske virkemidler muligheter til å beskytte egen teknologi – og potensielt også forsøke å (for)bli ledende i utvikling og bruk av ny teknologi, inkludert flerbruks- og militærteknologi.

Selv om vi har diskutert mange forhold som tilsier at staters – særlig stormakters – muligheter til å utføre økonomisk statshåndverk ser ut til å øke i takt med den teknologiske utviklingen, noterer vi oss likevel noen forhold som også kan utfordre bruken av økonomiske virkemidler. Vi oppsummerer dem kort her.

For det første minner vi om at mange/de fleste av handlingene vi har omtalt i dette kapittelet fordrer en sterk grad av statlig kontroll over kommersielle aktører. For eksempel vil både informasjons- og datainnsamling, tilrettelegging for påvirkningsoperasjoner og forsøk på forstyrrelser og sabotasje gjennom økonomisk statshåndverk kreve at kommersielle aktører samarbeider med staten – potensielt med (store) kostnader både økonomisk og omdømmemessig. I hvilken grad ulike stater vil lykkes med å påvirke og kontrollere økonomiske aktører til å tjene statens formål, er et tema innen økonomisk statshåndverk hvor det er behov for mer forskning (se også Norris 2016, 2021). Vi vurderer at temaet også bør studeres nærmere i lys av den teknologiske utviklingen. For eksempel kan det være relevant å undersøke nærmere hvordan endringer i organisasjonsformer, markedskonsentrasjon, graden av internasjonalisering, osv. (se kapittel 3 for detaljer) kan påvirke staters muligheter til å utøve kontroll over kommersielle aktører.

For det andre kjennetegnes den teknologiske utviklingen av at produkter, tjenester og systemer blir mer komplekse – blant annet som følge av at kunstig intelligens i økende grad blir anvendt til drift, vedlikehold og oppgaveløsning – i tillegg til intrikate og uoversiktlige (digitale) verdikjeder, høyere usikkerhet knyttet til verdien av tjenester for ulike brukere, m.m. (for detaljer, se delkapittel 3.2). Den økte kompleksiteten som følger med den teknologiske utviklingen kan ikke bare bidra til å gjøre mottakerland mer sårbare, men også gjøre det mer utfordrende for avsenderstater å innrette sitt økonomiske statshåndverk.

For det tredje kan ny teknologi og økt grad av tjenesteutsetting også bidra til å *redusere* sårbarheter. Arbeidsdeling, spesialisering og fokus på kjernevirksomheten bidrar med en mer effektiv utnyttelse av kompetanse og kapital. Å overlate oppgaver til underleverandører, i inn- og utland, kan derfor gjøre at bedrifter og offentlige virksomheter utfører egne hovedarbeidsoppgaver bedre samtidig som de mottar tjenester og varer med høyere kvalitet og/eller til en lavere kostnad enn de ville fått til selv. Det er nemlig skalautbytte i spesialisering og arbeidsdeling. Slike underleverandører kan spesialisere seg på å levere sikre systemer, varer og tjenester. De har også insentiver til å unngå å bli leddet som skaper sikkerhetsutfordringer for næringslivet og det offentlige i mottakerlandene. Det er derfor ikke sikkert at forsøk på å bygge kompetanse internt i egen virksomhet vil redusere sårbarhetene i en økonomi der teknologien blir mer og mer kompleks.

Selv om vi, basert på dette arbeidet, samlet sett vurderer at mulighetene for å utføre økonomisk statshåndverk blir styrket av den teknologiske utviklingen, gjenstår det likevel et (stort) behov for videre forskning på temaet for å få et bedre grep om nettoeffekten – både totalt, innenfor hver handlingsmåte av økonomisk statshåndverk og i kombinasjon med ikke-økonomiske virkemidler som del av staters sammensatte virkemiddelbruk.

5 Implikasjoner for Norge

I dette kapittelet diskuterer vi implikasjoner for norsk sikkerhet. Vi tar utgangspunkt i Norges nasjonale sikkerhetsinteresser, definert i Sikkerhetsloven (2018: § 1-5), og benytter forståelsen av sikkerhetsinteressene slik de er redegjort for i NSM (2019; se også Waage, Kvalvik og Lindgren 2021c).[53] Poenget med diskusjonen er å fremme noen hypoteser om hvordan staters endrede muligheter for å utføre økonomisk statshåndverk som følger i kjølvannet av nye teknologier, vil kunne påvirke norsk sikkerhet. Det er knyttet stor usikkerhet til hvordan nye teknologier vil se ut i fremtiden, hvordan disse teknologiene vil forme fremtidens økonomier og samfunn, og ikke minst hvordan nye teknologier vil påvirke staters økonomiske statshåndverk. Det er også stor usikkerhet knyttet til hvordan norsk sikkerhet vil påvirkes av nye måter å utføre økonomisk statshåndverk på som følge av den teknologiske utviklingen.

Vi presiserer at eksisterende FFI-rapporter fremhever flere utfordringer og anbefalinger knyttet til den teknologiske utviklingen og norsk sikkerhet. I dette kapittelet fokuserer vi på konsekvenser av den teknologiske utviklingen for staters muligheter til å utføre økonomisk statshåndverk, mens vi henviser til øvrige rapporter ved FFI for ytterligere drøfting av implikasjonene av ny teknologi, utover koblingen til økonomisk statshåndverk, for norsk sikkerhet (se for eksempel Bentstuen mfl. 2018; Farsund mfl. 2022; Sellevåg mfl. 2020, 2021).

I utgangspunktet kan alle de potensielle endringene i økonomisk statshåndverk, som beskrevet i kapittel 4, påvirke norske sikkerhetsinteresser i årene fremover. I dette kapittelet velger vi imidlertid å fokusere spesielt på implikasjoner innen tre områder som vi vurderer er av særlig relevans for norsk sikkerhet. Det er: data som strategisk ressurs (delkapittel 5.1), nye eller økte avhengigheter knyttet til kompetanse, tjenester, råvarer, komponenter og/eller produkter (delkapittel 5.2) og rivaliseringen mellom USA og Kina (delkapittel 5.3). Vi oppsummerer kapittelet i delkapittel 5.4.

5.1 Data som strategisk ressurs

Data er en ny innsatsfaktor i både økonomisk og strategisk aktivitet, og ny teknologi vil medføre at mulighetene for datainnsamling øker. Norske aktører, både i det private næringslivet, det offentlige og blant befolkningen, produserer daglig store mengder data om alt fra økonomi, transport, helse og kultur til forsvar og sikkerhet. Tilgang til slike data gir muligheter til å oppnå innsikt om norsk samfunn, økonomi og forsvar. Fremmede stater kan potensielt få tak i data direkte gjennom økonomiske aktører som investerer i virksomheter med slike data, etablerer

[53] I Sikkerhetsloven (2018: § 1-5) er Norges nasjonale sikkerhetsinteresser definert som: «landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til: a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet, b) forsvar, sikkerhet og beredskap, c) forholdet til andre stater og internasjonale organisasjoner, d) økonomisk stabilitet og handlefrihet, e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet.» Vi har lagt til grunn utdypningen/tolkningen av hver sikkerhetsinteresse som redegjort for av NSM (2019).

inngangsportaler gjennom oppkjøp av underleverandører eller tjenesteleverandører til norske virksomheter, og/eller selv leverer produkter og tjenester til Norge.

Dersom fremmede stater får tilgang til data gjennom økonomisk aktivitet, kan det utgjøre en trussel mot flere av Norges nasjonale sikkerhetsinteresser.

For det første kan norsk suverenitet og «de øverste statsorganers virksomhet, sikkerhet og handlefrihet» potensielt bli truet dersom data om det norske samfunnet, norsk økonomi og/eller norske innbyggere utnyttes til å forsøke å påvirke (sær)interesser og oppfatninger i Norge, som drøftet i seksjon 4.2.1. Det er viktig at både norske myndigheter, det norske næringslivet og den norske befolkningen er bevisst på hvordan økonomiske transaksjoner kan være en måte å komme i posisjon til å utføre påvirkningsoperasjoner i fremtiden – enten ved at de økonomiske transaksjonene i realiteten er motivert av slike strategiske hensyn eller ved at transaksjonene er kommersielt motivert, men likevel åpner muligheter som kan utnyttes på et senere tidspunkt. Det er imidlertid viktig å være klar over at trusler mot norsk suverenitet og politisk handlefrihet vil avhenge av hva man mener med handlefrihet til å ta beslutninger.[54] I likhet med Lindgren, Waage og Boye (2022; se også Waage mfl. 2022), vurderer vi at det er behov for å forstå bedre, og konkretisere, hvilke former for påvirkning (muliggjort av økonomisk statshåndverk) som kan utgjøre en trussel mot norske myndigheters frihet til å ta politiske og administrative beslutninger – og hvilke former av påvirkning som heller bør forstås som «vanlig» påvirkning utført av stater i internasjonal politikk (se også Bergaust og Sellevåg 2022).

For det andre kan mulighetene til å utføre etterretningsvirksomhet gjennom økonomisk aktivitet i Norge (se seksjon 4.2.3) samt å trekke ut data fra nettverk norske aktører er en del av for etterretningsøyemed (i.e. panoptikon, se seksjon 4.2.6) øke med den teknologiske utviklingen. Slike handlinger kan både utgjøre en trussel mot Norges nasjonale sikkerhetsinteresser knyttet til «de øverste statsorganers virksomhet, sikkerhet og handlefrihet», «forsvar, sikkerhet og beredskap» og «forholdet til andre stater og internasjonale organisasjoner». Sikkerhetsloven skal i utgangspunktet beskytte sensitive og skjermingsverdige data. Økte muligheter for datainnsamling kombinert med avanserte analyseverktøy som kunstig intelligens som styrker evnen til å trekke ut innsikt fra dataene, kan imidlertid medføre at data som ikke dekkes av sikkerhetsloven likevel kan ha strategisk verdi for utenlandske etterretningsorganisasjoner.

