



Ekomsikkerhetsutvalget

Utviklingstrekk og trender for kritisk digital infrastruktur

oslo**economics**

Tittel: Utviklingstrekk og trender for kritisk digital infrastruktur

Utarbeidet av: Oslo Economics

Oppdragsgiver: Ekomsikkerhetsutvalget

Publisert: Oktober 2024

Rapportnummer: 2024-83

Kontaktperson: Jostein Skaar / Partner

E-post: jsk@osloeconomics.no

Tel: 959 33 827

Foto/illustrasjon forside: International Telecommunications Union (ITU)

Innhold

1. Mandat, metode og informasjonskilder	1
1.1 Mandat	1
1.2 Metode og informasjonskilder	1
1.3 Leseveiledning	2
2. Samfunnets avhengighet av digitale tjenester	3
2.1 Kritisk digital kommunikasjons-infrastruktur	4
2.2 Samfunnets avhengighet av digitale tjenester	5
3. Geopolitiske trender	11
3.1 Utvikling i samspillet mellom teknologi og internasjonal politikk	11
3.2 Regulatoriske utviklingstrekk i EU og USA med mål om nasjonal kontroll	14
4. Markedsmessige og teknologiske trender	18
4.1 Høye krav til digital infrastruktur øker behovet for investeringer	18
4.2 Finansieringsbehov ved ny infrastruktur kan endre konkurransen i markedet	19
4.3 Geopolitisk rivalisering gjør utbygging av infrastruktur dyrere	21
4.4 Infrastrukturen kan utnyttes og bygges bedre ved bruk av ny teknologi	21
4.5 Lokal prosesseringskraft og reguleringer kan endre datasentermarkedet	24
4.6 Rimelig satellitteknologi komplementerer den digitale infrastrukturen på jorda	24
4.7 Oppsummering	25
5. Forventet markedsstruktur på mellomlang sikt	27
5.1 Infrastruktur for 5G-nett	27
5.2 Nasjonal og regional fiberinfrastruktur	27
5.3 Internasjonal fiberinfrastruktur	27
5.4 Bredbånd via satellitt	28
5.5 Lagring	28
5.6 Nærmere om skyleverandørene sine rolle	28
6. Oppsummering om risiko og behov for nasjonal kontroll	29
7. Referanser	31

1. Mandat, metode og informasjonskilder

Oslo Economics og NUPI har på oppdrag fra Ekomsikkerhetsutvalget analysert hvordan teknologiske- og markedsmessige endringer og geopolitisk utvikling kan påvirke nasjonal kritisk infrastruktur de neste årene. Her redegjør vi for mandatet, metoden og informasjonsgrunnlaget som ligger til grunn for analysen.

1.1 Mandat

Ekomsikkerhetsutvalget skal vurdere hvordan Norge kan ivareta nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur. For å kunne vurdere behovet for virkemidler for å sikre nasjonal kontroll, ønsket utvalget bistand til å beskrive utviklingstrekk og trender som belyser forventet utvikling av vår nasjonale kritiske infrastruktur i årene fremover. Oslo Economics og NUPI fikk i oppdrag å undersøke dette. Prosjektet er tredelt:

1. Beskrive forventede utviklingstrekk knyttet til samfunnets avhengighet av de digitale tjenestene de neste 5-8 årene. Dette innebærer en beskrivelse av hvor store samfunnsverdier som kan forventes å leveres over den digitale infrastrukturen.
2. Beskrive utviklingstrekk som har betydning for hvordan myndighetene kan ivareta nasjonal kontroll over viktige verdier og virksomheter i verdikjeden for disse digitale tjenestene. Dette inkluderer elementer som kan øke sårbarheten i forsyningen av de digitale tjenestene. Beskrivelsen skal også dekke forventede eierskapsstrukturer på nasjonalt, nordisk, EU- og globalt nivå.
3. Beskrive eventuelle utviklingstrekk som bidrar til å redusere sårbarheten i forsyningen av de digitale tjenestene.

Det er hovedsakelig tre ulike drivere for utviklingen som belyses i prosjektet: teknologiske endringer, markedsmessige endringer og konsekvenser av geopolitisk, sikkerhetspolitisk og regulatorisk utvikling.

1.2 Metode og informasjonskilder

For å besvare problemstillingene i oppdraget har vi benyttet oss av skriftlige kilder, statistikk og intervjuer.

Skriftlige kilder

I analysen har vi benyttet skriftlige kilder som vi har funnet gjennom nettsøk og dokumentgjennomgang. Vi har benyttet nettsøk for å kartlegge og forstå de ulike teknologiene. Her har nettstedene til ulike operatører og nyhetsartikler vært sentrale.

Dokumentgjennomgang har også vært en viktig del av vår informasjonsinnsamling. Under viser vi til eksempler på noen av de dokumentene og kildene vi har benyttet. Kapittel 8 gir en fullstendig oversikt over alle de skriftlige kildene vi har benyttet i vårt arbeid med denne rapporten.

For å kartlegge sentrale teknologiske trender, har vi gjennomgått rapporter som har forsøkt å fremskrive hvordan ulike deler av samfunnet vil påvirkes av teknologiske trender i årene som kommer. Eksempler på noen av disse rapportene er NAVs omverdensanalyse som skisserer hovedutfordringene Norge står overfor i årene som kommer og Deloitte sin rapport om trender i telekommarkedet.

For å forstå hvordan markedene vil se ut fremover i Europa, har det vært sentralt å se på dokumenter fra EU. Deler av kapittel 5 er derfor basert på rapporter utarbeidet av aktører som Europakommisjonen, BEREC og sentrale økonomer. Noen kilder har vært EUs «White Paper» om Europas behov for digital infrastruktur og hvordan det burde investeres i dette fremover. Videre har vi også gjennomgått Enrico Lettas rapport om fremtiden til EUs indre marked og Mario Draghis rapport om EUs konkurransepolitikk.

Statistikk

For å kartlegge vår avhengighet av den digitale infrastrukturen har vi sett på tall som sier noe om tilgang og bruk av internett og digitale løsninger. Noen sentrale kilder har vært:

- SSBs statistikk om nordmenns bruk av digitale medier, internett- og mobilbruk m.m.
- Statistikk fra ulike kilder over bruk av skytjenester, kunstig intelligens og 3D-printing i norske bedrifter.
- SSBs statistikk over bruk av digitale tjenester i offentlig sektor

Intervjuer

Vi har også gjennomført semistrukturerte intervjuer som et ledd i informasjonsinnsamlingen til prosjektet. I semistrukturerte intervjuer ligger det en intervjuguide til grunn for samtalen, men

informantene har selv kunnet styre samtalen og trekke frem de momentene de mener er av størst betydning.

Vi har intervjuet ulike aktører i verdikjeden. Dette inkluderer leverandører av skytjenester, fysisk infrastruktur, mobiloperatører og datasentre. Vi har også intervjuet tredjeparter som myndighetsorganer og bransjeorganisasjoner. Tabell 1-1 viser en oversikt over de vi har intervjuet i prosjektet.

Tabell 1-1: Intervjuobjekter

Markedsaktører	Myndighetsorgan/ Bransjeorganisasjon
Bulk	Nasjonal kommunikasjonsmyndighet
Ericsson	Utenriksdepartementet
Intility	Generalkonsulatet i San Francisco
Microsoft	European Competitive Telecommunications Association
Oneco	PTS (Sverige)
Skygard	
Space Norway	

Intervjuene har omhandlet følgende momenter, med noen justeringer når vi har snakket med myndighetsorganer og bransjeorganisasjoner:

- Innledende spørsmål om selskapet, hvilket spesifikt marked aktøren tilhører og hvordan dette markedet har endret seg over tid.
- Hvilke teknologiske trender aktøren ser for seg kommer til å påvirke ekomarkedet og den nasjonale kontrollen i verdikjeden.
- Hvordan geopolitiske trender og internasjonale reguleringer påvirker aktøren, men også ekomarkedet i stort.

1.3 Leseveiledning

Resten av rapporten er strukturert som følger. I kapittel 2 analyserer vi avhengigheten til kritisk digital infrastruktur og hvordan denne vil utvikle seg fremover. I kapittel 3 gjennomgås spesifikke trusler og det generelle geopolitiske bakteppe. I kapittel 4 og 5 gjennomgår vi teknologiske og markedsmessige trender, mens vi i kapittel 6 presenterer forventet markedsstruktur på mellomlang sikt. Kapittel 7 sammenstiller funnene i rapporten og beskriver den overordnede risikoen for svekket nasjonal kontroll over den nasjonale kritiske digitale infrastrukturen. Kapittel 8 inneholder referanselisten for prosjektet.

2. Samfunnets avhengighet av digitale tjenester

Norge er i dag en av de mest digitaliserte samfunnene i verden. Vi har en befolkning med høy digital kompetanse, som tar i bruk ny teknologi raskt. Samfunnet blir derfor i økende grad avhengige av digitale tjenester. Regjeringen har mål om ytterligere digitalisering av samfunnet, og bruk av skyteknologi, kunstig intelligens og tingenes internett vil sannsynligvis føre til at enda større verdier bæres over den digitale infrastrukturen.

En stadig større andel av samfunnet er avhengige av digitale tjenester. Det norske samfunnet er en av de mest digitaliserte samfunnene i verden. Vi kommer høyt ut i internasjonale rankinger av grad av digitalisering av offentlig sektor, og vi har en befolkning som er tidlig ute med å ta i bruk nye digitale tjenester. Med den teknologiske utviklingen er det også forventet at et stadig større arbeidsoppgaver vil automatiseres. Dette er med på å gjøre at vi har en av de mest produktive arbeidsstyrkene i verden, men det gjør også at stadig større samfunnsverdier bæres over den digitale infrastrukturen (Oslo Economics, 2023). Som samfunn er vi derfor sårbare for hendelser som bidrar til svikt i forsyningen av grunnleggende digitale tjenester som internett, talekommunikasjon og satellittbasert kommunikasjon.

Den digitale infrastrukturens betydning for samfunnet, har også bidratt til at teknologiske avhengigheter og kontroll over kritiske innsatsfaktorer i økende grad har blitt ansett som strategiske instrumenter i mulige konflikter. Leverandører i ulike land kan også være underlagt jurisdiksjon som pålegger disse leverandørene å utlevere data som de besitter til myndighetene i sine respektive land. Dette kan være med å utfordre den nasjonale suvereniteten over data som har betydning for et lands innbyggere. På bakgrunn av dette har det blitt økt fokus på nasjonal kontroll over forsyningskjeder for viktige teknologier i en rekke land.

Krigen i Ukraina og de økte spenningene mellom Kina og USA har løftet sikkerhetspolitikk høyere på agendaen, og illustrert i hvor stor grad økonomiske og teknologiske avhengigheter kan bli brukt som strategiske instrumenter i en potensiell konflikt. Politisk interesse for verdikjeder og økonomisk

sikkerhet har økt i takt med de politiske spenningene, om enn med et usikkert utfall på organiseringen av økonomisk aktivitet globalt.

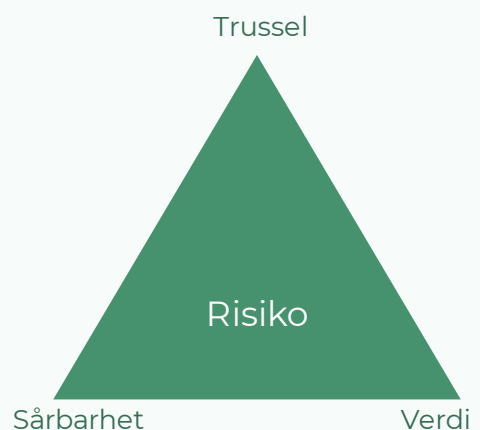
Den digitale infrastrukturen er kompleks, og de underliggende verdikjedene innenfor dette markedet er ofte lange og uoversiktlige. På lik linje med andre deler av økonomien, er forsyningskjedene for viktige innsatsfaktorer til den digitale infrastrukturen globale, og både varer og tjenester leveres fra andre land.

Eierskapsstrukturene for selskaper i ulike deler av verdikjeden kan også være uoversiktlige og endres over tid. Dette gjør at det er krevende å ha kontroll over hvilke aktører som har adgang til kritiske systemer i den digitale infrastrukturen.

Dette har gjort at det har blitt økt oppmerksomhet om nasjonal kontroll over verdikjeder til kritisk digital infrastruktur i en rekke land. Nasjonal kontroll er ikke et mål i seg selv, men skal forstås som et sett med virkemidler for å oppnå økt nasjonal sikkerhet. Nasjonal kontroll kan derfor ses på som virkemidler for å redusere risikoen for sikkerhetsbrudd i den digitale infrastrukturen.

Risiko er et produkt av sannsynlighet og konsekvens. Nærmere bestemt *sannsynligheten* for at en uønsket hendelse inntreffer og fører til en svikt og *konsekvensen* av de negative hendelsene som svikt i systemet medfører. Det kan iverksettes tiltak for å både redusere sannsynligheten for at hendelsen fører til svikt, og minimere de negative konsekvensene ved et eventuelt utfall. Sårbarhet er et systems manglende evne til å motstå at en uønsket hendelse inntreffer eller tåle at en uønsket hendelse inntreffer, uten at det får alvorlige konsekvenser (Direktoratet for sikkerhet og

Figur 2-1: Risikotrekant



beredskap, 2019). Figur 2-1 illustrerer sammenhengen mellom risiko, sårbarhet, trussel og verdi. Risikoen er høy dersom sannsynligheten for at en hendelse inntreffer (trussel) er høy, at systemets evne til å motstå eller begrense den uønskede hendelsen er lav (sårbarhet) og de påfølgende konsekvensene er store (verdi).

Formålet med denne analysen er å undersøke hvordan teknologiske, geopolitiske og markedsmessige trender vil påvirke samfunnsverdiene som bæres over den digitale infrastrukturen, og hvordan det vil påvirke behovet for behovet for nasjonal kontroll. Siden nasjonal kontroll er risikominimerende tiltak, har vi valgt å strukturere rapporten rundt risikotrekanten.