For det tredje kan data fra offentlig og private virksomheter i Norge dessuten være viktig for å styrke bedrifter i avsenderlandet sine evner til å bedrive produktutvikling og -forbedring, og derigjennom hevde seg i global konkurranse. Hvis slike data blir benyttet av fremmede stater utenfor NATO-alliansen til å utvikle militær- eller flerbruksteknologi, som kunstig intelligens, vil det kunne utgjøre en trussel mot sikkerhetsinteressene «forsvar, sikkerhet og beredskap» og «forholdet til andre stater og internasjonale organisasjoner». Vi kommer tilbake til hvordan

[54] I den forbindelse utdyper NSM (2019: punkt 3.1.1) som følger: «Sikring av Norges suverenitet innebærer at det norske selvstyret skal sikres. Det skal sikres at lovlige norske myndigheter har frihet og eksklusiv rett til å beslutte om politiske og administrative tiltak i Norge, i henhold til norske interesser, og iverksette disse. Sikkerhetsloven skal bidra til å avdekke og forhindre at fremmed makt og andre som ikke har lovlig beslutningsmyndighet i Norge påvirker beslutninger på fordekte eller åpenlyse måter.»

spesielt rivaliseringen mellom USA og Kina vil kunne påvirke norske sikkerhetsinteresser i delkapittel 5.3.

For det fjerde kan både økonomiske og ikke-økonomiske data spille en viktig rolle for avsenderstaten i forbindelse med å utforme mer effektiv bruk av økonomiske virkemidler mot Norge, inkludert å identifisere sårbarheter dens økonomiske statshåndverk kan rettes inn mot. Vi vurderer at slik bruk av data i prinsippet kan utgjøre en trussel mot alle de fem nasjonale sikkerhetsinteressene som redegjort for i Sikkerhetsloven (2018: § 1-5), ved at det kan styrke avsenderstatens muligheter til å utføre målrettet påvirkning, undergraving og sabotasje.

På grunn av den strategiske og sikkerhetsmessige betydningen av data, anbefaler vi at norske myndigheter vurderer i hvilken grad eksisterende reguleringer og lovverk kan hindre uønskede aktører fra å få tilgang til data produsert av næringslivet, offentlig virksomhet og forbrukere i Norge. I den forbindelse fremhever vi at det kan være krevende å vite hvilke data som har verdi, og hvordan de kan bli brukt i dag og i fremtiden. For eksempel nevner Matz, Appel og Kosinski (2020) hvordan lokasjonsdata potensielt kan være tett knyttet til helsedata, og at lokasjonsdata dermed burde beskyttes selv om slike data i utgangspunktet ikke fremstår som like sensitive som helsedata. Dersom eksisterende reguleringer og lovverk ikke gir tilstrekkelig hjemmel til å ivareta sikkerhetsaspekter knyttet til data, anbefaler vi at det utredes hvordan, og i hvilken grad, det er mulig – både lovmessig og praktisk gjennomførbart – å styrke beskyttelsen av data.

5.2 Nye eller økte avhengigheter

5.2.1 Kompetanse og tjenester

Henrich (2016, 2017) omtaler en sosialt sammenkoblet gruppes totale kunnskaps- og ferdighetsbrønn for «den kollektive hjernen». Det er et nyttig begrep for å forstå begrensningene i forståelsen av og kunnskapen om ny teknologi i Norge. Selv om befolkningen er høyt utdannet, er den liten. Antallet sysselsatte personer er i april 2022 2,9 millioner mennesker.[55] Det er derfor sterke begrensninger på hva den norske arbeidsstokken vil kunne mestre av ny teknologi, og allerede i dag rapporterer 50 prosent av NHOs medlemsbedrifter at de mangler kompetanse innen IKT (NIFU 2022). Det vil bli vanskeligere å holde seg oppdatert og forstå teknologiske nyvinninger. Kompleksiteten og samspillet mellom ulike teknologier, som kunstig intelligens, 5G og tingenes internett, vil også øke fremover. Selv om Norge vil kunne ha miljøer i privat og offentlig sektor med dyp kunnskap om enkeltteknologier, vil det være tilnærmet umulig å forstå programvare, virkemåte og sammenkoblinger av produkter og tjenester som bygger på disse teknologiene nasjonalt. Det medfører at norsk næringsliv og norsk offentlig sektor må regne med å bli avhengig av utenlandske aktører for (videre)utvikling, drift og vedlikehold av produkter og tjenester, for eksempel gjennom tjenesteutsetting.

I kapittel 4 drøftet vi hvordan den teknologiske utviklingen kan resultere i at enkelte stater kan oppnå økt potensial til å akkumulere og utøve makt gjennom økonomisk statshåndverk ved å

[55] https://www.ssb.no/arbeid-og-lonn/sysselsetting/statistikk/arbeidskraftundersokelsen.

utnytte avhengigheter til kompetanse. Det kan true norske nasjonale sikkerhetsinteresser på flere måter. Dersom tjenesteutsetting gir fysisk eller digital tilgang til for eksempel sentrale deler av norsk økonomi, kritisk infrastruktur og norske data kan det åpne muligheter for etterretning- eller sabotasjevirksomhet, enten gjennom den økonomiske aktiviteten i seg selv eller ved å tilrettelegge for fremtidige cyber- eller påvirkningsoperasjoner. Sikkerhetsloven skal hindre uønskede aktører fra å få slik tilgang, men med økt sammenkobling og avhengigheter mellom produkter og tjenester, kan det være at det oppstår nye inngangsportaler, som ikke er dekket av sikkerhetsloven.

Videre kan økt avhengighet av kompetanse fra utlandet potensielt gi fremmede stater muligheter til å utøve press mot norske offentlige virksomheter eller aktører i næringslivet, for å forsøke å påvirke norsk politikk og beslutningstaking. Det kan potensielt true «de øverste statsorganers virksomhet, sikkerhet og handlefrihet», men vi minner igjen om at det er behov for å forstå bedre hvorvidt og når påvirkning og press ved bruk av økonomiske virkemidler bør klassifiseres som sikkerhetstruende virksomhet. Det kan potensielt også utgjøre en trussel mot «økonomisk stabilitet og handlefrihet» og «samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet», dersom vedlikehold eller oppdateringer av systemer og infrastruktur som understøtter finansielle transaksjoner og andre samfunnsfunksjoner bortfaller over en periode. Det krever imidlertid at en avsenderstat er i stand til å utøve kontroll over de kommersielle aktørene som leverer tjenestene. Sikkerhetsinteressen «forsvar, sikkerhet og beredskap» kan potensielt også bli truet av avhengighet av utenlandsk kompetanse på nye teknologier, dersom Norge blir sårbart overfor eventuelle brudd i forsyningslinjene av tjenester som er kritiske for Forsvaret.

Samlet vurderer vi at utnyttelse av Norges avhengigheter av kompetanse kan gi enkelte stater økte muligheter til å uføre økonomisk statshåndverk mot Norge på måter som potensielt truer norske nasjonale sikkerhetsinteresser. I lys av dette, anbefaler vi videre forskning for å kartlegge innenfor hvilke områder Norge spesielt vil være avhengig av utenlandske aktører og vurdere behov for tiltak som eventuelt kan redusere Norges kompetanseavhengigheter der avhengighetene særlig kan være sikkerhetstruende. For å kartlegge avhengigheter, kan offentlige data kombinert med intervjuer og spørreundersøkelser hos næringslivsaktører og offentlig sektor være aktuelle datakilder. Det vil også bli viktig fremover å sikre at fremmede stater ikke kan utnytte kompetanse og levering av tjenester som pressmidler i en situasjon der Forsvaret enten må beskytte norsk territorium eller bistå NATO-allierte.

5.2.2 Råvarer, komponenter og produkter

Den teknologiske utviklingen bidrar til at visse typer råvarer blir svært sentrale i økonomien fremover, som litium, kobolt og REE. Såfremt slike råvarer produseres mange steder globalt, vil norsk sårbarhet overfor press fra enkeltstater eller brudd i forsyningslinjene bilateralt mellom to stater, ha liten innvirkning på norsk sikkerhet. Kinas dominans innenfor produksjon av REE på 2000-tallet viste imidlertid verden at avhengighetene av slike råvarer kan utnyttes når markedsposisjonen er betydelig, selv om bruken av dette «våpenet» også bidro til at land med høy etterspørsel etter disse jordartene sørget for en diversifisering av importporteføljen (se seksjon 4.1.2).

Norge importerer også høyteknologiske produkter og komponenter, inkludert maskinvare og programvare for kunstig intelligens, 5G, tingenes internett og skytjenester samt produkter som

bygger på disse teknologiene. Det kan også skape avhengigheter til forsyning, dersom enkelte aktører og stater får en dominerende posisjon som leverandør til norsk næringsliv og offentlig sektor. Vi har i denne rapporten pekt på at produkter og tjenester med nettverkseffekter blir mer sentrale med fremveksten av ny teknologi og at betydningen av data for å utvikle og forbedre produkter og tjenester øker. Land med store befolkningsgrupper, som Kina og India, har en fordel både når det gjelder antall brukere av et produkt eller tjeneste og muligheter for å samle inn store mengder data. Fremskrivninger av disse landenes økonomiske fremtid tilsier at deres innenlandske forbrukermarkeder vil bli stadig viktigere globalt (se Lindgren, Hemnes og Waage 2022). Vi har også drøftet hvordan særlig Kina vokser frem som et land som i økende grad er i stand til å levere ressurser, kompetanse og produkter som understøtter avanserte teknologiske systemer, og hvordan kinesiske bedrifter i fremtiden kan bli sentrale leverandører av slike systemer. Samlet fører disse utviklingstrekkene, alt annet like, til at den kinesiske økonomien blir stadig viktigere for både norsk næringsliv og norsk offentlig sektor.[56] Uten aktiv politikk i Norge, USA og blant andre allierte (se delkapittel 5.3), vil norske bedrifter og offentlige virksomheter sannsynligvis vil bli mer avhengige av leveranser fra kinesiske bedrifter. Det kan også gjelde andre land utenfor det vestlige sikkerhetsfellesskapet (inklusive USAs asiatiske allierte).

Både norske avhengigheter til råvarer samt høyteknologiske produkter og komponenter kan i prinsippet utnyttes av en avsenderstat på måter som er sikkerhetstruende, ved å forstyrre eller strype forsyningen for å legge press og/eller sabotere viktige eller kritiske samfunnsfunksjoner (og eventuelt også forsvarsfunksjoner). Slik utøvelse av makt kan potensielt true flere av de norske nasjonale sikkerhetsinteressene som redegjort for i Sikkerhetsloven (2018: § 1-5). Innenfor omfanget av denne rapporten har vi ikke hatt muligheten til å undersøke hvordan norsk samfunn og økonomi avhenger av disse typene råvarer, produkter og komponenter. Som for kompetanseavhengigheter, anbefaler vi derfor at videre forskning søker å kartlegge avhengigheter og identifisere tiltak som kan bidra til å redusere avhengigheter som spesielt gjør Norge sårbart for andre staters bruk av økonomisk statshåndverk. For å forstå avhengigheter kan man for eksempel ta i bruk bilaterale, åpent tilgjengelige handelsdata og beregne indekser for ulike staters ressurskapabiliteter globalt, samt bilaterale avhengigheter som sier noe om hvilke land Norge (og andre land) er spesielt avhengige av forsyning fra. Vi utdyper om slike kapabilitets- og avhengighetsstudier i delkapittel 6.2.