I denne rapporten er systemet som vi analyserer, den kritiske digitale infrastrukturen. Vi gir en beskrivelse av hva vi definerer som den kritiske digitale infrastrukturen i kapittel 2.1. I kapittel 2.2 beskriver vi forventet utvikling i samfunnets avhengighet av digitale tjenester og utvikling i hvilke samfunnsverdier som bæres over den digitale infrastrukturen, som sier noe om verdi og konsekvens av utfall i risikotrekanten. Deretter vil vi, i kapittel 3, identifisere hvilke trusler som eksisterer basert på utvikling i geopolitiske trender. Til slutt vil sårbarheter i den digitale infrastrukturen identifiseres gjennom en analyse av markedet og teknologiske trender i kapittel 4 og 5. I kapittel 6

oppsummerer vi utvikling i risiko og hvordan dette påvirker behovet for nasjonal kontroll.

2.1 Kritisk digital kommunikasjonsinfrastruktur

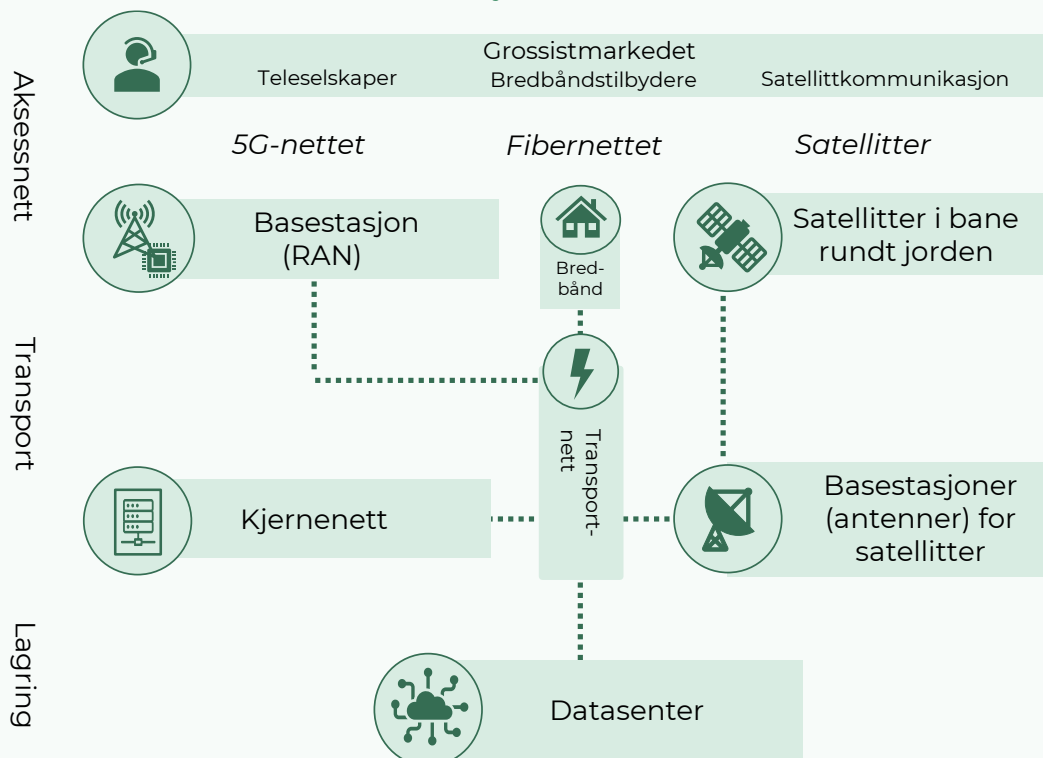
Det benyttes ofte ulike begreper for å definere digital infrastruktur. I dette prosjektet er formålet å vurdere kritisk infrastruktur for elektronisk kommunikasjon. Innledningsvis er det derfor nyttig å først klargjøre enkelte begreper og hva vi definerer som infrastruktur for elektronisk kommunikasjon i denne analysen. Infrastrukturen for elektronisk kommunikasjon kan defineres som alle systemer som er nødvendig for å sende, motta og lagre informasjon digitalt over tid og rom. Alle tjenester som deretter gjør det mulig å aksessere eller videre bearbeide denne informasjonen definerer vi som digitale tjenester.

Figur 2-2 viser en enkel fremstilling av viktige komponenter i infrastrukturen for elektronisk kommunikasjon.

2.1.1 Transportnettene

Transportnettet er den delen av infrastrukturen hvor informasjon sendes mellom ulike aksesspunkter i aktuelle deler av nettet. I transportnettet sendes informasjon i hovedsak over fiberoptiske kabler, men den kan også sendes via

Figur 2-2: Infrastruktur for elektronisk kommunikasjon



radiobølger mellom basestasjoner.

Transportnettene kan generelt sett sies å bestå av landsnett som deretter forgreiner seg utover i regionale og lokale nett. Transportnettene er i stor grad bygd opp i ringstrukturer, hvor signaler kan rutes via to eller flere fiberkabler mellom to punkter i nettet. Dette bidrar til å øke robustheten i nettene, siden ett enkelt brudd i en kabel ikke vil føre til svikt i forsyningen av signaler mellom to punkter.

I dag er det flere leverandører som leverer transportnettjenester i Norge. Trafikken mellom disse nettene overføres via ulike samtrafikkpunkter. De ulike leverandørene av nett benytter også ulike drift- og støttesystemer for å overvåke og styre sine nett. Disse systemene kalles gjerne kjernet, og er kritiske deler av deres respektive nett.

De nasjonale transportnettene er koblet til utenlandske transportnett via fiberkabler som går via sjø og land.

2.1.2 Aksesteknologier

Aksesnettet defineres som de punktene hvor sluttbrukere kan aksessere transportnettene med ulike teknologier. Vi skiller mellom tre ulike aksesteknologier; kablet bredbånd, mobilnettverk og satellitteknologi. Aksess via bredbånd er den fiber- eller kobberkabelen som kobler brukeren til transportnettene. De fleste bredbåndsbrukere vil sannsynligvis være koblet til nettet via én kabel, mens kritiske funksjoner gjerne vil være koblet til nettet via flere kabler for å redusere risikoen for signalsvikt som følge av brudd på bredbåndskabelen. Mobilbaserte tjenester kobles til transportnettene via **radiobølger** til basestasjoner som igjen er koblet til transportnettene via fiberkabler. I mange områder er det overlappende dekning fra flere basestasjoner, som gjør at dekningen vil kunne opprettholdes om enn med redusert kapasitet ved bortfallet av en basestasjon. Ved bruk av satellitteknologi vil en bakkestasjon transmittere radiosignaler til en satellitt som videregir signaler til mottakere på bakken enten direkte eller via andre satellitter.

2.1.3 Lagring av informasjon

Lagring av data gjøres i datasentre som enten driftes i egen regi eller av en tredjepart. NSM (2022) skiller mellom fire ulike typer datasentre:

- **Virksomhetsinterne datasentre:** Dedikert datasenter for sluttbruker på eget nettverk som driftes av sluttbruker selv eller av tredjepart.
- **Colocation datasentre:** Tredjepart tilbyr lokaler og drift av sluttbrukers eget utstyr sammen med andre kunder.
- **Et hyperscale datasenter** («stort dedikert datasenter») er større anlegg som ofte er designet for, og eid av, virksomheter med ekstreme krav til skalerbare og robuste tjenester.
- **Edge datasentre:** Mindre datasentre som plasseres lengere ute i nettverkene for å være nær sluttbruker for å ivareta krav til latens¹, lokal prosessering mm.

Skytjeneste er en applikasjon, dataprosessering eller lagring som tilbys på en ekstern lokasjon (SNL, 2023). Ved kjøp av skytjenester fra eksterne aktører inngår derfor lagring av data som en del av tjenesten. Ved bruk av skytjenester kan bruker velge om de ønsker å dele skytjenesteleverandørens systemer med andre brukere (allmenn sky), eller om de ønsker å ha dedikerte systemer til sine data (lukkede skytjenester). Skytjenester kan leveres av store internasjonale selskaper som har store hyperscale datasentre i flere land og på flere kontinenter. Ved bruk av allmenne skytjenester kan derfor dataene lagres langt unna sluttbruker.

2.2 Samfunnets avhengighet av digitale tjenester

Samfunnet blir i økende grad avhengig av digitale tjenester. Internett og digitalisering har de siste 30 årene forandret samfunnet på en grunnleggende måte. Det norske samfunnet er et av verdens mest digitaliserte (Regjeringen, 2021). Digitaliseringen av samfunnet har gjennomgått flere bølger siden de første datamaskinene ble oppfunnet rundt midten av det forrige århundret.

En av disse bølgene var oppfinnelsen av internett tidlig på 1990-tallet. Internett bidro til at informasjon ble enklere tilgjengelig, og at mer informasjon kunne utveksles raskere over store distanser. Dette bidro til å redusere behovet for fysisk nærhet mellom leverandør og kunder. Dette kombinert med reduksjon i fraktkostnader og en liberalisering av internasjonal handelspolitikk var

¹ På engelsk brukes begrepet «latency» om forsinkelse når informasjon sendes over et nettverk. «Latency» er derfor et mål på tiden det tar å sende informasjon over et nettverk. I

denne rapporten har vi brukt «tidsforsinkelse» som norsk begrep med samme betydning. (Amazon, 2024).

med å bidra til økt internasjonal handel fra slutten av 90-tallet og utover 00-tallet (Oslo Economics, 2023).

Utviklingen i verdenshandelen de siste tiårene har ikke bare vært økt handelsvolum og handel i flere typer varer. Den har også bidratt til å endre hvordan varer produseres og hvordan handelen organiseres. Særlig viktig er framveksten av stadig mer komplekse verdikjeder, hvor selskap samarbeider og koordinerer seg med strategiske partnere og spesialiserte leverandører (Gereffi, et al., 2005). Resultatet har vært en bevegelse mot mer desentraliserte og nettverksbaserte verdikjeder, hvor organiseringen er løser og produksjon spredd over store deler av verden (Kano & Oh, 2020). Konsekvensen har vært at handel i *varer under produksjon* nå utgjør en større del av den globale handelen enn *ferdige varer* (Coe & Yeung, 2015).

Denne utviklingen har resultert i at mange verdikjeder i samfunnet i dag enten direkte eller indirekte er avhengige av varer som produseres i andre land. De globale forsyningskjedene og desentraliserte selskapsstrukturene er avhengige av digitale tjenester for å utveksle informasjon, gjennomføre transaksjoner og for å organisere kompliserte logistikkjeder.

2.2.1 Skytjenester og smarttelefoner

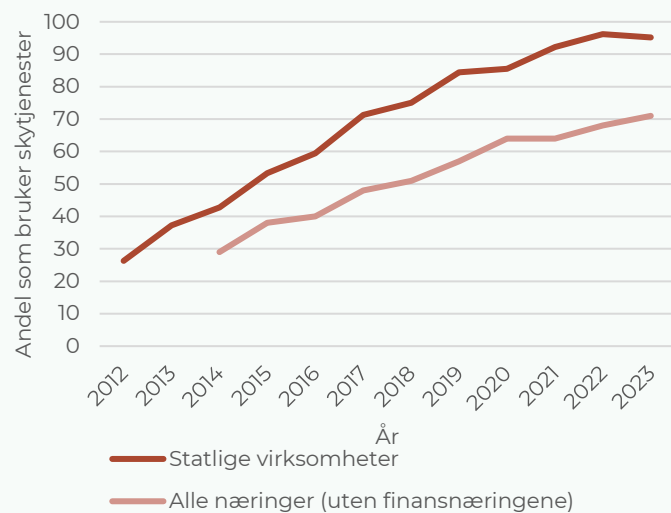
Den neste digitaliseringsbølgen kom med oppfinnelsen av smarttelefoner og skyteknologi. Skytjenester (cloud computing) er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett (Datatilsynet, 2018). Selskaper som tidligere hadde data på eget nettverk (on-premise), kunne nå kjøpe dette som en tjeneste fra en skyleverandør (Datatilsynet, 2018). Fordelene med skytjenester er blant annet at de er svært skalerbare, og det gir bedrifter rask tilgang til nye applikasjoner og teknologi. Videre gjør det at personer kan dele data og samarbeide enklere om å gjennomføre oppgaver. For eksempel ved at ansatte ikke må være på bedriftens nettverk for å få tilgang til bedriftens data og applikasjoner.

Det har gjort at svært mange virksomheter i offentlig og privat sektor har tatt i bruk skytjenester. I 2023 oppga 71 prosent av alle næringer, uten finansnæringene at de har kjøpt en eller flere skytjenester. Blant statlige virksomheter benytter omtrent 97 prosent skytjenester, inkludert økonomisystemer, webplattformer, prosjektverktøy, databaser, mm. De siste ti årene har det vært en økning på over 50 prosentpoeng i bruken av slike tjenester i statlige virksomheter.

Utviklingen med økt bruk av skytjenester har ført til at lagring og prosessering av data i større grad sentraliseres i store datasentre, som har økt datasentrenes betydning i den digitale infrastrukturen. Det har gjort at mange virksomheter i privat og offentlig sektor har blitt avhengig av internett for å få tilgang til sine data og applikasjoner. Dette gjør at verdien som bæres over transportnettene mellom datasentre, bedrifter og sluttbruker har økt.

Utviklingen av smarttelefoner har muliggjort utviklingen av applikasjoner på mobiltelefoner, og bedret tilgangen til internett via mobil. Dette har

Figur 2-3: Bruk av skytjenester i statlige virksomheter og privat næringsliv



Kilde: SSB. Kommentar: Finansnæringen var holdt utenfor undersøkelsen.

igjen bidratt til at mobiltelefonen i dag benyttes til stadig flere oppgaver som tidligere ble gjennomført manuelt, som for eksempel betalingsmidler, karttjenester, lese aviser mm.

Norge er et av landene med lavest kontantbruk, både når det gjelder mengden kontanter i omløp som andel av samlede betalingsmidler, og kontantbetalinger som andel av samlede betalinger. Ifølge Norges Bank utføres blant annet 83 prosent av alle betalinger mellom privatpersoner med mobiltelefon. Samtidig som andelen av mobilbetalinger har økt, har bruken av kontanter hatt en fallende trend (Norges Bank, 2024 (1)).

Norge scorer også høyt på digitale ferdigheter i befolkningen, og vi har en befolkning som raskt tar i bruk ny teknologi. Dette har også bidratt til at befolkningen har høye forventninger til at offentlige

tjenester skal være digitaliserte. Statlige virksomheter og kommuner tilbyr stadig flere digitale tjenester, og bruken av digitale tjenester har økt betraktelig. Dette inkluderer offentlig helsetjenester, kommunikasjon med innbyggere, skattemeldinger, saksbehandlingsprosesser mm. Dette har ført til at Norge i dag kommer høyt ut i rangeringer av grad av digitalisering av offentlige tjenester i ulike land (Kommunal- og moderniseringsdepartementet, 2020).

Oppsummert så har vi i dag et av verdens mest digitaliserte samfunn, hvor nær sagt alle verdikjeder i privat sektor enten direkte eller indirekte er avhengige av digitale tjenester. Vi har også en offentlig sektor som er blant de mest digitaliserte i verden. Vi har også en befolkning som i økende grad benytter digitale tjenester i hverdagen for å gjøre oppgaver som tidligere ble gjennomført manuelt, og som har høye forventninger til at oppgaver skal kunne gjennomføres digitalt. De digitale tjenestene som konsumeres i ulike deler av samfunnet utvikles og leveres også i økende grad fra skytjenester som leveres over internett fra sentraliserte datasentre. Det er derfor stadig større verdier som bæres over den digitale infrastrukturen.

2.2.2 Trender som indikerer en økning i samfunnsverdier

I det følgende vil vi gi en kort beskrivelse av utvalgte trender som indikerer at summen av samfunnsverdiene som bæres over den digitale infrastrukturen vil øke. Deretter vil vi peke på noen utvalgte trender som kan peke i en annen retning.

Behov for, og mål om, ytterligere digitalisering

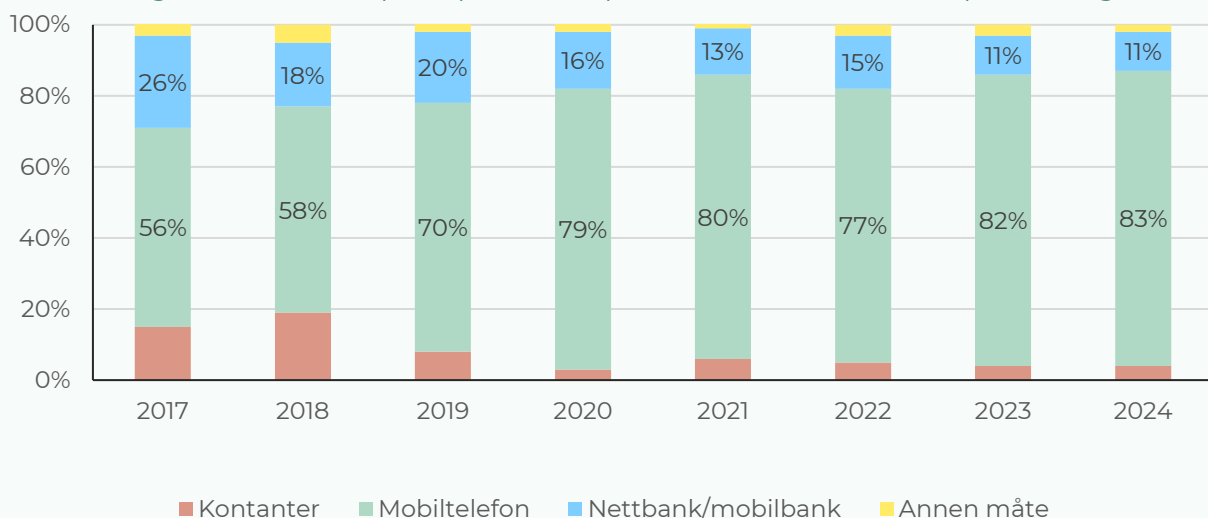
En utfordring fremover er at veksten i antallet personer i yrkesaktiv alder er ventet å stagnere, samtidig som antallet eldre vil øke betydelig. Disse demografiske endringene skaper betydelige utfordringer. Perspektivmeldingen 2024 fremhever viktigheten av å øke arbeidstilbudet for å møte disse utfordringene. I NAVs omverdensanalyse 2023-2035 legges det også vekt på omstilling og mangel på arbeidskraft. NAV peker på digitaliseringen som en stor mulighet for å lette og effektivisere arbeidet i tiden fremover (NAV, 2023). Andre utredninger, som for eksempel Helsepersonellkommissjonen, har også pekt på at det er behov for ytterligere digitalisering i helsevesenet i fremtiden for å kompensere for mangel på arbeidskraft.

Regjeringens digitaliseringsstrategi for offentlig sektor 2024-2030 har klare ambisjoner om videre digitalisering. Strategien har blant annet som mål at flere oppgaver skal løses digitalt og at brukerne skal oppleve én digital offentlig sektor (Digitaliserings- og forvaltningsdepartementet, 2024). Mangel på arbeidskraft i fremtiden vil derfor være en underliggende driver som taler for en ytterligere digitalisering i årene som kommer, som igjen vil bidra til at vi blir mer avhengige av digitale tjenester.

Bruk av kunstig intelligens

I teknologirådets årsrapport beskrives 2023 som året da kunstig intelligens for alvor ble en del av norsk samfunnsliv og politikk. To måneder etter

Figur 2-4: Betalingsmåter mellom privatpersoner. I prosent av det totale tallet på betalinger. 2017–2024.



lanseringen av ChatGPT i 2022 hadde chatboten nådd 100 millioner brukere, raskere enn noen annen digital tjeneste (Hu, 2023). En undersøkelse utført av Samfunnsøkonomisk Analyse (SØA) på vegne av NHO, Abelia, Finans Norge og Nelfo høsten 2023, viser at én av fire virksomheter har tatt i bruk kunstig intelligens i dag, men at det forventes at bruken vil øke (SØA, 2023).

KI tas i bruk i sektorer for å bidra til å automatisere oppgaver, forbedre beslutnings-prosesser og effektivisere arbeidsflyten. Arbeidsoppgaver som koding og tekstgjennomlesning er eksempler på arbeidsoppgaver som har stort effektiviseringspotensial ved bruk av KI.

I Norges KI-strategi er det et uttalt ønske om at Norge skal ha en sentral rolle innen anvendelse av KI (Kommunal- og moderniseringsdepartementet, 2020). For å oppnå dette målet er det behov for større kapasitet på nettet og flere datasentre som kan gi kjøling til prosessorene, ettersom KI har et stort behov for energi. Norge er attraktiv som lokasjon for datasentre siden tilgangen på fornybar og billig energi er god.

Bruk av KI vil dermed føre til at flere oppgaver som i dag gjennomføres manuelt vil kunne automatiseres, og at verdikjeder i økende grad blir avhengige av digitale tjenester. Dette vil igjen kunne føre til en økning i verdiene som bæres over den digitale infrastrukturen. Dersom Norge blir et attraktivt land for etablering av datasentre som leverer tjenester til andre land, kan det også føre til at infrastruktur i Norge får større verdi for virksomheter i andre land som benytter seg av datasentrene.

Fortsatt migrering til sky

Markedet for allmenne skytjenester er dominert av noen få store amerikanske aktører. Bekymringer knyttet til personvern og kontroll over egne data, samt regulatoriske uklarheter knyttet til hvilke data som kan plasseres i allmenne skytjenester og hos utenlandske leverandører, har også skapt usikkerhet knyttet til hvilke tjenester som kan benyttes for ulike typer data. I statsforvaltningen har det vært gjennomført flere prosjekter som har utredet hvilke typer løsninger som kan benyttes for lagring og prosessering lav ulike typer data.² Flere statlige virksomheter har derfor vært avventende med å migrere data som er beskyttelsesverdig ugradert over i skytjenester, og har derfor fortsatt å

benytte on-premise løsninger for disse dataene. Etter hvert som det utvikles ulike skytjenester for ulike deler av statsforvaltningen, vil derfor mer data i statsforvaltningen som i dag lagres on-premise migreres over i ulike skytjenester.

Større verdier bæres over de kommersielle nettene

Teknologisk utvikling vil gjøre at det i fremtiden i større grad vil være mulig å opprette virtuelle private nettverk innad i kommersielle 5G-nettene. Dette vil gjøre at kunder som i dag har egne fysiske private nettverk i større grad kan kjøpe dette som en tjeneste fra kommersielle telekomoperatører. Dette muliggjør blant annet at dagens nødnett sannsynligvis(?) vil migrere over i de kommersielle mobilnettene i fremtiden.

Internet of things og virtuell virkelighet

«Internet of Things» (IoT) og «Machine-to-machine» (M2M) dekker et vidt spekter av teknologier. IoT referer til alle tingene rundt oss som kan kobles til internett. Når tingene er koblet til nett kan de koble seg sammen, kommunisere med hverandre og omgivelsene. Typiske bruksområder i dag spenner fra smarthøytalere og sporingstjenester til digitale kjørebøker og sensorer som måler temperatur, strøm, luftkvalitet, fuktighet og vann (Telenor, 2023). Antallet enheter som er koblet til IoT økt betydelig, og det er forventet at antallet vil fortsette å øke i fremtiden. Disse enhetene vil produsere store mengder data, og vil være med på å drive utviklingen mot stadig mer digitaliserte verdikjeder.

Virtual reality (VR) kan oversettes til virtuell virkelighet, og er kunstig gjengivelse av miljø med bruk av bilder og lyd. VR-simuleringer blir stadig bedre innen felt som medisin, byggeteknikk og innenfor spillindustrien. Det er stor usikkerhet knyttet til hvilken grad VR blir tatt i bruk frem mot 2030. Dersom det blir tatt i bruk i økende grad, vil denne type teknologi sannsynligvis ha høye krav til båndbredde og lav tidsforsinkelse.

2.2.3 Trender som begrenser verdien som bæres over deler av infrastrukturen

Det har vært en økning i verdiene som bæres over den digitale infrastrukturen. En hendelse som fører til et samtidig utfall i hele infrastrukturen, ville derfor hatt store negative konsekvenser for samfunnet. Samtidig er verdien som bæres over nettene spredt på flere aktører og systemer. For eksempel er data lagret i flere datasentre,

² Utredning av Nasjonal sky og Felles IKT for departementsfelleskapet er to eksempler.

informasjon sendes over ulike fiberkabler og sluttbrukere kan få tilgang til nettene via ulike aksessteknologier. Alle disse ulike komponentene er igjen driftet av ulike virksomheter. Sannsynligheten for at det vil oppstå samtidig utfall i større deler av infrastrukturen vil derfor avhenge av konsentrasjonen i infrastrukturen.

Selv om verdien som bæres over infrastrukturen samlet sett øker, kan verdien som bæres over enkelte deler av infrastrukturen dermed reduseres dersom konsentrasjonen blir mindre. Dersom all internettrafikk er avhengige av én fiberkabel, vil verdiene som bæres den kabelen være svært stor. Dersom det derimot bygges ut flere fiberkabler, vil verdiene som bæres over den ene kabelen reduseres.

Over de siste årene har vi hatt utviklingstrekk som har bidratt til å redusere konsentrasjonen i enkelte deler av infrastrukturen. To tydelige eksempler er utbyggingen av flere fiberforbindelser til utlandet og utbyggingen av flere nasjonale transportnett.

Distribuerte skytjenester

Ovenfor beskriver vi at en stor andel av offentlig og privat sektor benytter skytjenester, og at dette er forventet å øke i fremtiden. Samtidig er det viktig å påpeke at de ikke nødvendigvis benytter skytjenester for alle typer tjenester og data. Videre benytter de fleste virksomheter en hybrid skystrategi, hvor de mest kritiske eller sensitive tjenestene plasseres i lukkede skytjenester og hvor eventuelt tjenester som ikke er egnet for sky forblir på eget nettverk. Videre tilbyr også flere leverandører distribuerte skyløsninger, hvor data kan lagres og prosesseres i en kombinasjon av allmenne og lukkede skytjenester, i co-location datasentre og på egne nettverk, men hvor de kan styres fra et enkelt kontrollpanel. Dette skal bidra til at kunder vil kunne ta i bruk applikasjoner og tjenester fra skyen på data som lagres på eget nettverk og at kunden vil kunne få tilgang til dataene selv uten internettforbindelse.

Denne trenden kan være med å begrense hvor store samfunnsverdier som plasseres ut i skyen, og dermed begrense verdiene som bæres over den digitale infrastrukturen.

Mot mer desentralisert lagring og prosessering av data

I fremtiden er det en forventning om at en større andel av dataene vil produseres, lagres og prosesseres nærmere sluttbruker. Dette skyldes blant annet fremveksten av IoT, at flere tjenester har behov for lav tidsforsinkelse og at det er ønskelig å begrense bruk av transittjenester. En del av denne utviklingen er økende bruk av Content

Delivery Networks (CDN). CDN innebærer at servere distribueres geografisk nærmere ut i nettene hvor innhold til en tjenestetilbyder mellomlagres. Dette innebærer at deler av prosesseringen av data skjer nærmere sluttbruker, fremfor at informasjon må sendes tilbake til tjenestetilbyderens kjerneservere. Dette gjøres for å redusere latency, bedre brukeropplevelse, øke sikkerheten og redusere bruken av transporttjenester. Sikkerheten økes ved at data gjerne spres på flere servere som er geografisk adskilt. Videre vil tjenesten bli mindre avhengig av tjenestetilbyderens host-server.