5.3 Rivaliseringen mellom USA og Kina

Norges nasjonale sikkerhetsinteresser inkluderer «forholdet til andre stater og internasjonale organisasjoner» (Sikkerhetsloven 2018: § 1-5). Det omfatter at Norge har et velfungerende samarbeid med andre land og internasjonale organisasjoner om statssikkerhet, samt bidrar til å ivareta allierte staters sikkerhet (NSM 2019). Waage mfl. (2022) og Udal mfl. (2022) drøfter hvordan etterretningsvirksomhet, teknologioverføring fra norske selskaper eller posisjonering for å utføre fremtidig sabotasje kan lede til at Norges samarbeid med andre land om statssikkerhet blir svekket. I tillegg kan det utgjøre en trussel mot allierte staters sikkerhet. Vi vurderer at den

[56] Merk imidlertid at dersom Norge i samarbeid med likesinnede land eller allierte innfører aktiv politikk for å gjøre seg mer uavhengig av kinesiske aktører, kan dette vise seg å ikke stemme.

teknologiske utviklingen medfører ytterligere implikasjoner for norske sikkerhetsinteresser knyttet til «forholdet til andre stater og internasjonale organisasjoner», spesielt USA.

Det er stor debatt i faget internasjonal politikk om USAs rolle i verden fremover, fremveksten av Kina som økonomisk og militær stormakt og fremtiden til sino-amerikanske relasjoner. Noen argumenterer for at USA burde trekke seg tilbake (Mearsheimer og Walt 2016; Posen 2014), mens andre mener USA skal fortsette å være dypt engasjert globalt (Brooks, Ikenberry og Wohlforth 2012; Brooks og Wohlforth 2016). Det virker sannsynlig at USA fortsatt vil være en globalt engasjert supermakt. Men fokuset vil fortsette å flytte seg mot Øst-Asia. Mens USA i flere tiår har ført en involveringspolitikk (*engagement*) for å sørge for at Kina blir en ansvarlig bidragsyter i den internasjonale orden (Zoellick 2005), er det lite som minner om akademisk støtte til denne politikken nå (Campbell og Ratner 2018; Friedberg 2018; Harding 2015; Jisi mfl. 2018; Mattis 2018). Det er nå bred amerikansk politisk og akademisk enighet om å forstå Kina som en utfordrer til den USA-ledede verdensorden (Shifrinson 2018). Det er stor debatt om Kina virkelig kan eller vil kunne utfordre USA. Noen argumenterer for at Kina vil være i stand til å gjøre det og at krig derfor er mer sannsynlig enn usannsynlig med dagens politikk i Washington og Beijing (Allison 2015; Mearsheimer 2014). Andre mener USA vil fortsette å være den viktigste økonomien og stormakten i verden (Beckley 2008, 2012, 2020; Cox 2012) og at risikoen for krig mellom Washington og Beijing er overdrevet. Uavhengig av hva man mener om Kinas evne til å bli en mer sentral stormakt enn USA, er det klart at Kinas fortsatte økonomiske, teknologiske og militære fremgang, samt deres mer selvhevdende (*assertive*) utenrikspolitikk regionalt og globalt, har bidratt til rivalisering – en superkonflikt (Tunsjø 2020), altså en konflikt mellom supermaktene USA og Kina. Denne utviklingen modnet frem under President Trump, fortsetter under President Biden, og vil sannsynligvis fortsette i årene fremover.

Rivaliseringen mellom USA og Kina vil ha konsekvenser for Norge. Norge er medlem av NATO-alliansen og USA er Norges fremste sikkerhetsgarantist. Hvis Beckley (2022) har rett i sin analyse, vil USA legge press på sine allierte til å «velge side, overtale dem til å omdirigere forsyningskjeder og omfavne [det amerikanske] økosystemet av teknologier og standarder». Det er mulig rivaliseringen mellom Kina og USA blir mindre dramatisk enn dette, men Norge må uansett forvente å bli trukket mer med i politiske og økonomiske forsøk på å demme opp for den kinesiske økonomiske og teknologiske fremgangen. NATOs (2022: 5) nye strategiske konsept nevner Kina som en utfordrer for første gang: «Folkerepublikken Kinas (PRC) uttalte ambisjoner og tvangspolitikk utfordrer våre interesser, sikkerhet og verdier». NATO (2022) peker på at Kinas politiske, økonomiske og militære virkemidler har globalt nedslag, ødeleggende hybride, cyber- og påvirkningsoperasjoner, mål om å kontrollere teknologiske og industrielle sektorer, skape avhengigheter, forsøk på å underminere den regelbaserte orden og utdyping av det strategiske partnerskapet med Russland som grunnlag for hvordan Kina utfordrer alliansens interesser, sikkerhet og verdier. NATO (2022: 5,7) argumenterer for at fremvoksende og disruptive teknologier «endrer konflikters karakter, får større strategisk betydning og blir nøkkelarenaer for global konkurranse» og at NATO vil promotere innovasjon og beskytte «våre innovasjonsøkosystemer».

For å ivareta norske nasjonale sikkerhetsinteresser knyttet til «forholdet til andre stater og internasjonale organisasjoner» kan det derfor bli viktigere fremover at Norge beskytter norsk (og alliert) teknologi og data (se også delkapittel 5.1) samt bidrar i satsningen på norsk (og alliert) næringsvirksomhet innen viktige høyteknologiske industrier. For eksempel fremhever det amerikanske forsvarsdepartementets 5G-strategimplementeringsplan hvordan amerikansk samarbeid med allierte land og andre partnere for å hindre «uautorisert utenlandsk tilgang» til 5G-infrastrukturen er ett av fire prioriterte innsatsområder (*lines of effort*) (Department of Defense 2020: 2, 15). I den forbindelse virker det også sannsynlig at det vil bli økt press på norske virksomheter til å bli mindre avhengige av kinesiske leverandører og verdikjeder, og til å redusere Kinas tilgang til ressurser, komponenter og kompetanse som styrker og fremmer kinesisk teknologiutvikling. Det ligger utenfor omfanget av dette oppdraget å gjennomføre en grundig evaluering av implikasjonene for norsk økonomi og sikkerhet av teknologirivaliseringen mellom USA og Kina, som kan styrke beslutningsgrunnlaget for norske myndigheters politikk og lovgivning på feltet. Vi anbefaler derfor videre forskning på de økonomiske og sikkerhetsmessige konsekvensene av teknologirivaliseringen for en småstat som Norge, som er avhengig av handel og investeringer i teknologi, råvarer, kunnskap og andre ressurser med andre land. Herunder anbefaler vi også å øke kunnskapen om den norske økonomiens avhengighet til Kina per dags dato, for eksempel gjennom analyser av økonomiske data og intervjuer med næringslivsaktører (se også delkapittel 5.2).

5.4 Oppsummering av kapittelet

I dette kapittelet har vi drøftet implikasjoner av rapportens analyser for norsk sikkerhet, med utgangspunkt i de nasjonale sikkerhetsinteressene som definert i Sikkerhetsloven (2018: § 1-5). Vi argumenterer for at data fra norsk næringsliv, offentlig virksomhet og samfunn vil være av interesse for fremmede stater og må behandles og ivaretas som en strategisk ressurs. Vi anbefaler at norske myndigheter vurderer i hvilken grad eksisterende reguleringer og lovverk kan hindre uønskede aktører fra å få tilgang til data produsert av næringslivet, offentlig virksomhet og forbrukere i Norge – eventuelt at det utredes hvordan, og i hvilken grad, det er mulig å styrke beskyttelsen av data. Videre bidrar ny teknologi til at Norge kan bli mer avhengig av visse typer kompetanse, tjenester, råvarer, komponenter og produkter, som potensielt kan utnyttes av enkelte andre stater i deres økonomiske statshåndverk mot Norge. I første omgang anbefaler vi at Norge får bedre oversikt over hva slags avhengigheter som er kritisk for norsk sikkerhet og hvem som leverer dette til Norge. Deretter diskuterer vi hvordan rivaliseringen mellom USA og Kina sannsynligvis også vil smitte over på Norge ved at det blant annet blir økt press fra USA og NATO om å beskytte og fremme egen teknologi samt skape større uavhengighet fra kinesiske leverandører i høyteknologiske forsyningskjeder. Det er dette som i eksisterende litteratur blir kalt «det nye økonomiske statshåndverket», og vi tror det vil bli viktigere fremover, også for Norge.

6 Oppsummering

6.1 Oppsummering av rapporten

Globalisering av verdens økonomier, økt betydning av internasjonale finansmarkeder, digitalisering og fremvoksende økonomier, herunder spesielt Kinas, økende sentralitet i verdensøkonomien, har transformert staters evne til å benytte økonomiske virkemidler for å fremme sine interesser i internasjonal politikk. Vi kaller slik statlig virkemiddelbruk økonomisk statshåndverk (*economic statecraft*). Den teknologiske utviklingen under den fjerde industrielle revolusjonen vil endre hvordan stater kan ta i bruk økonomiske virkemidler, men eksisterende litteratur om økonomisk statshåndverk har i liten grad tatt inn over seg konsekvenser av ny teknologi. Formålet med denne rapporten er å redusere dette gapet i eksisterende forskning ved å styrke forståelsen av hvordan den teknologiske utviklingen kan påvirke staters evne til å ta i bruk økonomiske virkemidler og å drøfte implikasjoner for norsk sikkerhet. Formålet omhandler imidlertid komplekse og omfattende temaer, som det vil kreve mer ressurser å oppnå fullstendig innsikt i enn hva som var tilgjengelig i oppdraget som ligger til grunn for denne rapporten. Rapporten danner et grunnlag som nye studier kan bygge videre på.