Over de siste årene har det vært en økning bruk av tjenester som krever stor båndbredde, som streaming, sosiale medier og gaming. I disse kategoriene har det stor verdi for tilbydere at data prosesseres nærmere sluttbruker siden det bedrer brukeropplevelsen. Derfor har det vært en vesentlig økning i bruk av CDN over de siste årene. Det er også forventet at dette markedet vil øke betydelig i årene som kommer, og særlig dersom man får tjenester som virtuell virkelighet.

Sluttbrukere diversifiserer

Som drøftet ovenfor er det store verdier som bæres over den digitale infrastrukturen. Dette gjør også at de økonomiske konsekvensene for bedrifter er store dersom de mister tilgang på digitale tjenester. Dette gjør at mange bedrifter har høy betalingsvillighet for å investere i tiltak som bidrar til å øke robustheten i tilgangen på digitale tjenester. Ett eksempel er at kunder har en multi-cloud strategi hvor de benytter flere skyleverandører, eller bruk av CDN og at kunder kjøper nettverkstjenester fra flere leverandører for å spre sin egen trafikk.

2.2.4 Oppsummering

Norge har en befolkning med høy digital kompetanse, og som raskt tar i bruk nye digitale tjenester. Teknologiske fremskritt over de siste 30 årene har ført til at vi i dag er ett av de mest digitaliserte samfunnene i verden. Mange av verdikjedene i samfunnet er direkte eller indirekte avhengige av digitale tjenester, og vi har en av de mest digitaliserte offentlige sektorene i verden. Vi som samfunn blir derfor i økende grad avhengige av den underliggende infrastrukturen.

I årene som kommer forventer vi at samfunnet blir stadig mer digitalisert. Regjeringens digitaliseringsstrategi legger klare mål for at Norge skal bli det mest digitaliserte samfunnet i verden innen 2030. Teknologiske trender som bruk av kunstig intelligens, skytjenester, virtuell virkelighet og en fortsatt økning i antall IoT-enheter vil være med å øke bruken av internett, og at digitale

tjenester blir en stadig mer integrert del av verdikjeder i samfunnet.

Samtidig er det viktig å påpeke at den digitale infrastrukturen ikke er en enkeltstående enhet, men bestående av flere aktører og systemer. Over de siste årene har vi hatt en trend mot mer diversifisering i enkelte deler av infrastrukturen, blant annet ved at vi har fått flere transportnett og flere utenlandsforbindelser. Det er også en trend mot at sluttbrukere i økende grad er opptatt av sikker kommunikasjon, og implementerer tiltak for

å spre trafikk og data geografisk og hos flere tilbydere. Disse trendene bidrar til at verdier spres på ulike deler av infrastrukturen, som er med på å begrense de negative konsekvensene av sikkerhetsbrudd hos enkeltstående aktører eller systemer.

På tross av dette er vår vurdering at verdien som bæres over infrastrukturen vil være økende i årene som kommer, som isolert sett er med på å øke risikoen.

3. Geopolitiske trender

Det er mer uro i verden, og spenninger internasjonalt øker behovet for kontroll over kritisk teknologi og teknologisk infrastruktur. Hos våre samarbeidspartnere EU og USA har det de siste årene blitt gjort mye for å styrke kontrollen og sikkerheten med økonomiske avhengigheter, særlig med utenlandske investeringer og viktige verdikjeder. Økt robusthet hos våre samarbeidspartnere kan øke vår egen robusthet, men skaper også forventninger om at vi fatter lignende tiltak her hjemme. Tiltak for nasjonal kontroll må derfor være tilpasset den geopolitiske konteksten, og ikke avvike for mye fra våre nærmeste samarbeidspartnere.

3.1 Utvikling i samspillet mellom teknologi og internasjonal politikk

Samspillet mellom digital teknologi og globale maktrelasjoner har vært i en rivende utvikling over de siste 20 årene. De tidlige fasene av digitalisering var preget av en idé om at digital teknologi var annerledes og krevde tilrettelegging for særegne styreformers hvor ikke-statlige aktører spilte en større rolle. Konflikter om styring og makt dreide seg primært om avgrensede temaer rundt staters atferd, samt internasjonaliseringen av amerikanske nøkkelfunksjoner, mens bredere diskusjoner om sterkere statlig kontroll var lite til stede i vestlige land (DeNardis & Raymond, 2013). Særlig i vestlige land, med amerikanske myndigheter og private teknologiselskaper i spissen, kan dette knyttes til en idé om at minimal politisk intervensjon i styringen av det digitale rom var den beste måten å sikre økonomisk vekst og best utnyttelse av ny teknologi. Selv om denne oppfattelsen hadde grobunn i ideologisk overbevisning og genuin tro på de frigjørende mulighetene for denne teknologien, så var det også påvirket av de rådende maktkonstellasjonene (Powers & Jablonski, 2015). Så lenge vestlige selskaper var dominerende som teknologileverandører var det lite ønske og behov for sterkere statlig inngripen og kontroll.

Argumenter om sterkere statlig kontroll kom i all hovedsak fra autoritære stater som Kina og Russland, som argumenterte for «digital suverenitet» og sterkere statlig kontroll i møte med det de oppfattet som amerikansk dominans (Inkster, 2016; Nocetti, 2015).

Utover 2010-tallet skjedde derimot en rekke utviklinger som satte behovet for nasjonal kontroll høyere på agendaen i Europa og USA. Et første utviklingstrekk så stadig mer politisk oppmerksomhet rundt de nasjonale sikkerhetsutfordringene digitalisering førte med seg. Både konsekvensene og kostnadene av omfattende sikkerhetsbrudd ble gradvis tydeligere. To angrep i 2017, WannaCry og NotPetya, ble samlet estimert til å koste 14 milliarder dollar og førte til omfattende forstyrrelser i en rekke sektorer som helse og global handel (Greenberg, 2018; Berr, 2017). Den økte politiske oppmerksomheten rundt cybersikkerhetsutfordringer skapte en pådriver for sterkere statlig kontroll og regulering for å sikre kritiske samfunnsinteresser. Samtidig førte den økonomiske veksten til Kina - og den stadig sterkere rollen til selskaper som Huawei og ZTE som leverandører av essensielt nettverksutstyr – til at vestlige land måtte ta stilling til teknologiavhengighet til land som ikke var sikkerhetspolitiske allierte (Inkster, 2019). Videre skapte framveksten av monopol-tendenser for essensielle digitale tjenester enda en maktpolitisk dynamikk, hvor den politiske makten og innflytelsen til store teknologiselskaper i økende grad ble problematisert (Bremmer, 2021). Alle disse utviklingstrekkene og tilknyttede bekymringer har blitt definerende for den politiske mobiliseringen rundt sterkere statlig inngripen i vestlige land. Denne alternative forståelsen av digital suverenitet adresserer en rekke sammensatte problemstillinger rundt digital teknologi, som har til felles et ønske om økt politisk kontroll og nasjonal autonomi (Monsees & Lambach, 2022).

I så måte er maktpolitikken rundt digital teknologi tett knyttet til bredere geopolitiske utviklingstrekk, hvor økonomisk politikk og sikkerhetspolitikk i stadig større grad er to sider av samme fenomen. Økte geopolitiske spenninger mellom USA og Kina har gitt seg uttrykk i problematisering av handel mellom de to landene, særlig etter presidentskapet til Donald Trump (Nye, 2020). Samtidig har det også i Europa vært en gradvis vridning mot å se handel og geopolitikk i sammenheng, særlig på EU-nivå (Danzman & Meunier, 2024). Denne eksisterende utviklingen ble ytterligere komplisert av en rekke

uforutsette globale hendelser som satte søkelyset på risikoen nasjonal avhengighet førte med seg, slik som Covid-19 pandemien som illustrerte risikoen i økonomiske avhengigheter, globale verdikjeder, og deres robusthet ovenfor globale kriser (McNamara & Newman, 2020). Mer lokaliserte hendelser som strandingen av Ever Given i Suez-kanalen illustrerte hvordan selv svært lokale hendelser kunne få store globale konsekvenser om de rammet eller tok ut knutepunkter i globale nettverk. Samtidig ble den Russiske invasjonen av Ukraina en illustrasjon på et mer anspent globalt klima hvor militære invasjoner i Europa igjen var et reelt alternativ. Den pågående krigen har også tydelig vist at digital teknologi spiller en nøkkelrolle i moderne krigføring, og er en potensiell nasjonal sårbarhet.

Som følge av den geopolitiske utviklingen de siste 20 årene har digital teknologi gått fra å være et område som tidligere var preget av relativ høy grad av samarbeid, global samhandling, og felles teknologiutvikling, til å bli et av de viktigste stridsområdene mellom stater internasjonalt. Det er også et område som lenge var styrt av private selskaper, og hvor myndigheter i hovedsak var fokusert på å utforme politikk for å fremme økonomisk vekst. Det globale stemningsskifte rundt økonomiske avhengigheter, maktrelasjoner, og sikkerhetspolitikk har derimot skapt et økende press for sterkere statlig innblanding. Av flere har dette blitt omtalt som en ny «æra» og et brudd med den neoliberale konsensusen til global økonomi som har vært førende siden slutten på den kalde krigen (Gerstle, 2022; Roberts, et al., 2019). En rekke land har et økt fokus på å redusere problematiske avhengigheter, styrke nasjonal kontroll og legge sterkere føringer for økonomisk samhandling begrunnet i nasjonal sikkerhet. I denne utviklingen har maktrelasjonene i det digitale rom, karakterisert av sterke avhengigheter, monopolistiske tendenser, og store samfunnsmessige konsekvenser, vært både et nøkkelområde og et område hvor utfordringene ble tidlig synlige. For de kommende årene peker de fleste piler i retning av en enda mer aktiv og intervensjonsvennlig stat som søker sterkere nasjonal kontroll over en kritisk og global infrastruktur.

3.1.1 Sikkerhetsrelaterte hendelser i det digitale rom og ønsker om nasjonal kontroll

Teknologiske og økonomiske avhengigheter blir i dag i økende grad sett på som potensielle sårbarheter som fører med seg risiko for nasjonal sikkerhet. Stemningsskiftet i vestlige land rundt slike avhengigheter, og sikkerhetsutfordringene ved å beholde åpne økonomier, reflekterer en rekke

kjente og reelle risikoer som kan føre til uønskede hendelser.

En kjent problemstilling ved avhengighet av utenlandske teknologileverandører er muligheten for tap av sensitiv informasjon. Digital teknologi er svært kompleks og dynamisk, noe som gjør det vanskelig å spore og verifisere kildekoder. De begrensede mulighetene til å teknologisk verifisere digitale produkter og tjenester begrenser mulighetene for å ta i bruk utstyr fra leverandører man ikke har tillit til (Lysne, 2018). For kritisk digital infrastruktur, som høyst sannsynlig vil bære sensitiv informasjon som er ønskelig å skjeme, vil manglende nasjonal kontroll øke risikoen for at slik informasjon kommer på avveie.

Tilsvarende kan teknologiavhengighet skape usikkerhet rundt kritiske tjenesters tilgjengelighet langs spektrumet fred-krise-krig. For kritisk digital infrastruktur stilles det høye krav til deres tilgjengelighet uavhengig av situasjon, og tilgjengeligheten er særlig viktig ved kriser og en mulig krigssituasjon. Både bortfall av kritiske tjenester, og usikkerhet rundt deres tilgjengelighet, vil i en krisesituasjon være svært problematisk.

En annen utfordring ved manglende kontroll er en utilstrekkelig evne til å sikre verdikjeder. Selv om private selskaper også er avhengige av sine verdikjeder, og har en egeninteresse av å sikre disse, er det ikke gitt at behovet for samfunnsikkerhet blir tilstrekkelig ivarett av markedsdynamikker alene. Ikke minst er dette en risiko under omfattende sikkerhetspolitiske kriser eller store globale kriser som demonstrert under Covid-19-pandemien. For kritisk digital infrastruktur er det essensielt at disse er fungerende ikke bare i spekteret fred-krise-krig nasjonalt, men også ved uforutsette globale kriser eller naturkatastrofer.

Videre kan manglende kontroll føre til en begrenset evne til å påvirke beslutninger og styringsavgjørelser for kritisk infrastrukturleverandører. Beslutninger rundt investeringer, innkjøp, oppkjøp og salg kan alle potensielt påvirke momentene over og bidra til å øke risiko og introdusere sårbarheter. Særlig for kritisk infrastruktur og tjenester kan derfor et behov for økt kontroll også omhandle styringsbeslutninger og tilknyttede konsekvenser.

Digital sikkerhet på samfunnsnivå er kjennetegnet av offentlig-privat samarbeid. Selv om dette samarbeidet delvis er forankret i lovverk og etablerte institusjoner, er det også en betydelig grad av uformelt samarbeid og informasjonsutveksling på flere nivåer involvert i dette arbeidet. For det uformelle samarbeidet er

gjensidig tillit en viktig komponent, og manglende nasjonal kontroll over kritisk infrastruktur kan utfordre denne gjensidige tilliten, og i så måte undergrave det nasjonale arbeidet for digital sikkerhet.

Til slutt er det en risiko ved manglende nasjonal kontroll at Norge blir sett på som problematisk blant våre nærmeste allierte og potensielt en «bakdør» i det sikkerhetspolitiske samarbeidet. Om kontroll over kritisk digital infrastruktur blir vesentlig dårligere enn våre sikkerhetspolitiske partnere kan dette utfordre det bredere samarbeidet, skape friksjon og misnøye, og begrense videre samarbeid. Når britene vurderte å tillate begrenset bruk av Huawei i deres 5G-nettverk indikerte amerikanske myndighetspersoner at dette kunne begrense graden av etterretningsinformasjon de var villige til å dele. For Norge vil det være utfordrende om graden av nasjonal kontroll blir så mangelfull at våre partnere begrenser samarbeidet.

Om manglende nasjonal kontroll introduserer en rekke risikoen er det også risiko forbundet med for omfattende nasjonale kontrolltiltak. Digital infrastruktur er ikke bare viktig på egen hånd, men er en essensiell innsatsfaktor i en rekke sektorer og offentlige funksjoner. Dette gjør økte kostnader og mangelfulle investeringer problematisk og kan over tid bidra til å svekke norsk innovasjon, konkurranseevne og videre utbygging av digital infrastruktur. Om nasjonale kontrolltiltak blir for omfattende kan dette begrense utenlandske investeringer og Norges mulighet til å holde følge med den videre teknologitvillingen.

Manglende harmonisering, særlig med regelverk i EU, kan også skape handelspolitiske utfordringer og begrense Norges evne til å delta i internasjonale og nordiske samarbeid for informasjonsutveksling. Manglende harmonisering vil også øke kostnadene ved å drifte digital infrastruktur i Norge, og bli en belastning for næringslivet som er større enn den ellers hadde trengt å være. En lignende dynamikk kan også oppstå rundt tilgangen på begrensede sikkerhetsressurser og kompetanse, hvor særegne og omfattende nasjonale kontrolltiltak kan hemme tilgangen på begrenset kompetanse ytterligere.

Det er også en risiko for at omfattende nasjonale kontrolltiltak fører til mottiltak mot norske interesser, særlig om tiltakene blir rettet mot enkeltland eller blir oppfattet å være rette mot enkeltland. Både den generelle økningen av geopolitiske spenninger rundt handel og digital teknologi, og en oppfatning av at Norge er særskilt vanskelig i denne utviklingen kan være problematisk. Som en liten og åpen økonomi er det

ikke nødvendigvis i Norges interesse å bidra til ytterligere handelsbarrierer utover kritiske sektorer med særskilt betydning for nasjonal sikkerhet.

3.1.2 Ivaretagelse av nasjonal kontroll i den geopolitiske konteksten

Spørsmålet om nasjonal kontroll og en endret geopolitisk kontekst er ikke bare en avveining mellom ulike risikoen, men også et spørsmål om hva som legges i begrepet nasjonal kontroll. Om nasjonal kontroll forstås som en selvstendig nasjonal evne til styre over alle aspekter av kritisk digital infrastruktur vil omfanget bli særdeles stort, og tilsvarende konsekvensene. Om det derimot forstås noe mer begrenset, som en evne til å forhindre de mest problematiske sikkerhetsmessige konsekvensene av teknologiavhengighet, gjerne i samarbeid med allierte, krever det langt mer begrensede tiltak. For den siste forståelsen henger spørsmålet om nasjonal kontroll også tett sammen med sikkerhetspolitiske utviklingstrekk og potensielt økte geopolitiske spenninger. Dette har både en direkte effekt, i at økte geopolitiske spenninger skaper et økt behov for nasjonal kontroll, og en indirekte effekt i at økte spenninger kan føre til endrede reguleringer og handlingsmønstre hos nære allierte.

Relevante tiltak for økt nasjonal kontroll er de tiltakene som klassifiseres som «defensive» geøkonomiske tiltak, det vil si tiltak som har et primært fokus på å styrke nasjonal motstandskraft og minske sårbarheten for at økonomiske avhengigheter kan misbrukes. Eksempler på tiltak som hører inn under såkalte defensive tiltak er industripolitikk for å diversifisere og øke motstandskraften til verdikjeder, investering og eierskapskontroll, handelspolitiske tiltak mot relevante subsidierte varer, generell sikring av verdikjeder, instrumenter for å motvirke økonomisk maktbruk, sikring av kritisk infrastruktur, og begrensede eksportkontroller for å hindre tap av kritisk teknologi (Danzman & Meunier, 2024).

Investering og eierskapskontroll er relevante tiltak som øker graden av nasjonal kontroll. Gitt at disse er utformet på en måte som harmoniserer med lignende tiltak i for eksempel EU, og håndheves på en måte som tar hensyn til de økonomiske konsekvensene, har de også begrensede negative effekter. Som investeringskontrollutvalget trakk fram i sin anbefaling om innføring av et strengere regelverk i Norge, har de fleste europeiske land allerede utviklet og tatt i bruk lignende regelverk. I samme gruppe er begrensede eksportkontroller for å hindre tap av kritisk teknologi relevant i den grad norske produsenter er ledende på

teknologitvilling på feltet, og sikring av verdikjeder og kritisk infrastruktur er relevant som generelle sikringstiltak.

For et lite land som Norge kan industripolitikk for diversifisering, handelspolitiske tiltak og instrumenter for å motvirke økonomisk maktbruk være relevante, men primært i samarbeid med allierte land. For avgjørelsen om Huawei's rolle i utrulling av 5G-nettverk var det alternative leverandører fra Sverige og Finland, noe som gjorde det mulig å velge utstyrsleverandører fra allierte land. Derimot var det ikke alternative leverandører basert i Norge. I en slik situasjon vil industripolitikk på nasjonalt nivå være kontraproduktivt, mens tiltak som del av en gruppe allierte land som koordinerer politikk og samarbeider ha en gunstig effekt. På den andre siden kan spissede tiltak der alliert samarbeid kommer til kort være relevant i særskilte tilfeller, slik som offentlig støtte til utbygging av flere undersjøiske kabler for å sikre mer diversifisert tilgang til internett nasjonalt.

Samtidig er det her verdt å merke seg betydningen av utviklingen i allierte land. Økende geopolitiske spenninger vil ikke bare øke behovet for kontroll i Norge, men også hos våre allierte. Der det nasjonale handlingsrommet for å utvikle handelspolitiske tiltak og industripolitikk er begrenset, er slike tiltak langt mer aktuelt i en større skala. Som vil bli utdypet i større grad lenger ned, er utviklingen i både USA og EU mot en mye mer intervensjonistisk politikk, særlig for kritiske teknologier. Behovet for nasjonal kontroll ved økte geopolitiske spenninger må derfor sees i lys av dette. En framtidig utvikling hvor vestlige land kollektivt øker sin evne til å levere kritisk teknologi og infrastruktur vil kreve mer begrensede tiltak på nasjonalt nivå.

Gitt industripolitisk koordinering blant vestlige land og et fortsatt tett transatlantisk sikkerhetspolitisk samarbeid vil behovet for nasjonal kontroll derfor være langt mindre. I en slik situasjon er det sannsynlig at leverandører basert i land vi er allierte med vil lykkes i å ta over eller beholde markedsandeler for kritiske tjenester, og at Norge vil kunne benytte seg av disse. Det vil fortsatt være spørsmål om markedskonsentrasjon og skjeve avhengigheter, slik som diskusjonen om europeisk avhengighet av amerikansk teknologi, men behovet for nasjonal kontroll vil påvirkes i mindre grad. Tiltak som investeringskontroll, sikring av

kritisk infrastruktur, og snevre eksportkontroller vil likevel være aktuelle, gitt at de geopolitiske spenningene ikke minsker betraktelig.

Et annet mulig scenario er økt interesse for industripolitikk hos allierte, men forverrede transatlantiske relasjoner og usikkerhet rundt framtiden for det sikkerhetspolitiske samarbeidet. I en slik situasjon vil behovet for større teknologuavhengighet for Europa melde seg for alvor. I den grad det lykkes å etablere et styrket europeisk samarbeid vil dette også minske behovet for nasjonal kontroll, men potensielt øke behovet for harmonisering. Om det europeiske samarbeidet for teknologuavhengighet ikke lykkes, og de transatlantiske relasjonene er under press, vil Norges sikkerhetspolitiske situasjon forverres og behovet for nasjonal kontroll øke betydelig. I en slik situasjon vil Norge måtte se etter nære allierte land, som de nordiske landene, for å bygge en større grad av egen kapasitet gjennom for eksempel industripolitikk og handelspolitiske tiltak. Kostnadene ved en slik utvikling vil trolig være svært høye.

I sum er behovet for nasjonal kontroll, geopolitiske spenninger, og utviklingen i allierte land tett sammenbundet. Av vurderte tiltak³ for å øke kontroll er det kun noen av tiltakene som er relevante på nasjonalt nivå og også for disse er det gunstig å utvikle harmoniserte regelverk i tråd med våre allierte. Økte geopolitiske spenninger stiller større krav til kontroll og etterprøving av sikkerhetspolitiske risikoer forbundet med økonomisk aktivitet i Norge og for leverandører til kritisk infrastruktur. Samtidig er det viktig å treffe balansen mellom tiltak på nasjonalt og overnasjonalt nivå, avveining mellom risiko og kostnad, og behovet for å harmonisere og koordinere politikk med allierte land. I så måte er det høyst relevant å også vurdere utviklingen i reguleringer og politiske tiltak i EU og USA.

3.2 Regulatoriske utviklingstrekk i EU og USA med mål om nasjonal kontroll

Som diskutert over henger behovet for nasjonal kontroll tett sammen med både geopolitiske

³ Industripolitikk for å diversifisere og øke motstandskraften til verdikjeder, investering og eierskapskontroll, handelspolitiske tiltak mot relevante subsidierte varer, generell sikring av verdikjeder, instrumenter for å motvirke

økonomisk maktbruk, sikring av kritisk infrastruktur, og begrensede eksportkontroller for å hindre tap av kritisk teknologi,

utviklinger og utviklingen blant våre nære allierte. Tettere samarbeid og harmonisering av tilnærming i Europa og i det transatlantiske samarbeidet gjør behovet for nasjonale tiltak mindre. Samtidig er det viktig at Norge henger med i den internasjonale regulatoriske utviklingen, både for vår egen sikkerhets del og med tanke på framtidig samarbeid. Denne delen vurderer den regulatoriske utviklingen i USA og EU i stort. En fullstendig gjennomgang av de relevante reguleringene og deres konsekvenser for spørsmål om kontroll er utenfor omfanget at dette prosjektet, men denne delen skisserer opp de generelle utviklingstrekkene og noen av de viktigste reguleringene som et bakteppe for behovet for nasjonale tiltak.

3.2.1 USA

Utviklingen i Washingtons tilnærming er tett knyttet opp til den endrede relasjonen til Kina. Økonomisk vekst i Kina har skapt et gjensidig avhengighetsforhold hvor det fra amerikansk side er en økende skepsis mot avhengigheter til Kina innenfor områder som handel, investeringer og teknologi (Nye, 2020). Denne skepsisen har også stammet fra oppfatningen om at kinesiske selskaper i stor grad opererer i forlengelse av staten, og i så måte er mer eksplisitte geopolitiske aktører. Fra amerikansk side har det vært jevnlig anklager om industrispionasje, subsidier, og begrensninger på amerikanske selskaper i Kina som urettferdige praksiser (Gertz & Evers, 2020). Sett i sammenheng med de gradvis forverrede relasjonene har dette skapt en økt interesse for å begrense tilgangen til særlig kinesiske selskaper i den amerikanske økonomien.

Med Trumps tiltredelse i 2016, endret retorikken rundt global handel seg merkbart fra amerikansk side. Økonomisk velstand ble i sikkerhetsstrategien fra 2017 definert som et mål for nasjonal sikkerhet, og retorisk markerte Trump en tydelig avstand fra frihandel til fordel for en mer nasjonal orientert økonomisk politikk. Skiftet har i stor grad fortsatt under Bidens presidentskap med en rekke subsidier, lån, tariffen og skatteinsentiver for å styrke USAs økonomiske posisjon (Edmonstone, 2024). Disse har vært tydelig motivert av et ønske om å beholde et teknologisk overtak, og sørge for

amerikansk ledelse også i neste generasjons kritiske teknologier. Ledet an av Infrastructure, Investment and Jobs Act (IIJA), Inflation Reduction Act (IRA) og Chips and Science Act er det anslått at USAs samlede investeringer i dette nye paradigmet vil bli opp mot 4 billioner dollar (Graham, 2024).

I tillegg til industripolitikk, har USA strammet grepet og etablert sterkere nasjonal kontroll. Kontroll på investeringer i den amerikanske økonomien har foregått gjennom Committee on Foreign Investment in the United States (CFIUS), etablert i 1975 og som siden har fått utvidede fullmakter ved flere anledninger. I utgangspunktet begrensede myndigheter har blitt utvidet til å kunne blokkere investeringer som truer nasjonal sikkerhet (med en utvidelse i 1988), og også når det gjelder kritisk infrastruktur (utvidelse i 2007). Med Foreign Investment Risk Review Modernization Act i 2018 ble CFIUS igjen gitt større fullmakter og et økt fokus på kritiske teknologier og den kumulative effekten av oppkjøp på markeds kontroll (US Treasury, 2020). I 2022 utstedte Joe Biden en presidentordre som spesifiserte at CFIUS ved utenlandske investeringer skulle særlig vurdere effekten på verdikjeder, amerikansk lederskap i nye teknologier, bredere investeringstrender, cybersikkerhetsrisiko, og risikoen mot persondata for amerikanske personer (US White House, 2022). For utvalgte teknologiske områder har Washington i tillegg indikert en politikk basert på «small yard, high fence» hvor særlige kritiske teknologier og innsatsfaktorene bak disse pålegges strenge begrensninger, også for utgående investeringer, men med ønske om størst mulig grad av åpenhet for handel i andre varer. For 2024 har den oppdaterte listen med kritiske teknologier 18 oppføringer⁴ som til dels kan tolkes bredt, slik som kunstig intelligens (US White House, 2024).