Gjennom intervjuer og en workshop med forskere ved FFI samt gjennomgang av eksisterende litteratur, har rapporten søkt å besvare tre problemstillinger: 1) hvordan kan den teknologiske utviklingen i 4IR påvirke økonomisk aktivitet på måter som former mulighetsrommet for økonomisk statshåndverk?, 2) hvordan kan den teknologiske utviklingen endre mulighetsrommet for staters bruk av økonomisk statshåndverk?, og 3) hva kan implikasjonene være for norsk sikkerhet? Vi har fokusert på teknologier som løftes frem som særdeles viktige innen den teknologiske utviklingen i eksisterende forskning ved FFI, og som vi vurderer vil kunne ha størst implikasjoner for staters muligheter til å bruke økonomisk statshåndverk. Disse teknologiene er: kunstig intelligens og stordata, 5G, skytjenester og tingenes internett. Der det er relevant, trekker vi imidlertid også inn andre teknologier i diskusjonen.

Vi identifiserer flere måter disse teknologiene potensielt påvirker økonomisk aktivitet. Økonomisk aktivitet vil igjen påvirke staters evne til å ta i bruk økonomisk statshåndverk. Noen av utviklingstrekkene kan vi identifisere fra samfunnsøkonomisk litteratur, mens andre fremkommer av eksisterende forskning ved FFI. For det første øker betydningen av tilgang til data for å utvikle og forbedre produkter og tjenester. For det andre blir produkter, tjenester og systemer mer komplekse. For det tredje stilles det høyere krav til kompetanse for å anskaffe, utvikle, drifte og vedlikeholde produkter og systemer, som resulterer i at bedrifter i økende grad har behov for å sette ut tjenester til andre selskaper som besitter nødvendig kunnskap og kompetanse på området. For det fjerde er det flere forhold ved den teknologiske utviklingen som både driver økt markedskonsentrasjon, organisasjonsendringer og økt internasjonalisering av arbeidsoppgaver som tidligere ble utført lokalt. For det femte blir både arbeidsoppgaver og beslutningstaking i økende grad utført av maskiner i stedet for mennesker, noe som medfører økt avhengighet av maskiner i hverdagen. Og for det sjette kan fremvoksende markeders demografiske og

økonomiske utvikling, i takt med den teknologiske utviklingen, gjøre selskaper mer avhengig av markedstilgang til disse markedene for å hevde seg i internasjonal konkurranse.

Forståelsen av hvordan den teknologiske utviklingen kan påvirke økonomisk aktivitet, lar oss i neste omgang drøfte hvordan staters muligheter til å utføre økonomisk statshåndverk potensielt blir endret av teknologiske fremsteg. Vi skiller mellom økonomisk statshåndverk hvor avsenderstaten utøver makt og økonomisk statshåndverk som resulterer i at avsenderstaten akkumulerer økt økonomisk – eller annen – makt som muliggjør fremtidig virkemiddelbruk, også med ikke-økonomiske virkemidler (f.eks. cyberoperasjoner).

Vi finner at den teknologiske utviklingen kan påvirke økonomisk statshåndverk på flere måter. Innen utøvelse av makt, vil den teknologiske utviklingen kunne styrke enkelte avsenderstaters muligheter for å utnytte avhengigheter til kompetanse, ressurser, komponenter, osv. til (fordekt) å sabotere systemer. Innen akkumulering av makt, vurderer vi at den teknologiske utviklingen særlig vil styrke mulighetene til å utnytte økonomisk aktivitet til å hente inn informasjon og data, til bruk i etterretningsformål og/eller til å forsøke å forme (sær)interesser og oppfatninger i mottakerlandet (f.eks. gjennom skreddersydde politiske budskap eller spredning av (des)-informasjon). Datainnsamling, også gjennom åpne kilder, kombinert med avanserte analyseverktøy som kunstig intelligens, kan dessuten potensielt benyttes til å gjøre bruken og innrettingen av en stats økonomiske statshåndverk mer effektiv. Enkelte stater kan i tillegg oppnå økte muligheter til å etablere seg som en sentral leverandør av viktige ressurser, produkter og kompetanse som følge av den teknologiske utviklingen, og slike avhengigheter kan i neste omgang åpne muligheter for strategisk bruk for å fremme disse statenes interesser globalt. Vi tar også med oss at sårbarheter for sabotasjeforsøk mot infrastruktur generelt ser ut til å øke med den teknologiske utviklingen, blant annet på grunn av flere angrepspunkter og økt automatisering av arbeidsoppgaver. I den forbindelse kan økonomiske virkemidler være en måte å komme i posisjon til å utføre sabotasje, enten gjennom eierskapskontroll eller ved å tilrettelegge for fremtidig sabotasje spesielt i cyberdomenet (f.eks. ved programvareoppdateringer av leverte systemer).

Vi retter også oppmerksomhet mot det «nye» økonomiske statshåndverket, hvor det som i utgangspunktet er innenlandsk næringspolitikk, men som i voksende grad er geopolitisk motivert, også burde inkluderes i forståelsen av økonomisk statshåndverk. I dette perspektivet brukes økonomiske virkemidler til å fremme og beskytte egen teknologi- og industriutvikling. Teknologirivaliseringen mellom USA og Kina har gitt opphav til det økte fokuset på denne formen for økonomisk statshåndverk over de senere årene.

Hva har innsikten om den teknologiske utviklingens påvirkning på staters muligheter til å utføre økonomisk statshåndverk å si for Norge og norsk sikkerhet? For det første vil dataene som produseres i det norske samfunnet være av interesse for fremmede stater, og vi tror at den teknologiske utviklingen vil gjøre data til en stadig viktigere ressurs i økonomisk statshåndverk. Vi anbefaler at norske myndigheter vurderer i hvilken grad eksisterende reguleringer og lovverk kan hindre uønskede aktører fra å få tilgang til data produsert av næringslivet, offentlig virksomhet og forbrukere i Norge. For det andre bidrar ny teknologi til at Norge kan bli mer avhengig av visse typer kompetanse, tjenester, råvarer, komponenter og produkter. Disse avhengighetene kan gjøre enkelte staters muligheter til å utnytte økonomiske statshåndverk mot

Norge mer potent. I første omgang anbefaler vi at Norge får bedre oversikt over hva slags kompetanse, tjenester, råvarer, komponenter og produkter som er kritisk for norsk sikkerhet og hvem som leverer dette til Norge. For det tredje mener vi det er sannsynlig at rivaliseringen mellom USA og Kina i økende grad også vil ha implikasjoner for Norge, blant annet ved at det blir økt press fra USA og NATO om å beskytte norsk (og alliert) teknologi og skape større uavhengighet fra kinesiske leverandører i høyteknologiske forsyningskjeder. Vi anbefaler at norske myndigheter styrker forskningen på økonomiske og sikkerhetsmessige konsekvenser av rivaliseringen for en småstat som Norge.

For å håndtere potensielt sikkerhetstruende konsekvenser av fremmede staters bruk av økonomisk statshåndverk mot Norge som følge av den teknologiske utviklingen, vurderer vi at det er behov for å styrke evnen til å koordinere på tvers av domener og sektorer nasjonalt. For eksempel spenner endringene og implikasjonene vi har drøftet i denne rapporten på tvers av tradisjonelle fagfelt som internasjonal økonomi og cybersikkerhet. Vi tror også det vil bli økt behov for internasjonalt samarbeid rundt å håndtere potensielle negative sikkerhetskonsekvenser av økonomisk aktivitet, blant annet fordi den teknologiske utviklingen gjør det lettere å komme i posisjon til å spionere eller sabotere ved å utnytte kommersielle aktører i et tredjeland. For eksempel kan potensielt investeringer og oppkjøp i Tyskland eller Sverige i større grad enn før ha negative sikkerhetskonsekvenser for Norge. Fremover vil det også være viktig å spre kunnskap til næringslivsaktører og forbrukere om hvilken rolle økonomisk aktivitet kan spille i å tilrettelegge for datainnsamling, etterretning, påvirkning og sabotasje, slik at eventuelle forsøk på sikkerhetstruende virksomhet blir forebygget eller oppdaget.

6.2 Videre studier

I denne rapporten har vi begynt å utforske koblingen mellom teknologisk utvikling og staters muligheter for å utføre økonomisk statshåndverk. Det gjenstår mange ubesvarte spørsmål som videre studier kan søke å besvare.

Noen av spørsmålene har vi allerede omtalt tidligere i rapporten. Selv om vi identifiserer mange årsaker til at den teknologiske utviklingen ser ut til å øke (enkelte) staters potensial til å kunne ta i bruk økonomiske virkemidler i kapittel 4, vurderer vi at det også er behov for å forstå bedre hvilke utfordringer den teknologiske utfordringen kan føre til for bruken av økonomisk statshåndverk. Spesielt anbefaler vi videre studier å fokusere på: 1) statens evne til å utøve kontroll over økonomiske aktører i lys av den teknologiske utviklingen, herunder hvordan ny teknologi påvirker markedskonsentrasjon, organisasjonsformer og graden av internasjonalisering, 2) på hvilke måter kompleksitet forbundet med ny teknologi kan gjøre det mer utfordrende for avsenderstaten å utøve økonomisk statshåndverk, og 3) på hvilke måter den teknologiske utviklingen kan bidra til å redusere mottakerlandets sårbarheter ovenfor avsenderstatens økonomiske statshåndverk.

I denne rapporten identifiserte vi også flere gap og utfordringer i eksisterende litteratur i delkapittel 2.3, som vil være relevante temaer for videre studier.

For det første noterte vi oss at det er en skjevhet i litteraturen om økonomisk statshåndverk – med eller uten ny teknologi – i retning av stormakter som USA og Kina. Nye studier kan derfor undersøke grundigere hvordan små og mellomstore staters muligheter for å benytte økonomiske virkemidler potensielt endrer seg som følge av den teknologiske utviklingen enn hva som har vært mulig innenfor rammene av dette oppdraget. Slike studier kan bidra til å identifisere hvilke muligheter Norge har til både å beskytte seg mot andre staters økonomiske statshåndverk og å fremme egne interesser ved utnyttelse av økonomiske virkemidler.