For telekombransjen har det i tillegg vært et fungerende uformelt organ som vurderer sikkerhetsrisikoen ved utenlandsk deltagelse i telekombransjen. Lenge kjent som «Team Telecom», var det en samling av byråer med ansvar for ulike deler av nasjonal sikkerhet som ga råd til den føderale kommunikasjonskommisjonen (FCC) om mulige sikkerhetsrisikoer ved utgivelse av lisenser for å delta i det amerikanske

⁴ Per 2024 inkluderer listen følgende teknologiområder (på originalspråk): Advanced Computing, Advanced Engineering Materials, Advanced Gas Turbine Engine Technologies, Advanced and Networked Sensing and Signature Management, Advanced Manufacturing, Artificial Intelligence, Biotechnologies, Clean Energy Generation and Storage, Data Privacy, Data Security, and Cybersecurity Technologies, Directed Energy, Highly

Automated, Autonomous, and Uncrewed Systems (UxS), and Robotics, Human-Machine Interfaces, Hypersonics, Integrated Communication and Networking Technologies, Positioning, Navigation, and Timing (PNT) Technologies, Quantum Information and Enabling Technologies, Semiconductors and Microelectronics, Space Technologies and Systems

telekommerket. I 2021 ble prosessen formalisert og gitt et tydelig mandat om å vurdere sikkerhet og etterforskningshensyn ved utstedelse av lisenser gitt en viss andel av utenlandsk eierskap (US Department of Justice, 2024). Samtidig ble mandatet utvidet til også å kunne spore tidligere utstedte lisenser i lys av nye sikkerhetsutfordringer.

Videre har USA fra føderal side et sterkere fokus enn tidligere på verdikjeder og mulige avhengigheter. I 2019 annonserte Donald Trump en presidentordre som ga mandat til å utestenge leverandører fra verdikjeden om disse kunne antas å samarbeide med fiendtlige makter (US White House, 2019). En gjennomgang i 2021 av fire kritiske verdikjeder for halvledere, batterier, kritiske mineraler og medisiner illustrerer både den politiske viljen til å styrke nasjonal kontroll og de mange utfordringene (US White House, 2021). Gjennomgangen identifiserte flere flaskehals og utfordringer i de relevante verdikjedene, og påla andre departementer å gjennomføre lignende gjennomganger, men dekket bare fire snevre områder med en metodikk som er lite gjennomførbart i stor skala (Newman & Farell, 2023).

Utviklingen i USA bærer preg av den tiltagende stormaktsrivaliseringen med Kina, og dets konsekvenser for amerikansk ledelse innenfor de fleste viktige teknologiområdene. Tiltakene som har vært satt i verk for å ivareta nasjonal kontroll har derfor vært en kombinasjon av økte minimumskrav for sikkerhet, subsidier og sterke beskyttelser av utpekte teknologier og infrastrukturer, samt målrettede tiltak mot å begrense tilgangen til ikke-allierte stater, med et særlig fokus på Kina.

3.2.2 EU

Mens stormaktsrivaleriet mellom USA og Kina har spilt seg stadig mer ut gjennom økonomisk politikk og teknologi, var EU lenge en mindre aktiv aktør i sammenvevingen av økonomi og sikkerhet. I de senere år har EU likevel vært gjennom et betydelig skifte, med mer omfattende reguleringer og et sterkere behov for teknologisk uavhengighet.

Omkring 2017 skjedde et skifte i Brussels tilnærming til tematikken kontroll og økonomisk sikkerhet. Daværende kommisjonspresident Jean-Claude Juncker uttalte at EU ikke kunne være naive frihandelspromotører og annonserte at unionen skulle arbeide mot en felles europeisk regulering av investeringskontroll. Selv om skiftet dels hadde begynt markerte det overgangen til et EU som formulerte en posisjon i geoøkonomisk politikk («åpen strategisk autonomi»), utdypet gjennom strategier rundt forholdet til Kina (2019), en gjennomgang av handelspolitikken (2021), og

utviklingen av en økonomisk sikkerhetsstrategi ferdigstilt i 2023 (Danzman & Meunier, 2024).

Siden 2017 har regelverket for økonomisk sikkerhet blitt gradvis ekspandert og utvidet med blant annet oppdaterte regler for eksportkontroll (2021), tiltak mot utenlandske subsidier (2023), og et felles instrument mot økonomisk maktbruk samme år. Mest relevant i denne sammenheng er likevel reguleringen rundt investeringskontroll som ble vedtatt i 2019 og vært i bruk siden oktober 2020 (senest utvidet i 2024). Reguleringen gir EU-kommisjonen myndighet til å vurdere og gjennomgå potensielle investeringer, og tar høyde for investorer fra tredjeland som potensielt kan sikre seg effektiv deltagelse i styring av selskapene de investerer i. Medlemslandene skal etablere screening som tar høyde for om investeringene gjelder kritisk infrastruktur, kritisk teknologi, kritiske råvarer, sensitiv informasjon og/eller ytringsfrihet og styring av media. Selv om det ikke skaper regulering på EU-nivå, bidrar det til en sterkere samkjøring og koordinering på europeisk nivå. Et viktig moment er at reguleringen også gir EU-kommisjonen direkte myndighet til å vurdere prosjekter av interesse for EU og/eller de som har betydelig økonomisk støtte fra EU og/eller de som er dekket av særskilt lovgivning. I en utvidelse i 2024 ble tiltak satt i verk for å ytterligere forbedre koordinering på tvers at medlemslandene og tydeliggjøre og heve minstekravene.

Samtidig har EU også iverksatt en rekke tiltak som kan klassifiseres som industripolitikk, primært innenfor definerte og avgrensede sektorer. Viktigst av disse er tiltak for å styrke Europas posisjon innenfor det grønne skiftet og digital teknologi. Industristrategien av 2020 identifiserte disse sektorene som særlig viktige, og en foreslått Chips Act introdusert i 2022 vil sette særlig fokus på Europas avhengighet av importerte halvledere. For kritiske teknologier har kommisjonen også introdusert en Strategic Technologies for Europe Platform (STEP), som skal fasilitere investeringer i særlig kritiske teknologier og styrke Europas uavhengighet. Digitale sektorer som skytjenester, 5G, kunstig intelligens og cybersikkerhet er eksplisitt nevnt som satsningsområder, med en total budsjettamme på 160 milliarder euro. For å styrke satsningen på europeisk teknologi skal prosjekter som støttes av programmet i tillegg få utdelt et «sovereignty seal» for å lettere tiltrekke ytterligere investeringer og verifisere at prosjekter bidrar til økt europeisk autonomi. EU har også iverksatt eller støttet tiltak rettet mot konkrete sektorer, som en lang rekke initiativ for å øke europeisk selvstendighet innenfor skytjenester (BEREC, 2024).

EU har også gradvis markert seg som en mer koordinert og omfattende aktør innenfor cybersikkerhet, regulering av digital teknologi, og beskyttelse av kritisk digital infrastruktur. Nye reguleringer som Digital Services Act (2022) og Digital Markets Act (2022) adresserer ubalanser og manglende kontroll over kritiske digitale tjenester og plattformer og Data Act (2024) skal tilrettelegge for bedre deling av data. De stadig mer omfattende reguleringene rundt cybersikkerhet er både et uttrykk for økende bekymring for digitale sårbarheter og et ønske om å styrke EUs konkurranseevne. Etter Russlands invasjon av Ukraina i 2022 og påfølgende alvorlige cyberangrep rettet mot blant annet kritisk infrastruktur og kommunikasjonsnettverk fikk EU fortgang på en rekke tiltak både på krav til cybersikkerhet, men også harmonisering mellom etater og medlemsland.

I 2023 trådte felles regler for cybersikkerhet under NIS2-direktivet i kraft, som bygget ut det eksisterende NIS-direktivet på samme område. EUs Cybersecurity Act, vedtatt i 2019 og videreutviklet i 2023, styrket den felles-europeiske organisasjonen for cybersikkerhet ENISA og etablerte en sertifiseringsordning for cybersikkerhetsprodukter og tjenester. Cyber Resilience Act, som ble godkjent relativt raskt etter invasjonen av Ukraina i 2022 og som ventes vedtatt i nær framtid, sikter på å heve sikkerhetsnivået for både hardware og software som tilbys på det europeiske markedet, og vil potensielt gi kommisjonen myndighet til å utestenge produkter som ikke har tilfredsstillende standard fra EU.

I sum har EU utviklet seg vesentlig de siste 10 årene til å ta en større og mer omfattende rolle for å ivareta europeiske interesser i styringen av global økonomi og teknologi. Gjennom sitt globale avtrykk som regulatorisk supermakt har EU satt som mål å heve minstenivået for cybersikkerhet og digital regulering både blant sine medlemsland og for teknologileverandører. I tillegg til de stadig mer omfattende reguleringene av digital teknologi har EU endret karakter fra en forkjemper for frihandel og økonomisk åpenhet, til en mer strategisk orientert geoøkonomisk aktør. Dette har både gitt seg uttrykk i en rekke reguleringer som strammer kontrollen over økonomisk samhandling, koordinering blant medlemslandene i møte med

økonomisk maktbruk, og gryende investeringer i nøkkelindustrier for å styrke europeisk teknologiavhengighet og handlingsrom. Draghi-rapporten, utgitt i 2024 som et innspill for EUs framtidige industrielle politikk, peker ut en retning for Europa som går enda lenger i å bruke økonomisk politikk for å styrke Europas strategiske posisjon og geopolitiske innflytelse (Draghi, 2024). Hvilken retning EU tar videre, og i hvilken grad tiltakene for å styrke europeisk uavhengighet lykkes, vil ha stor betydning for Norges handlingsrom og behov for nasjonal kontroll.

3.2.3 Oppsummering

Det er mer uro i verden, og spenninger internasjonalt øker behovet for kontroll over kritisk teknologi og teknologisk infrastruktur.

Der teknologiutvikling globalt lenge var preget av samarbeid og sterke gjensidige avhengigheter, har sikkerhetsbekymringer rundt disse avhengighetene skapt et økende behov for sterkere nasjonal kontroll. Hos våre samarbeidspartnere EU og USA har det de siste årene blitt gjort mye for å styrke kontrollen og sikkerheten med økonomiske avhengigheter, særlig med utenlandske investeringer og viktige verdikjeder.

For Norges del peker den globale utviklingen mot et behov for å øke nasjonal kontroll også her hjemme, samtidig som tiltakene må være balanserte og i harmoni med tiltakene i andre land. Norge som en liten åpen økonomi er avhengige av samarbeid med leverandører og land som vi har et sikkerhetspolitisk samarbeid med for å kunne levere trygge og gode digitale tjenester. Dermed vil behovet for nasjonal kontroll bli påvirket av arbeidet i EU og USA med å bygge opp mer robuste og autonome verdikjeder.

Over de neste 5-10 årene er det sannsynlig at verdikjeder i EU og USA blir mindre avhengige av leverandører fra land som vi ikke har et sikkerhetspolitisk samarbeid med. Økt robusthet hos våre samarbeidspartnere vil da være med på å øke vår egen robusthet. Gitt en slik utvikling vil tiltakene for nasjonal kontroll kunne være mer begrensede, tilpasset alliertes tiltak, og målrettet mot risikoer forbundet med for eksempel investeringer og eierskap.

4. Markedsmessige og teknologiske trender

I Norge er både fiberinfrastrukturen og 5G-nettet godt bygget ut, og eies og driftes i dag av kjente selskap med nordiske eiere. Bruk av skyteknologi og kunstig intelligens kan endre hvordan 5G-nettverkene driftes i fremtiden. Det er mange strategiske samarbeid mellom ulike aktører i verdikjeden om innovasjon. Innen datalagring ser vi at det kan bli økende interesse for å investere i datalagringscentre i Norge. Satellitteknologi kan avhjelpe brudd i informasjonsinfrastrukturen i en beredskapssammenheng som følge av naturkatastrofer eller liknende, men det er usikkert om det er tilstrekkelig tilbud av satellitter til å tilby Norge nødvendig kapasitet i en konfliktsituasjon.

4.1 Høye krav til digital infrastruktur øker behovet for investeringer

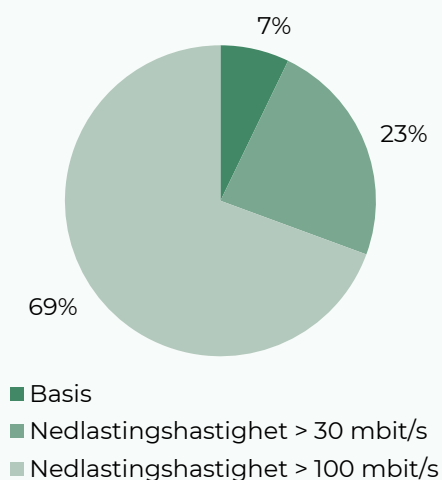
Som drøftet tidligere driver høyere krav til den digitale infrastrukturen frem et behov for investeringer. Overgangen til et femte generasjons mobilnettverk (5G) er sentral for at flere smarte gjenstander kan fungere optimalt. Overgangen til et 5G-nett krever imidlertid store investeringer fra teleoperatørene som eier og driver nettverkene (Deloitte, 2024). Investeringene i fast fiberinfrastruktur i transportnettene ligger stort sett bak oss, men det er både i EU og Norge utfordringer knyttet til å øke andelen husstander som er tilknyttet fibernetet.

Norge

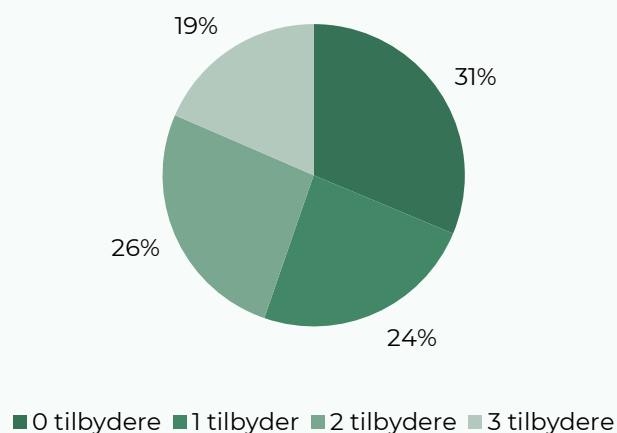
I Norge har utbyggingen av 5G-nettverkene kommet langt, selv om det fremdeles er behov for investeringer. I følge Nkom (2023) hadde 69 prosent av husholdningene i første halvår 2024 tilgang de raskeste hastighetene på over 100 Mbits per sekund. Dette er en økning på 7 prosent siden fjoråret (se Figur 4-1 (Nkom, 2024)). Utbyggingen av det tredje mobilnettet kommer også stadig lengre, slik at valgmulighetene øker for en stadig større del av befolkningen. 19 % av befolkningen hadde

Figur 4-1: Husholdningers internetthastighet og tilgang til tilbydere

a) Hastighet



b) Tilgang til tilbydere per husstand



Mbit/s og % antall husholdninger

Tilbydere med mer enn 100 Mbit/s

Kilde: (Nkom, 2023). Forklaring:

tilgang fra alle de tre mobilnettene (Telenor, Telia, Ice) på de hastighetene som er i Nkoms høyeste kategori. 26 prosent av husstandene kan velge mellom to tilbydere, mens 24 prosent kun har høyeste hastighet fra en mulig tilbyder (se Figur 4-1)

Utbyggingen av transportnettet for fiber har kommet langt i Norge, selv om det fremdeles er utfordringer knyttet til aksessnett for kunder som er bosatt i rurale områder, og svak konkurranse i enkelte områder.