For det andre fremhevet vi hvordan det mangler en helhetlig, systematisk og kvantitativ oversikt over ulike staters økonomiske og teknologiske kapabiliteter. Slike beregninger har imidlertid allerede blitt utledet i forskningslitteraturen for utvalgte lands finanskapabiliteter (Armijo, Tirone, og Chey 2020; se også Lindgren, Hemnes og Waage 2022), og vi anbefaler en utvidelse til å dekke alle deler av lands økonomiske statshåndverkskapabiliteter, ikke kun finansielle kapabiliteter. For teknologiske kapabiliteter kan det være relevant å utarbeide indekser for egenskaper slik som patenter innen 4IR-teknologier (kunstig intelligens, tingenes internett, skytjenester, 5G, m.m.), universiteter høyt oppe på relevant rangeringslister, antall forskere, antall publikasjoner i aktuelle topptidsskrifter (Science, Nature, osv.), antall siteringer, og lignende.

Videre anbefaler vi å utvikle en metode for å estimere lands avhengigheter av økonomiske innsatsfaktorer som varer, tjenester, finans, teknologi og humankapital fra andre land. Det vil gi mer informasjon om hvor Norge er sårbart overfor andre lands bruk av økonomisk statshåndverk, spesielt de typene virkemidler der makten er noenlunde proporsjonal med størrelsen på den økonomiske interaksjonen. Kapabilitets- og avhengighetsanalysene vil samlet styrke innsikten i ulike lands muligheter til å utnytte ulike strategier av økonomisk statshåndverk, også sett opp mot ny teknologi. Mens avhengighetsperspektivet vil si noe om lands økonomiske avhengighet til et annet land, vil kapabilitetstilnærmingen tilby et anslag på et lands potensial for økonomisk statshåndverk, inkludert ved å utnytte ny teknologi, på generelt grunnlag.

Til slutt anbefaler vi også at nye studier fokuserer på et bredere utvalg av teknologier som kjennetegner 4IR i tillegg til de fire teknologiene som har vært i fokus i denne rapporten (kunstig intelligens, 5G, skytjenester og tingenes internett). Det kan avdekke nye måter den teknologiske utviklingen potensielt påvirker økonomisk aktivitet og økonomisk statshåndverk som ikke har blitt analysert i arbeidet med denne rapporten.

Forkortelser

4IR	Den fjerde industrielle revolusjonen
5G	Femte generasjons mobilnett
BNP	Bruttonasjonalprodukt
FFI	Forsvarets forskningsinstitutt
IKT	Informasjons- og kommunikasjonsteknologi
IoT	Tingenes internett
IT	Informasjonsteknologi
JD	Justis- og beredskapsdepartementet
KI	Kunstig intelligens
ML	Maskinlæring
NSM	Nasjonal sikkerhetsmyndighet
REE	Sjeldne jordarter (*rare earth elements*)
RMB	Kinesiske renminbi
USD	Amerikanske dollar

Referanser

Acemoglu, Daron og Pascual Restrepo. 2018. «The Race between Man and Machine: Implications of Technology for Growth, Factor Shares, and Employment». *American Economic Review* 108(6): 1488–1542.

Aggarwal, Vinod K og Tim Marple. 2020. «Digital Currency Wars? US-China Competition and Economic Statecraft». 15(4): 78–85.

Aggarwal, Vinod K. og Andrew W. Reddie. 2018. «Comparative Industrial Policy and Cybersecurity: A Framework for Analysis». *Journal of Cyber Policy* 3(3): 291–305.

Aggarwal, Vinod K. og Andrew W. Reddie. 2020. «New Economic Statecraft: Industrial Policy in an Era of Strategic Competition». *Issues & Studies* 56(02): 2040006.

Aggarwal, Vinod K. og Andrew W. Reddie. 2021. «Economic Statecraft in the 21st Century: Implications for the Future of the Global Trade Regime». *World Trade Review* 20(2): 137–51.

Aghion, Philippe, Benjamin F. Jones og Charles I. Jones. 2019. «Artificial Intelligence and Economic Growth». I *The Economics of Artificial Intelligence: An Agenda*, red. Ajay Agrawal, Joshua S. Gans og Avi Goldfarb. Chicago: Chicago University Press, 237–90.

Agrawal, Ajay, Nicola Lacetera og Elizabeth Lyons. 2016. «Does Standardized Information in Online Markets Disproportionately Benefit Job Applicants from Less Developed Countries?» *Journal of International Economics* 103: 1–12.

Aho, Brett og Roberta Duffield. 2020. «Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China». *Economy and Society* 49(2): 187–212.

Akerman, Anders, Edwin Leuven og Magne Mogstad. 2022. «Information Frictions, Internet, and the Relationship between Distance and Trade». *American Economic Journal: Applied Economics* 14(1): 133–63.

Akter, Shahriar mfl. 2020. «Transforming Business Using Digital Innovations: The Application of AI, Blockchain, Cloud and Data Analytics». *Annals of Operations Research*. https://doi.org/10.1007/s10479-020-03620-w (1. august 2021).

Allison, Graham. 2015. «The Thucydides Trap: Are the U.S. and China Headed for War?» *The Atlantic*.

Andås, Harald. 2020. *Emerging Technology Trends for Defence and Security*. Forsvarets forskningsinstitutt. FFI-rapport 20/01050.

Armijo, Leslie Elliott, Daniel C. Tirone og Hyoung-kyu Chey. 2020. «The Monetary and Financial Powers of States: Theory, Dataset, and Observations on the Trajectory of American Dominance». *New Political Economy* 25(2): 174–94.

Autor, David mfl. 2020. «The Fall of the Labor Share and the Rise of Superstar Firms». *The Quarterly Journal of Economics* 135(2): 645–709.

Ayres, Ian. 2007. *Super Crunchers – How Anything Can Be Predicted*. John Murray Publishers Ltd.

Baldwin, David A. 1971. «The Power of Positive Sanctions». *World Politics* 24(1): 19–38.

Baldwin, David A. 1985. *Economic Statecraft*. Princeton, NJ: Princeton University Press.

Baumol, William J. 1967. «Macroeconomics of Unbalanced Growth: The Anatomy of Urban Crisis». *The American Economic Review* 57(3): 415–26.

Beadle, Alexander William og Sverre Diesen. 2015. *Globale trender mot 2040 - implikasjoner for Forsvarets rolle og relevans*. Forsvarets forskningsinstitutt. FFI-rapport 15/01452.

Beadle, Alexander William, Sverre Diesen, Tore Nyhamar og Eline Knarrum Bostad. 2019. *Globale trender mot 2040 - et oppdatert fremtidsbilde*. Forsvarets forskningsinstitutt. FFI-rapport 19/00045.

Beckley, Michael. 2008. *Unrivaled: Why America Will Remain the World's Sole Superpower*. Ithaca, NY: Cornell University Press.

Beckley, Michael. 2012. «China's Century? Why America's Edge Will Endure». *International Security* 36(3): 41–78.

Beckley, Michael. 2020. «Conditional Convergence and the Rise of China: A Political Economy Approach to Understanding Global Power Transitions». *Journal of Global Security Studies*. https://academic.oup.com/jogss/advance-article/doi/10.1093/jogss/ogaa010/5754022 (17. juli 2020).

Beckley, Michael. 2022. «Enemies of My Enemy: How Fear of China Is Forging a New World Order». *Foreign Affairs* 101(2): 68–85.

Bentstuen, Ole Ingar. 2020. «5G – evner vi å håndtere kompleksiteten?» Presentert på Inside Telecom konferansen 2020, Oslo, 6. oktober.

Bentstuen, Ole Ingar. 2022. *Trender innen IKT – relatert til militærmakt*. Forsvarets forskningsinstitutt. FFI-rapport 22/00544.

Bentstuen, Ole Ingar, Bodil Hvesser Farsund, Lasse Øverlier og Geir Køien. 2018. *Sikkerhetsutfordringer i fremtidens EKOM-tjenester*. Forsvarets forskningsinstitutt. FFI-rapport 17/17047.

Benzell, Seth og Erik Brynjolfsson. 2019. *Digital Abundance and Scarce Genius: Implications for Wages, Interest Rates, and Growth*. Cambridge, MA: National Bureau of Economic Research. http://www.nber.org/papers/w25585.pdf (2. juli 2019).

Bergaust, Julie Celine og Stig Rune Sellevåg. 2022. «Dissecting and revising: A systematic conceptualisation of hybrid interference». Forsvarets forskningsinstitutt. Artikkelutkast.

Bergh, Arild. 2019. *Social Network Centric Warfare – Understanding Influence Operations in Social Media*. Forsvarets forskningsinstitutt. FFI-rapport 19/01194.

Bergh, Arild. 2020. *Påvirkningsoperasjoner i sosiale medier – oversikt og utfordringer*. Forsvarets forskningsinstitutt. FFI-rapport 20/01694.

Birkemo, Gunn Alice, Petter Kristiansen og Bodil Hvesser Farsund. 2021. *Risiko ved strategisk samarbeid innen IKT – rammeverk og vurdering*. Forsvarets forskningsinstitutt. FFI-rapport 21/00527. Unntatt offentlighet.

Blackwill, Robert D. og Jennifer M. Harris. 2016. *War by Other Means: Geoeconomics and Statecraft*. Cambridge, MA: Harvard University Press.

Bloom, Nicholas, Luis Garicano, Raffaella Sadun og John Van Reenen. 2014. «The Distinct Effects of Information Technology and Communication Technology on Firm Organization». *Management Science* 60(12): 2859–85.

Bloom, Nicholas, Charles I. Jones, John Van Reenen og Michael Webb. 2020. «Are Ideas Getting Harder to Find?» *American Economic Review* 110(4): 1104–44.

Bodamer, Florian David og Kaija E. Schilde. 2021. «Weaponized Weapons». I *The Uses and Abuses of Weaponized Interdependence*, Brookings Institution Press, 203–20.

Bresnahan, Timothy F. og Manuel Trajtenberg. 1995. «General Purpose Technologies 'Engines of Growth'?» *Journal of Econometrics* 65: 83–108.

Brooks, Stephen G., G. John Ikenberry og William C. Wohlforth. 2012. «Don't Come Home, America: The Case against Retrenchment». *International Security* 37(3): 7–51.

Brooks, Stephen G. og William C. Wohlforth. 2016. *America Abroad: The United States' Global Role in the 21st Century*. Oxford: Oxford University Press.

Brummer, Matthew. 2020. «Innovation and Threats». *Defence and Peace Economics* 0(0): 1–22.

Bruvoll, Janita A, Monica Endregard og Odd Busmundrud. 2020. *Kritiske samfunnsfunksjoner – en framgangsmåte for status- og tilstandsvurderinger*. Forsvarets forskningsinstitutt. FFI-rapport 20/02355.