Europa

I enkelte andre europeiske land har man kommet svært kort med utrulling av fullverdige 5G-nett. Dette fører til at det mellom enkelte EU-land nesten er en generasjons forskjell i mobilnett, og også ulikheter i utbyggingen av dekningsfor fibernet. Dette er en bekymring for EU-kommisjonen, som peker på at utbyggingen ikke er i rute til å nå målene som er fastlagt i strategien for EUs digitale tiår (European Commission, 2023).

Sett under ett anser Kommisjonen at den digitale infrastrukturen i EU ikke enda er tilstrekkelig utbygget til å bære behovet for trafikk som en mer data-drevet og digital økonomi vil skape. EU-kommisjonen anslår at det er et investeringsbehov på mellom 150 – 220 milliarder euro for å få et fullverdig 5G-nett i tråd med EUs målsettinger (European Commission, 2024).

Flere rapporter som drøfter europeisk konkurransedyktighet og fremtiden til det indre marked, peker på behovet for velutbygget kommunikasjonsinfrastruktur for at EU skal lykkes med å bli en konkurransedyktig, grønn og digital økonomi i fremtiden (Draghi, 2024; Letta, 2024).

Organisering av eierskapet i infrastruktur

For de selskapene som eier infrastruktur har det i en periode vært utfordrende å synliggjøre hvilke verdier disse infrastrukturinvesteringene bidrar til å bygge opp i selskapene som eier dem. Det har også vært et behov for å rendyrke den delen av virksomheten som har som oppgave å eie og å drifte infrastruktur.

Telenor har for eksempel samlet sitt eierskap i infrastruktur i et eget selskap, Telenor Infrastruktur. Ifølge Telenor skal selskapet synliggjøre den underliggende verdien i infrastruktur og utvikle dette som forretningsområde videre. Selskapet skal

også øke ressursutnyttelsen ved å optimalisere drift og betjene eksterne kunder (Telenor, 2024). Forretningsområdet har ansvar for tårn, fiber og datasentre i Norden. Telenor har etablert 100 prosent eide tårnselskaper i Norge, Sverige og Finland og eier 50 prosent av felleskontrollerte tårnselskaper i Sverige (Net4Mobility, 3GIS) og Danmark (TTT) (Telenor Towers, 2024). Telenors fibernet ble skilt ut i et eget selskap med Telenor som majoritetseier (70%) og to andre finansielle medeiere.⁵ Transaksjonen verdsatte fibernet til Telenor til 36 milliarder kroner (Telenor, 2022).

Telia har også en målsetting om å samarbeide med eksterne parter for å realisere verdier og å videreutvikle sine digitale infrastruktureiendeler. Selskapet skilte i 2021 ut sine tårn i Norge og Finland i et eget selskap, og solgte 49 prosent av eierandelene til eksterne investorer (Telia Company, 2021).⁶

Global Connect, som har et av de mest omfattende fibertransportnettene i Norge ble i 2017 solgt til det svenske oppkjøpsfondet EQT. Fondet solgte en 15 prosent eierandel av Global Connect til Abu Dhabis statlige investeringsfond Mubadala (Mubadala, 2022). Salget ble vurdert av regjeringen å ha betydning for nasjonal sikkerhet, og ble derfor behandlet i henhold til statens retningslinjer for screening. Regjeringen godkjente transaksjonen på visse vilkår som har som mål å ivareta nasjonale sikkerhetsinteresser (Regjeringen, 2023).

4.2 Finansieringsbehov ved ny infrastruktur kan endre konkurransen i markedet

Rapportene til både Letta og Draghi stiller spørsmålsteget ved om dagens organisering av det europeiske telekommunikasjonsmarkedet tillater bygging av europeiske telekomaktører som har tilstrekkelig kapital og teknologi og kompetanse til å drive frem investeringer i digital infrastruktur.

De viser til at amerikanske mobil-selskaper har langt flere kunder per operatør, og langt høyere profittmarginer per kunde. USA er imidlertid ett nasjonalt mobilmarked, mens telekommarkedet i EU fremdeles består av nasjonale markeder.

Liberalisering av nasjonale monopoler

Svært mange av de største operatørene i Europa er arvtakere til statlige regulerte telemonopoler som hadde nasjonale markeder som sine utgangspunkt. Dette inkluderer selskaper som Deutsche Telekom, Orange, Telefonica, BT Group, Telenor og Telia. Flere av disse har fortsatt en nasjonalstat som største eier, og i noen få tilfeller også majoritetseier.

Det er også flere aktører der staten har solgt seg helt ut – der BT Group i Storbritannia trolig er det mest prominente eksemplet. I Norden er den norske stat majoritetseier i Telenor og den svenske stat har et betydelig minoritetseierskap i Telia (41%). I Finland, Danmark og Island har statene solgt seg helt ut av de historiske statlige telemonopolene (hhv. Sonera/TeliaSonera, TDC og SIminn). Historiske statlige monopoler som BT Group (UK) og TDC (Danmark) har i dag sine største eiere i hhv. India og Australia.

Siden liberaliseringen av telekommarkedene, med oppløsning av de statlige telemonopolene har det vært sterk vektlegging av regulering for å legge til rette for nyetablering i markedet. I denne perioden har det vokst frem en betydelig tilstedeværelse av nye selskaper som i *ikke* har røtter i historiske statlige monopoler. Særlig aktørene Vodafone og CK Hutchison (også kjent under merkevaren «3») har en betydelig tilstedeværelse i mange land. I Norge er mobiloperatøren ICE et eksempel på det samme.

I en periode har det vært betydelig grad av internasjonalisering på eierskapssiden. Vodafone har i utgangspunktet røtter i Storbritannia, men har et statlig UAE-basert selskap som største eier. CK Hutchison er eid av et privat Hong Kong-basert investeringsselskap med blant annet Li Ka-Shing på eiersiden. Al Telekom er en aktør med tilstedeværelse i flere øst-europeiske land og er i dag eiet av det mexicanske selskapet America Movil, med Carlos Slim på eiersiden. Aktører som Deutsche Telekom, Telefonica, Orange, Liberty Global, Telenor og Telia har betydelig tilstedeværelse i mange land.

Konvergens mellom fiber og mobilnett

Over de siste 10-20 årene har vi sett en rekke oppkjøp og fusjoner mellom eiere av mobilbasert og kabelbasert infrastruktur både i Norge og Europa. Eksempler fra senere år i Norge er Telias oppkjøp av Get/TDC i 2018, og Lyse sitt oppkjøp av ICE i 2022. I Danmark kjøpte bredbåndsaktøren Norlys i 2024 opp Telia sin danske mobilvirksomhet.

Det er tilsvarende eksempler i hele Europa. For eksempel har både Telefonica og Vodafone kjøpt hver sine fastnettaktører i Tyskland. Telenor har fra

relativt gammelt av vært aktive både innen mobilbasert og kabelbasert infrastruktur i både Sverige, Danmark og Finland gjennom oppkjøp av bredbåndsaktører i disse landene.

Generelt ser vi at største mobilselskapene i Europa også er blant de største aktørene innenfor både bredbånd til sluttbrukere og regional og nasjonale fibertransportnett. Skillet mellom mobil og fiber viskes videre ut ved at flere teleselskaper tilbyr lokalt 5G-nett til næringsbygg via fiber, og at enkelte husstander tilbys «trådløst bredbånd» via 5G.

Fremdeles nasjonale markeder

Til tross for at det har vært en periode med betydelig konsolidering, har det også vært nedvalg og fraksjoner som tyder på at det kan være krevende å ha virksomhet i flere land enn i kjernemarkedet, selv innen EU/EØS. Eksempelvis hadde Telenor mobilvirksomhet i Bulgaria, Ungarn, Montenegro og Serbia, men solgte ut sin virksomhet i 2018. Telenor etablerte seg samtidig i Finland i 2019. Telenor har fortsatt en stor tilstedeværelse i utvalgte land i fremvoksende markeder. Telia har hatt en lignende utvikling. I dag er selskapet primært aktive i Norden og Baltikum, men har tidligere vært aktive blant annet i Spania, Moldova, Tyrkia og Aserbajdsjan. I 2024 solgte Telia seg også ut av sin mobilvirksomhet i Danmark. Tele2 er i dag kun aktive i Sverige og Baltikum, men har tidligere vært til stede i Østerrike, Kroatia, Danmark, Norge, Frankrike, Tyskland, Italia, Nederland og UK.

Frem til nå har EU-kommisjonen og nasjonale konkurransemyndigheter og telekommyndigheter i Europa opprettholdt en streng fusjonskontroll for fusjoner mellom konkurrerende mobiloperatører i samme nasjonale marked. Det har særlig vært et fokus på å opprettholde flere uavhengige mobilnett for å opprettholde konkurransen.

Enkelte tar til orde for å endre dette for å tillate konsolideringer av operatører i samme marked. Dette er kontroversielt, og flere andre aktører, slik som ECTA peker på at konkurransepolitikken har bidratt til rimelige priser på telekom tjenester i Europa, særlig sammenliknet med USA.

Spørsmålet i det videre er om EU-kommisjonen dreier mot å vektlegge hensynet til å bygge større europeiske selskaper, med muskler til både å finansiere infrastruktur noe sterkere enn hensynet til konkurranse i markedet og lave priser til konsumentene.

4.3 Geopolitisk rivalisering gjør utbygging av infrastruktur dyrere

Samtidig som investeringsbehovene vokser, har globale spenninger mellom Kina og vestlige land ført til at rimelige leverandører som skapte mer konkurranse nå holdes utenfor markedet. Deres tilstedeværelse kunne potensielt redusert kostnadene ved utbygging og drift av nettene, samt bidratt med mer innovasjon og raskere teknologiutvikling.

Globalt er det fire store helintegreerte tilbydere av 5G-nettverksinfrastruktur Huawei, Nokia, Ericsson, og ZTE (Lenninghan, 2024). Ifølge markedsanalysebyrået Dell Oro Group hadde disse fire aktørene om lag 70 % av markedet i 2023. Huawei er den største aktøren globalt, og er markedsleder i Asia, Sør-Amerika og Afrika. Huawei har også hatt noe tilstedeværelse i Europa, men her er det Ericsson og Nokia som er markedsledere. I USA er også Nokia og Eriksson markedsledere, men med utfordrere som amerikanske Cisco og Sør-koreanske Samsung (Bicheno, 2024).

Den økende spenningen mellom USA og Europa på den ene siden og Kina på den andre siden har ført til at Huawei og ZTE har blitt valgt bort som tilbydere av utstyr og tjenester i USA og flere europeiske land. I USA gikk reguleringene så langt som å pålegge mobiloperatører som benyttet utstyr fra Huawei å erstatte dette med utstyr fra leverandører som er godkjent av amerikanske myndigheter («rip and replace») (Braverman, et al., 2021).

I Norge ga regjeringen føringer for hvordan sikkerhetsloven måtte forstås som innebar at teleoperatører måtte sørge for at minst halvparten av nettet ble bygget ut med utstyr fra land Norge har sikkerhetspolitiske samarbeid med. I praksis medførte dette at operatørene ikke kunne ha Huawei som eneleverandør av nettverkstjenester. Både Telia og Telenor annonserte at de ville bruke Ericsson som leverandør for utbygging av 5G-nettet (Zondag & Tollersrud, 2019).

Reguleringene som har ekskludert ZTE og Huawei har hatt sikkerhetspolitiske begrunnelser i de landene hvor de har blitt innført. I praksis har resultatet vært at Nokia og Ericsson sin markedsposisjon har blitt styrket. De kinesiske tilbyderne har hevdet at reguleringene har hatt proteksjonistiske motiver. I Europa mener de at motivet har vært å beskytte europeiske verdikjeder tilknyttet Nokia og Ericsson, mens de har anklaget USA for å benytte sikkerhetspolitiske begrunnelser

for å beskytte voksende amerikanske leverandører som Samsung og Cisco.

Flere er bekymret for at konsentrasjonen i markedet for infrastruktur i Europa og USA vil føre til at det blir svakere konkurranse og høyere priser ved utbygging av nett i Europa og USA (kilde). En annen bekymring er knyttet til at de europeiske leverandørene vil tilby utstyr som er teknologisk underlegent det som kinesiske leverandører alternativt kunne tilbudt, og at dette vil føre til dårligere infrastruktur. Bekymringen knytter seg ikke bare til den potensielt svakere konkurranse, men også til at investeringene i forsknings-utvikling og innovasjonsarbeid hos de to europeiske leverandørene til sammen kun utgjør en tredjedel av det som investeres hos Huawei (Morris, 2024).

4.4 Infrastrukturen kan utnyttes og bygges bedre ved bruk av ny teknologi

Samtidig som mengden datatrafikk i nettet vil øke i fremtiden, er det teknologier som gjør at man kan utnytte nettet bedre. I dette avsnittet vil vi beskrive hvordan skyteknologi og kunstig intelligens kan påvirke hvordan ekomtjenester leveres i fremtiden.