Bruvoll, Janita A, Aasmund Thuv og Geir Enemo. 2020. *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene*. Forsvarets forskningsinstitutt. FFI-rapport 20/01560.

Campbell, Kurt M. og Ely Ratner. 2018. «The China Reckoning: How Beijing Defied American Expectations». *Foreign Affairs* 97(2): 60–70.

Chiu, Dominic. 2017. *The East Is Green: China's Global Leadership in Renewable Energy*. Center for Strategic & International Studies. New Perspectives in Foreign Policy Issue 13, Summer 2017. https://www.csis.org/east-green-chinas-global-leadership-renewable-energy (5. juli 2022).

Christensen, Clayton M. 1997. *The innovator's dilemma: When new technologies cause great firms to fail*. Cambridge, MA: Harvard Business School Press.

Clarke, Michael, Matthew Sussex og Nick Bisley, red. 2020. *The Belt and Road Initiative and the Future of Regional Order in the Indo-Pacific*. New York, NY: Lexington Books.

Cockburn, Iain M., Rebecca Henderson og Scott Stern. 2018. *The Impact of Artificial Intelligence on Innovation*. Cambridge, MA: National Bureau of Economic Research. NBER Working Paper Series.

Cohen, Benjamin J. 2009. «Sovereign Wealth Funds and National Security: The Great Tradeoff». *International Affairs* 85(4): 713–31.

Cohen, Benjamin J. 2019. *Currency Statecraft: Monetary Rivalry and Geopolitical Ambition*. Chicago: University of Chicago Press.

Cox, Michael. 2012. «Power Shifts, Economic Change and the Decline of the West?» *International Relations* 26(4): 369–88.

Cremér, Jacques, Yves-Alexandre de Montjoye og Heike Schweitzer. 2019. *Competition Policy For the Digital Era*. Directorate-General for Competition. Final report for the European Commission.

Crouzet, Nicolas og Janice Eberly. 2018. «Intangibles, Investment, and Efficiency». *AEA Papers and Proceedings* 108: 426–31.

Daugherty, Paul R. og H. James Wilson. 2018. *Human + Machine: Reimagining Work in the Age of AI*. Harvard Business Review Press.

De Loecker, Jan, Jan Eeckhout og Gabriel Unger. 2020. «The Rise of Market Power and the Macroeconomic Implications*». *The Quarterly Journal of Economics* 135(2): 561–644.

Department of Defense. 2018. «Summary of the 2018 Department of Defense Artificial Intelligence Strategy – Harnessing AI to Advance Our Security and Prosperity.»

Department of Defense. 2020. «Department of Defense 5G Strategy Implementation Plan».

Diamond, Peter A. 1971. «A Model of Price Adjustment». *Journal of Economic Theory* 3(2): 156–68.

Diesen, Sverre. 2018. *Lavintensivt hybridangrep på Norge i en fremtidig konflikt*. Forsvarets forskningsinstitutt. FFI-rapport 18/00080.

Dombrowski, Peter J. og Eugene Gholz. 2006. *Buying military transformation: Technological innovation and the defense industry*. New York, NY: Columbia University Press.

Dombrowski, Peter J. og Eugene Gholz. 2009. «Identifying Disruptive Innovation Innovation Theory and the Defense Industry». *Innovations: Technology, Governance, Globalization* 4(2): 101–18.

Domingos, Pedro. 2015. *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*. London: Basic Books.

Drezner, Daniel W. 1998. «Conflict Expectations and the Paradox of Economic Coercion». *International Studies Quarterly* 42(4): 709–31.

Drezner, Daniel W. 2008. «Sovereign Wealth Funds and the (In)Security of Global Finance». *Journal of International Affairs* 62(1): 115–30.

Drezner, Daniel W., Henry Farrell og Abraham L. Newman, red. 2021. *The Uses and Abuses of Weaponized Interdependence*. Washington, D.C.: Brookings Institution Press.

Duffie, Darrell. 2022. «Can China Conquer Crypto? Beijing's Dangerous Quest to Control Digital Currencies». *Foreign Affairs*.

Early, Bryan R. og Menevis Cilizoglu. 2020. «Economic Sanctions in Flux: Enduring Challenges, New Policies, and Defining the Future Research Agenda». *International Studies Perspectives* 21(4): 438–77.

Ernst, Dieter og Linsu Kim. 2002. «Global Production Networks, Information Technology and Knowledge Diffusion». *Industry and Innovation* 9(3): 147–53.

Esposito, Christian mfl. 2018. «On the Disaster Resiliency within the Context of 5G Networks: The RECODIS Experience».

Farrell, Henry og Abraham L. Newman. 2019. «How Global Economic Networks Shape State Coercion». *International Security* 44(1): 42–79.

Farsund, Bodil Hvesser mfl. 2022. *Utviklingen av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet (revidert rapport)*. Forsvarets forskningsinstitutt. FFI-rapport 22/00631.

Farsund, Bodil Hvesser, Anne Marie Hegland og Frode Lillevold. 2016. *LTE i Forsvaret – sårbarheter knyttet til ulike forretningsmodeller*. Forsvarets forskningsinstitutt. FFI-rapport 16/00808.

Fauske, Maria Fleischer. 2020. *Automatisering i fremtidens arbeidsliv – hva sier forskningen?* Forsvarets forskningsinstitutt. FFI-rapport 20/03037.

Fidler, Mailyn. 2018. «African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts». *Council on Foreign Relations*. https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts (23. mai 2022).

Fjellvåg, Helmer. 2022. «sjeldne jordarter». *Store norske leksikon*. http://snl.no/sjeldne_jordarter (15. juli 2022).

Flaaten, Geir. 2021. «Historisk vedtak: Nå er Bergen Engines-salget offisielt stanset». *E24*. https://e24.no/norsk-oekonomi/i/OQ73Qb/historisk-vedtak-naa-er-bergen-engines-salget-offisielt-stanset (11. februar 2022).

Friedberg, Aaron L. 2018. «Competing with China». *Survival* 60(3): 7–64.

Garicano, Luis. 2000. «Hierarchies and the Organization of Knowledge in Production». *Journal of Political Economy* 108(5): 874–904.

Goddard, Stacie E. 2021. «The Road to Revisionism - How Interdependence Gives Revisionists Weapons for Change». I *The Uses and Abuses of Weaponized Interdependence*, Brookings Institution Press, 84–98.

Goddard, Stacie E, Paul K MacDonald og Daniel H Nexon. 2019. «Repertoires of Statecraft: Instruments and Logics of Power Politics». *International Relations* 33(2): 304–21.

Goddard, Stacie E og Daniel H. Nexon. 2016. «The Dynamics of Global Power Politics: A Framework for Analysis». *Journal of Global Security Studies* 1(1): 4–18.

Goldfarb, Avi og Catherine Tucker. 2019. «Digital Economics». *Journal of Economic Literature* 57(1): 3–43.

Gordon, Robert J. 2012. *Is U.S. Economics Growth Over? Faltering Innovation Confronts the Six Headwinds*. Cambridge, MA: National Bureau of Economic Research. NBER Working Paper Series.

Govella, Kristi. 2021. «The Adaptation of Japanese Economic Statecraft: Trade, Aid, and Technology». *World Trade Review* 20(2): 186–202.

Griliches, Zvi. 1957. «Hybrid Corn: An Exploration in the Economics of Technological Change». *Econometrica* 25(4): 501.

Gutiérrez, Germán og Thomas Philippon. 2017. *Declining Competition and Investment in the U.S.* Cambridge, MA: National Bureau of Economic Research. NBER Working Paper Series.

Hansen, Bjørn Jervell, Jonas Halvorsen og Eirik Anette Flynn Opland. 2022. *Stordata og avansert analyse – sluttrapport for FFI-prosjekt «Informasjonsintegrasjon for et moderne forsvar»*. Forsvarets forskningsinstitutt. FFI-rapport 21/02647.

Harari, Yuval N. 2016. *Homo Deus: A Brief History of Tomorrow*. London: Harvill Sacker.

Harding, Harry. 2015. «Has U.S. China Policy Failed?» *The Washington Quarterly* 38(3): 95–112.

Hasegawa, Masanori. 2018. «Close Economic Exchange with a Threatening State: An Awkward Dilemma over China». *Asian Security* 14(2): 155–71.

Henrich, Joseph. 2016. «Our Collective Brain». *Project Syndicate*.

Henrich, Joseph. 2017. *The Secret of Our Success: How Culture Is Driving Human Evolution, Domesticating Our Species, and Making Us Smarter*. Princeton, NJ: Princeton University Press.

High-Level Expert Group on Artificial Intelligence. 2019. «A Definition of AI: Main Capabilities and Disciplines».

Hillman, Jonathan E. 2021. *The Digital Silk Road - China's Quest to Wire the World and Win the Future*. London: Profile Books Ltd.

Hungerland, Nils og Kenddrick Chan. 2021. *Assessing China's Digital Silk Road: Huawei's Engagement in Nigeria*. LSE Working paper 11/2021.

Iansiti, Marco og Karim R. Lakhani. 2020. *Competing in the age of AI: Strategy and Leadership When Algorithms and Networks Run the World*. Boston, MA: Harvard Business School Press.

Igata, Akira og Brad Glosserman. 2021. «Japan's New Economic Statecraft». *The Washington Quarterly* 44(3): 25–42.

Jisi, Wang mfl. 2018. «Did America Get China Wrong? The Engagement Debate». *Foreign Affairs* 97(4).

Johnson, Chandler. 1982. *MITI and the Japanese Miracle: The Growth of Industrial Policy, 1925–1975*. Stanford, CA: Stanford University Press.

Jones, Benjamin F. 2009. «The Burden of Knowledge and the "Death of the Renaissance Man": Is Innovation Getting Harder?» *Review of Economic Studies* 76: 283–317.

Jones, Charles I. 1995. «R & D Based Models of Economic Growth». *Journal of Political Economy* 103(4): 759–84.

Jones, Charles I. 2002. «Sources of U.S. Economic Growth in a World of Ideas». *The American Economic Review* 92(1): 220–39.

Karásková, Ivana. 2019. «How China Influences Media in Central and Eastern Europe». *The Diplomat*. https://thediplomat.com/2019/11/how-china-influences-media-in-central-and-eastern-europe/ (23. februar 2022).

Karásková, Ivana, Tamás Matura, Richard Q Turcsányi og Matej Šimalčík. 2018. «Central Europe for Sale: The Politics of China's Influence».

Kastner, Scott L. og Margaret M. Pearson. 2021. «Exploring the Parameters of China's Economic Influence». *Studies in Comparative International Development* 56(1): 18–44.

Keng, Shu, Jean Yu-Chen Tseng og Qiang Yu. 2017. «The Strengths of China's Charm Offensive: Changes in the Political Landscape of a Southern Taiwan Town under Attack from Chinese Economic Power». *The China Quarterly* 232: 956–81.

Kennedy, Andrew B. og Darren J. Lim. 2018. «The innovation imperative: technology and US–China rivalry in the twenty-first century». *International Affairs* 94(3): 553–72.

Kibar, Osman. 2021. «OPERASJON LAZAREV: Slår alarm om kartlegging av Norges kritiske infrastruktur». *Dagens Næringsliv*.

https://www.dn.no/magasinet/teknologi/spionasje/russland/etterretningstjenesten/operasjon-lazarev-slar-alarm-om-kartlegging-av-norges-kritiske-infrastruktur/2-1-1085420 (16 mai. 2022).

Klepper, Karina Barnholt mfl. 2021. *Teknologiutviklingens betydning for politiet, PST og Den høyere påtalemyndighet*. Forsvarets forskningsinstitutt. FFI-rapport 21/02532.

Korinek, Anton og Joseph Stiglitz. 2021. «Artificial Intelligence, Globalization, and Strategies for Economic Development». *Institute for New Economic Thinking Working Paper Series*: 1–53.

Kveberg, Torbjørn og Siw Tynes Johnsen. 2014. *Cyberdomenet, cybermakt og norske interesser*. Forsvarets forskningsinstitutt. FFI-rapport 13/02712.

Lewis, Joanna. 2012. *Green Innovation in China*. New York: Columbia University Press.

Lindgren, Petter Y. 2019. «Advancing the Role of Social Mechanisms, Mediators, and Moderators in Securitization Theory: Explaining Security Policy Change in Japan». *Asian Security* 15(3): 343–64.

Lindgren, Petter Y. og Matthew Brummer. 2022. *Four Future Worlds of US-China Rivalry: Artificial Intelligence, Economic Growth, and the Distribution of Power in Global Politics*. Artikkelutkast.

Lindgren, Petter Y., Petter Fredrik Hemnes og Kristin Waage. 2022. *Kinas potensial for økonomisk statshåndverk – kinesisk økonomi og interaksjon med omverden*. Forsvarets forskningsinstitutt. FFI-rapport 22/00421.

Lindgren, Petter Y. og Ane Ofstad Presterud. 2020. *Oppbemanning av Forsvaret i koronaens tid: en samfunnsøkonomisk analyse*. Forsvarets forskningsinstitutt. FFI-rapport 21/00886.

Lindgren, Petter Y. og Ane Ofstad Presterud. 2021a. *Expanding the Norwegian Armed Forces in the Time of Corona*. Munich Personal RePEc Archive. MPRA Paper.

Lindgren, Petter Y. og Ane Ofstad Presterud. 2021b. «High Unemployment and the Armed Forces: The Costs and Benefits of Recruiting Military Personnel in Norway». *Defence and Peace Economics* publisert online: 1–25.

Lindgren, Petter Y. og Ane Ofstad Presterud. 2021c. «Øke bemanningen i Forsvaret i dramatisk nedgangskonjunktur? En samfunnsøkonomisk vurdering». *Samfunnsøkonomen* 135(1): 45–59.

Lindgren, Petter Y. og Kristin Waage. 2021a. «Kinas bruk av økonomisk statshåndverk: Hva Kina vil og hva det får til». *Internasjonal Politikk* 79(4): 331–40.

Lindgren, Petter Y. og Kristin Waage. 2021b. «Kinas bruk av økonomisk statshåndverk: Hva Kina vil og hva det får til». *Internasjonal Politikk* 79(4): 331–40.

Lindgren, Petter Y. og Kristin Waage. 2022. *A typology of economic statecraft* [arbeidstittel]. Artikkelutkast.

Lindgren, Petter Y., Kristin Waage og Ebba Boye. 2022. *Økonomisk statshåndverk og nasjonale sikkerhetsinteresser: hvordan kan Kina true Norge?* Artikkelutkast.

Lindgren, Petter Y. og Wrenn Yennie Lindgren. 2019. «The Relationship Between Narratives and Security Practices: Pushing the Boundaries of Military Instruments in Japan». *Asian Perspective* 43(2): 325–50.

Lund, Ketil, Frank Trethan Johnsen og Arild Bergh. 2021. *Bruk av skytjenester i Forsvaret - muligheter og utfordringer*. Forsvarets forskningsinstitutt. FFI-rapport 21/00136.

Malkin, Anton. 2020. «The Made in China Challenge to US Structural Power: Industrial Policy, Intellectual Property and Multinational Corporations». *Review of International Political Economy*: 1–33.

Mancini, Federico, Bodil Farsund og Frode Lillevold. 2017. *Sikkerhetsarkitektur for Forsvarets informasjonsinfrastruktur*. Forsvarets forskningsinstitutt. FFI-rapport 17/01169.

Mastanduno, Michael. 1998. «Economics and Security in Statecraft and Scholarship». *International Organization* 52(4): 825–54.

———. 2021. «Hegemony and Fear - The National Security Determinants of Weaponized Interdependence». I *The Uses and Abuses of Weaponized Interdependence*, Brookings Institution Press, 67–83.

Mattis, Peter. 2018. «From Engagement to Rivalry: Tools to Compete with China». *Texas National Security Review* 1(4).

Matz, Sandra C, Ruth E Appel og Michal Kosinski. 2020. «Privacy in the Age of Psychological Targeting». *Current Opinion in Psychology* 31: 116–21.

Mayer-Schönberger, Viktor og Thomas Ramge. 2018. *Reinventing Capitalism in the Age of Big Data*. London: John Murray.

McAdam, Douglas, Sidney Tarrow og Charles Tilly. 2001. *Dynamics of Contention*. New York, NY: Cambridge University Press.

Mearsheimer, John J. 2014. *The Tragedy of Great Power Politics*. Updated edition. New York, NY: Norton.

Mearsheimer, John J. og Stephen M. Walt. 2016. «The Case for Offshore Balancing». *Foreign Affairs* 95(4).

Molas-Gallart, Jordi. 1997. «Which Way to Go? Defence Technology and the Diversity of 'Dual-Use' Technology Transfer». *Research Policy* 26(3): 367–85.

Moran, Theodore H. 2013. «Foreign Acquisitions and National Security: What Are Genuine Threats? What Are Implausible Worries?» I *World Scientific Studies in International*

Economics, WORLD SCIENTIFIC, 371–93. http://www.worldscientific.com/doi/abs/10.1142/9789814390842_0011 (26. november 2020).

Mowery, David C. 2009. «National Security and National Innovation Systems». *The Journal of Technology Transfer* 34(5): 455–73.

Maal, Maren, Marianne Isaachsen og Knut Torget. 2017. *Tverrsektoriell sårbarhet – Hvordan få oversikt over sårbarhet i kritiske samfunnsfunksjoner?* Forsvarets forskningsinstitutt. FFI-rapport 16/00723.

NATO. 2022. *Strategic Concept*. Adopted by Heads of State and Government at the NATO Summit in Madrid.

Nelson, Richard R., red. 1993. *National innovation systems: A comparative analysis*. New York, NY: Oxford University Press.

NIFU. 2022. «NHOs kompetansebarometer: To av tre bedrifter har udekket kompetansebehov». *Nordisk institutt for studier av innovasjon, forskning og utdanning*. https://www.nifu.no/news/nhos-kompetansebarometer-to-av-tre-bedrifter-har-udekket-kompetansebehov/ (18. september 2022).

Norris, William J. 2016. *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*. Ithaca, NY: Cornell University Press.

Norris, William J. 2021. «China's Post-Cold War Economic Statecraft: A Periodization». *Journal of Current Chinese Affairs* 50(3): 294–316.

NOU 2015:13. 2017. «Digital sårbarhet - sikkert samfunn – Beskytte enkeltmenneske og samfunn i en digitalisert verden».

NSM. 2019. *Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner*. Nasjonal Sikkerhetsmyndighet.

Nye, Joseph S. 2020. «Power and Interdependence with China». *The Washington Quarterly* 43(1): 7–21.

O'Connor, Sean. 2019. «How Chinese Companies Facilitate Technology Transfer from the United States».

Oren, Eitan og Matthew Brummer. 2020a. «Reexamining Threat Perception in Early Cold War Japan». *Journal of Cold War Studies* 22(4): 71–112.

Oren, Eitan og Matthew Brummer. 2020b. «Threat perception, government centralization, and political instrumentality in Abe Shinzo's Japan». *Australian Journal of International Affairs* 74(6): 721–45.

Pape, Robert A. 1997. «Why Economic Sanctions Do Not Work». *International Security* 22(2): 90–136.

Peksen, Dursun. 2009. «Better or Worse? The Effect of Economic Sanctions on Human Rights». *Journal of Peace Research* 46(1): 59–77.

Pepermans, Astrid. 2018. «China's 16+1 and Belt and Road Initiative in Central and Eastern Europe: economic and political influence at a cheap price». *Journal of Contemporary Central and Eastern Europe* 26(2–3): 181–203.

Posen, Barry R. 2014. *Restraint: A New Foundation for U.S. Grand Strategy*. Ithaca, NY: Cornell University Press.

Reilly, James. 2013. *China's Economic Statecraft: Turning Wealth into Power*. Sydney: LOWY Institute for International Policy.

Reppy, Judith, red. 2000. *The Place of the Defense Industry in National Systems of Innovation*. Cornell University.

Retter, Lucia mfl. 2020. *Relationships between the Economy and National Security: Analysis and Considerations for Economic Security Policy in the Netherlands*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR4287.html (19. desember 2020).

Rjaanes, Mats mfl. 2020. *Teknologiske trender – mulige konsekvenser for Luftforsvaret*. Forsvarets forskningsinstitutt. FFI-rapport 20/01894.

Roberts, Cynthia, Leslie Elliott Armijo og Saori N. Katada. 2017. *The BRICS and Collective Financial Statecraft*. Oxford: Oxford University Press.

Rosenberg, Elizabeth, Peter E Harrell, Dr Gary M Shiffman og Sam Dorshimer. 2019. *Financial Technology and National Security*. Center for a New American Security.

Rosvold, Knut A. 2016. «aktuator». *Store norske leksikon*. https://snl.no/aktuator.

Sachs, Jeffrey D. 2019. «Some Brief Reflections on Digital Technologies and Economic Development». *Ethics & International Affairs* 33(02): 159–67.

Samuels, Richard J. 1994. *'Rich Nation, Strong Army': National Security and the Technological Transformation of Japan*. Ithaca, NY: Cornell University Press.

Schwab, Klaus. 2017. *The Fourth Industrial Revolution*. London: Currency.

Segal, Adam. 2021. «Huawei, 5G, and Weaponized Interdependence». I *The Uses and Abuses of Weaponized Interdependence*, Brookings Institution Press, 149–58.

Sellevåg, Stig Rune mfl. 2020. *Samfunnssikkerhet mot 2030 – utviklingstrekk*. Forsvarets forskningsinstitutt. FFI-rapport 20/00530.

Sellevåg, Stig Rune mfl. 2021. *Samfunnsutvikling frem mot 2030 – utfordringer for politiet, PST og påtalemyndigheten*. Forsvarets forskningsinstitutt. FFI-rapport 21/01132.

Shifrinson, Joshua. 2018. «Should the United States Fear China's Rise?» *The Washington Quarterly* 41(4): 65–83.

Sikkerhetsloven. 2018. «Lov om nasjonal sikkerhet (LOV-2018-06-01-24)». https://lovdata.no/dokument/NL/lov/2018-06-01-24.

Sivertsen, Eskil Grendahl mfl. 2022. *Uønsket utenlandsk påvirkning? – kartlegging og analyse av stortingsvalget 2021*. Forsvarets forskningsinstitutt. FFI-rapport 21/02746.

Sivertsen, Eskil Grendahl, Nina Hellum, Arild Bergh og Anne Lise Bjørnstad. 2021. *Hvordan gjøre samfunnet mer robust mot uønsket påvirkning i sosiale medier*. Forsvarets forskningsinstitutt. FFI-rapport 21/01237.

Skjelland, Espen mfl. 2019. *Hvordan styrke forsvaret av Norge? Et innspill til ny langtidsplan (2021–2024)*. Forsvarets forskningsinstitutt. FFI-rapport 19/00328.

Skjelland, Espen mfl. 2022. *Forsvarsanalysen 2022*. Forsvarets forskningsinstitutt. FFI-rapport 22/00659.

Stigler, George J. 1961. «The Economics of Information». *Journal of Political Economy* 69(3): 213–25.

Stolpe, Audun, Bjørn Jervell Hansen og Jonas Halvorsen. 2019. *Stordatasystemer og deres egenskaper*. Forsvarets forskningsinstitutt. FFI-rapport 18/01676.

Strand, Ole Martin og Janne Merete Hagen. 2015. *Med Propagandaens århundre unnagjort – hva er propagandatrusselen mot et digitalisert Norge?* Forsvarets forskningsinstitutt. FFI-rapport 15/00811.

Tarrow, Sidney. 1998. *Power in Movement: Social Movements and Contentious Politics*. New York, NY: Cambridge University Press.

Telia. 2022a. «5G vs 4G - dette er forskjellen». *Telia*. https://www.telia.no/nett/5g/5g-vs-4g/ (25. mars 2022).

Telia. 2022b. «Dette er 5G». *Telia*. https://www.telia.no/nett/5g/ (25. mars 2022).

The Economist. 2017a. «Data is giving rise to a new economy». *The Economist*. https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy (30. juni 2022).

The Economist. 2017b. «The world's most valuable resource is no longer oil, but data». *The Economist*. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (30. juni 2022).

Thurbon, Elizabeth og Linda Weiss. 2021. «Economic Statecraft at the Frontier: Korea's Drive for Intelligent Robotics». *Review of International Political Economy* 28(1): 103–27.

Triplett, Jack E. 1999. «Economic Statistics, the New Economy, and the Productivity Slowdown». *Business Economics*: 13–17.

Tunsjø, Øystein. 2020. «USA og Kina står foran en superkonflikt». *Dagens Næringsliv*. https://www.dn.no/innlegg/superkonflikt/kald-krig/geopolitikk/innlegg-usa-og-kina-star-foran-en-superkonflikt/2-1-857459 (16. august 2020).

Tusikov, Natasha. 2021. «Internet Platforms Weaponizing Choke Points». I *The Uses and Abuses of Weaponized Interdependence*, Brookings Institution Press, 133–48.

Udal, Julie Helseth, Kristin Waage, Pernille Engebretsen og Petter Y. Lindgren. 2022. *Russisk økonomisk statshåndverk – implikasjoner for norsk sikkerhet*. Forsvarets forskningsinstitutt. FFI-rapport 22/00426.

Varian, Hal R. 1980. «A Model of Sales». *American Economic Review* 70(4): 651–59.

Voldhaug, Jan Erik mfl. 2021. *Hvordan kan ny IKT gjøre Forsvaret bedre?* Forsvarets forskningsinstitutt. FFI-rapport 21/01819.

Wei, Chi-hung. 2013. «China's Economic Offensive and Taiwan's Defensive Measures: Cross-Strait Fruit Trade, 2005–2008*». *The China Quarterly* 215: 641–62.

Weiss, Linda. 2021. «Re-Emergence of Great Power Conflict and US Economic Statecraft». *World Trade Review* 20(2): 152–68.

Wilson, Jeffrey D. 2018. «Whatever happened to the rare earths weapon? Critical materials and international security in Asia». *Asian Security* 14(3): 358–73.

Wirtz, Bernd W., Jan C. Weyerer og Carolin Geyer. 2019. «Artificial Intelligence and the Public Sector-Applications and Challenges». *International Journal of Public Administration* 42(7): 596–615.

Wong, Stan Hok-wui og Nicole Wu. 2016. «Can Beijing Buy Taiwan? An empirical assessment of Beijing's agricultural trade concessions to Taiwan». *Journal of Contemporary China* 25(99): 353–71.

Waage, Kristin mfl. 2021. *Økonomiske virkemidler for å oppnå strategiske mål – en oversikt*. Forsvarets forskningsinstitutt. FFI-notat 21/00140.

Waage, Kristin. 2022. *Kunstig intelligens i forsvarssektorens støttevirksomhet – hva sier litteraturen om status, anvendelser, implementering, suksessfaktorer og gevinster?* Forsvarets forskningsinstitutt. FFI-rapport 22/00425.

Waage, Kristin, Sverre Kvalvik og Petter Y. Lindgren. 2021a. «Investeringer og andre økonomiske virkemidler – når truer de nasjonal sikkerhet?» *Norsk Militært Tidsskrift* 191(3): 14–21.

Waage, Kristin, Sverre Kvalvik og Petter Y. Lindgren. 2021b. «Nye trusler fra økonomiske virkemidler». *Dagens Næringsliv*.

Waage, Kristin, Sverre Kvalvik og Petter Y. Lindgren. 2021c. *Utenlandske investeringer og andre økonomiske virkemidler – når truer de nasjonal sikkerhet?* Forsvarets forskningsinstitutt. FFI-rapport 20/03149.

Waage, Kristin og Petter Y. Lindgren. 2021. «Book review: The belt and road initiative and the future of regional order in the Indo-Pacific». *International Journal of Asian Studies*: 1–4.

Waage, Kristin, Petter Y. Lindgren, Ebba Boye og Ingrid Dørum Haug. 2022. *Kinesisk økonomisk statshåndverk og implikasjoner for norsk sikkerhet*. Forsvarets forskningsinstitutt. FFI-rapport 22/00422.

Xiaotong, Zhang og James Keith. 2017. «From Wealth to Power: China's New Economic Statecraft». *The Washington Quarterly* 40(1): 185–203.

Yan, Karl. 2022. «Rethinking China's quest for railway standardization: competition and complementation». *Journal of Chinese Governance* 7(1): 111–36.

Yeh, Chih-Liang. 2018. «Pursuing Consumer Empowerment in the Age of Big Data: A Comprehensive Regulatory Framework for Data Brokers». *Telecommunications Policy* 42(4): 282–92.

Zoellick, Robert B. 2005. «Whither China: From Membership to Responsibility?» https://2001-2009.state.gov/s/d/former/zoellick/rem/53682.htm.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan, med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål

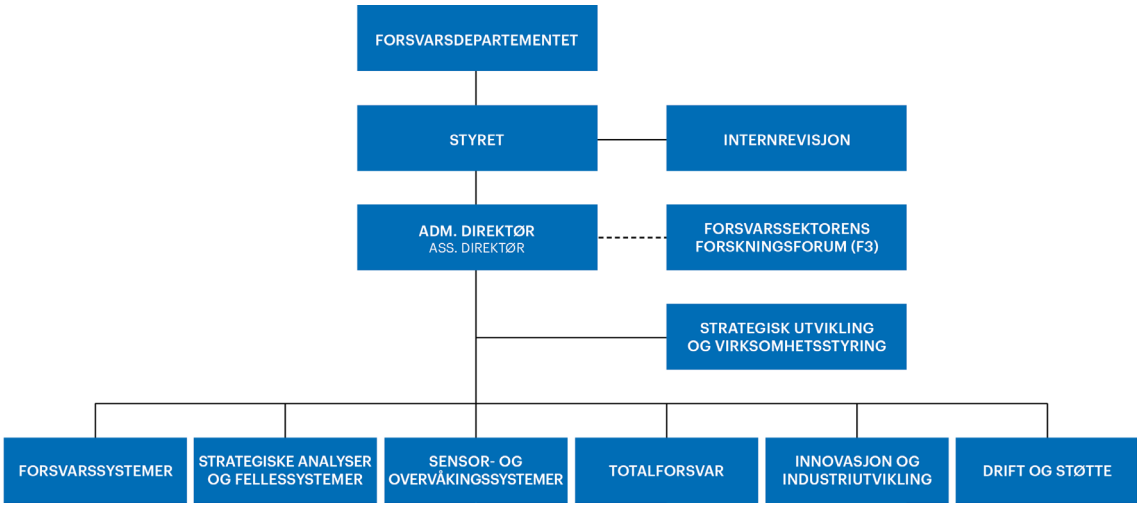
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier

Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en