Bruk av skyteknologi

BEREC har i en egen rapport beskrevet hvordan skyteknologi benyttes av telekomselskaper i dag, og hvordan det kan komme til å benyttes i fremtiden (BEREC, 2024). De finner at telekomselskaper har en risikobasert tilnærming til hvilke typer tjenester som plasseres i skytjenester som de ikke drifter selv. Typisk plasserer de tjenester med lav risiko ut i allmenne skytjenester. Eksempler på dette er tjenester knyttet til oppfølging av kunder, som fakturering, kundeanalyser eller oppfølging av leverandører. Foreløpig er det derimot få telekomaktører som har valgt å plassere mer kritiske funksjonene, som drift av kjernenettene, ut i allmenn sky. Disse driftes i hovedsak egne løsninger.

Videre finner rapporten at det er en trend mot økt bruk av teknologier som benyttes i skytjenester i for å drifte nettverkene, som virtualisering av kjernettnettfunksjoner. Bruk av virtualisering, softwarbaserte nettverk og virtualiserte nettverksfunksjoner gjør det mulig å kontrollere og styre nettverkene ved hjelp av software fremfor dedikerte fysisk hardware, som routere og svitsjer. Dette gjør at kontrollen og styringen av nettverkene kan sentraliseres. Dette bidrar til at nettverkene kan driftes mer effektivt, og reduserer behovet for investeringer i ytterligere nett. Samtidig

vil det øke kompleksiteten i netten, og øke verdien på operasjonene som gjøres sentralt.

Virtualisering av nettverksfunksjoner er særlig benyttet i mobilnettverk. I BERECs rapport oppgis at det har vært utbredt bruk av virtualisering av nett i mobilnettverk over de siste 6-7 årene (BEREC, 2024). Med virtualisering av nettverksfunksjonene er det i økende grad mulig å drifte nettverkene fra en sky. Selv om det testes ut å benytte skyteknologi for å operere kjernenettfunksjoner, virker det som at det er få som har valgt å plassere kjernefunksjoner i allmenne skytjenester. I enkelte land har telekomselskaper inngått samarbeid med skytjenesteleverandører hvor de tester ut å plassere 5G-kjernen i virtuelt lukkede skytjenester fra allmenne skyleverandører.

Deutsche Telekom og Google annonserte i 2022 et strategisk samarbeid for å utforske hvordan nye nettverksmodeller kan ta i bruk kraften i både skyteknologi og «edge computing» innen drift av kjernenettet, analyse av nettverket og analyse av brukeropplevelsene i nettverket. Samarbeidet ble videre forsterket i 2023, da de samme aktørene sammen med Ericsson annonserte at de hadde demonstrert gjennom en pilot hvordan kjernenettet til Deutsche Telekom kan migreres til Google Distributed Cloud Edge. Ifølge aktørene demonstrerte piloten hvordan skybaserte løsninger kan gjøre nettet raskere, mer fleksibelt og mer skalerbart i fremtiden (Geelen, 2023)).

Kunstig intelligens for drift av nettverk

I fremtiden vil kunstig intelligens og maskinlæring kunne benyttes på flere områder av telekomselskaper. BEREC har gjennomført en undersøkelse blant telekomoperatører i Europa om hvordan de tror kunstig intelligens og maskinlæring vil kunne benyttes i telekomsektoren i fremtiden (BEREC, 2023). Det pekes blant annet på at ved overgang til mer bruk av softwarebaserte nett og visualiserte nettverksfunksjoner, vil kunstig intelligens og maskinlæring kunne benyttes for å automatisk drifte og kontrollere nettverkene, optimalisere bruken av nettene, forutse fremtidig behov og skreddersy løsninger til kunder mm. I rapporten anslås det at det er sannsynlig at bruken av AI-applikasjoner for operasjonell drift vil være normen i løpet av de neste 6 til 10 årene blant telekomselskaper. Videre vil overgangen til AI-tjenester kunne føre til at skyleverandører må oppdatere deler av infrastrukturen for å sørge for at de har tilstrekkelig prosessorkraft for å kunne drifte KI-applikasjoner.

Mange telekomoperatører inngår derfor strategiske samarbeid med ulike aktører for å teste ut mulighetene for å benytte kunstig intelligens i sin

drift. For eksempel har Telenor inngått et samarbeid med Nvidia for å utvikle KI-applikasjoner for blant annet å drifte sine nettverk i Norden.

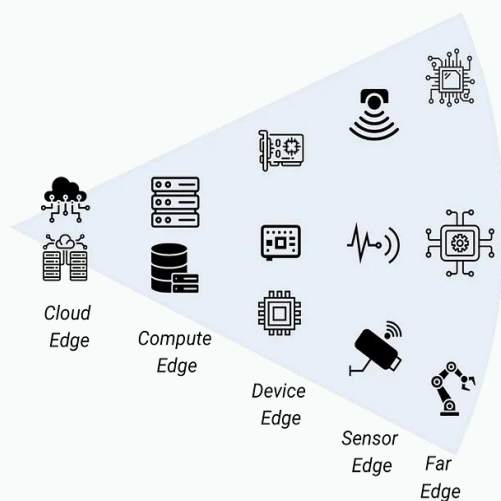
Open-RAN

I 5G-nettverkene har det også vært en utvikling mot virtualisering av funksjonene ved basestasjonene, såkalt OpenRAN. Dette gjør det mulig å splitte mellom software og hardware, hvor det tradisjonelt har vært benyttet dedikert hardware. Hardware for flere basestasjoner kan deretter samles i mindre edge-datasentre nærmere basestasjoner. OpenRAN gjør det mulig å kjøpe hylleware hardware, og kan bidra til å øke konkurransen om leveranser av ulike komponenter til basestasjoner. Det kan gi mobilnettverksoperatører større fleksibilitet i valg av leverandør, og at kontroll og drift av basestasjonen kan gjøres sentralt fra en sky.

Både OpenRAN og virtualisering av nettverksfunksjoner gjør at 5G-nettverkene utvikler seg i retning av en tjenestebasert skyarkitektur. Dette innebærer at 5G nettet kan driftes fra en sky, og hvor applikasjoner og tjenester for å drifte nettene kan leveres via åpen APIer, som for eksempel OpenGateway initiativet. Dette er et samarbeidsprosjekt mellom både skyleverandører, mobilnettverksoperatører og tredjepartsleverandører som er ledet av GSMA, som er en bransjeorganisasjon for mobiloperatører som arbeider for standardisering og innovasjon innenfor mobiloperatørmarkedet. Gjennom åpne APIer får mobilnettverksoperatørene tilgang til en felles plattformer for utvikling av applikasjoner for drift av mobilnettverk som kan deles mellom ulike operatører. Dette gjør at mobilnettverksoperatører raskt kan implementere nye applikasjoner for drift av nettene.

Flere peker på Open-RAN-teknologi som en mulighet til å bygge ut 5G-nettet på en mer kostnadseffektiv måte (Wooden, 2023).

Figur 4-2: Ulike former for Edge



Kilde: (Munday, 2023)

Markedsandelen til Open-Ran økte raskt gjennom 2021-2023, og er forventet å ha en markedsandel på mellom 6-10 prosent innen utgangen av 2024. Dell' Oro Group forventer at markedsandelen vil øke til mellom 15 og 20 prosent innen 2027.

I USA har Biden-administrasjonen avsatt 1,5 milliarder amerikanske dollar i et fond for innovasjon i leverandørleddet for nettverksutbyggere, med mål om å gjøre Open-RAN teknologi sikkert, effektivt og kommersielt konkurransedyktig (National Telecommunications and Information Administration, 2024). Amerikanske myndigheter bygger også partnerskap med andre lands myndigheter for å promotere rimeligere utbygging av 5G-infrastruktur, særlig i land hvor det fra USAs side er ønskelig å demme opp for kinesisk innflytelse og kinesiske teknologileverandører (Lenninghan, 2024). I tillegg er flere av de ledende leverandørene av Open-RAN arkitektur⁷ og produsentene av deler til Open-RAN-teknologi amerikanske. Et markeds-gjennombrudd for Open-RAN vil antagelig betydelig styrke markedsposisjonen til disse amerikanske selskapene.

I Europa har det vært noen pilotprosjekter med utprøving av Open-RAN teknologi i regi av utbyggere av 5G-infrastruktur. Vodafone har

implementert arkitekturen på flere hundre basestasjoner i Storbritannia, og planlegger å utvide dette til flere tusen. Tilsvarende planlegger Deutsche Telekom å ha implementert teknologien på 3000 basestasjoner innen 2026. I Norge forventer vi ikke bruk av Open-RAN i løpet av de neste 5-8 år, blant annet av hensyn til driftssikkerhet i nettet.

Forventningene om rask utrulling av Open-RAN teknologi har generelt blitt justert ned noe i løpet av 2023, både på grunn av teknologiske komplikasjoner ved utrulling, og fordi de etablerte RAN-aktørene har vist seg mer konkurransedyktige enn forventet (Satari, 2024a).

Eksempler på samarbeid om utrulling av Open-RAN i USA mellom telekomtilbydere slik som AT&T, tradisjonelle RAN-leverandører som Ericsson og produsenter av deler Fujitsu, viser at utrulling av Open-RAN kan vise seg å bli mer en gradvis overgang til en mer åpen og kostnadseffektiv arkitektur, enn en revolusjonær disruptjon av de tradisjonelle RAN-leverandørene.

Edge computing

Det er forventet at det i fremtiden vil bli økt etterspørsel etter at prosessering og lagring av data skjer nærmere sluttbruker, såkalt edge computing. Edge computing er alternativet til at informasjon sendes frem og tilbake til et sentralt plassert datasenter, potensielt i et annet land eller en verdensdel. Det er ofte litt ulikt hva som legges i edge. Figur 4-2 viser en enkel fremstilling av ulike former for edge. Edge computing kan både foregå i et mindre datasenter nær sluttkunden. Videre kan edge også innebære at sluttkunden installerer servere i egen bygning, eller at enhetene eller sensorene har innebygd prosessorkapasitet.

Flere nettverksoperatører (mobil og fast bredbånd) ser derfor på mulighetene til å tilby lagring og prosesseringskapasitet lenger ut i sine nettverk, for eksempel ved basestasjoner eller mindre datasentre (MECs). Dersom de har virtualisert sitt mobilaksessnettverk (VRan eller OpenRAN), vil de også kunne co-lokalisere hardware som benyttes til mobilaksessnettverket og med hardware som benyttes til slutt kunder.

Edge computing gjøres for å redusere tidsforsinkelse, bedre brukeropplevelse, øke sikkerheten og redusere bruken av transporttjenester. I fremtiden er det forventet at det vil bli et økt behov for prosessering nærmere

⁷ For eksempel Parallel Wireless, Mavenir og JMA Wireless.

sluttbruker som følge av utviklingen av Internet of Things, virtuell virkelighet og bruk av kunstig intelligens.

Kunstig intelligens på edge

Det krever stor prosesseringskapasitet for å trene store språkmodeller. Dette gjør at selve treningen av slike modeller sannsynligvis vil måtte gjøres sentralt i større datasentre. Etter at treningen er overstått, vil modellene kunne tolke og analysere ny data basert på kunnskap den har opparbeidet seg fra treningsdatasettet, såkalt «Inference» (Zhou, et al., 2019).

En trend er at deler av prosessering knyttet til store språkmodeller muligens skal kunne gjennomføres på edge, og da særlig det som er knyttet til Inference. Fordelen med dette er at det vil redusere behovet for transitt mellom sluttbruker og datasenteret, det vil redusere tidsforsinkelse og at enheter ikke vil trenge å være koblet til internett for at KI-applikasjonene skal kunne fungere. Derfor er det flere selskaper som arbeider med å utvikle teknologi som gjør det mulig å kjøre KI-applikasjoner på edge.

Flere telekomoperatører ser derfor på muligheten for å kunne tilby tilstrekkelig prosessor- og lagringskapasitet langt ute i sine nettverk som kan være med å understøtte KI-applikasjoner hos sluttbrukere i fremtiden. Det er flere samarbeidskonstellasjoner mellom ulike aktører i verdikjeden som. Blant annet har Nvidia, Ericsson, Nokia og T-Mobile et samarbeid om å etablere et AI-RAN Innovation Center. Målet er å utvikle en plattform for å utvikle løsninger som gjør det mulig å benytte kunstig intelligens for å optimalisere mobilnettverkene, men også hvordan de kan levere edge computing tjenester til sluttbruker som understøtter deres bruk av kunstig intelligens (T-Mobile, 2024).

Per i dag kan det virke som at edge computing og desentralisering av prosesseringsressurser fortsatt er på et tidlig stadium. Vi ser allikevel at det etableres en rekke samarbeidskonstellasjoner mellom skyleverandører og telekomselskaper om samarbeide om å levere distribuerte skytjenester innenfor telekomaktørens nettverk og leverandører av komponenter til mobilaksessnettverk, som Ericsson og Nokia, og leverandører som Nvidia.

Strategiske samarbeid

Generelt sett er det en gjennomgående trend at det er mange strategiske samarbeid mellom ulike aktører i verdikjeden om å utvikle nye produkter og tjenester, men også hvordan de kan utfylle hverandre og bundle tjenester som selges til sluttbruker.

4.5 Lokal prosesseringskraft og reguleringer kan endre datasentermarkedet

Det er forventet at det vil skje relativt store endringer i markedet for lagring og prosessering av data. Utviklingen av store språkmodeller vil kreve stor prosesseringskraft for å trene modellene. Dette gjør at det er behov for en ny generasjon datasentre (high performance datacenters) som har stabil tilgang til energi og har stor prosesseringskraft. Trening av modellene har heller ikke behov for å gjennomføres nær sluttbruker. Denne trenden taler derfor for økt bygging av nye store sentraliserte datasentre med stor prosesseringskraft i områder med stabil tilgang på store mengder kraft. Dette førte blant annet til at Meta annonserte at de terminerte en kontrakt om å bygge ut to datasentre i Danmark, siden de opprinnelige datasentrene som var planlagt bygd ikke ville støtte AI-tjenester (Reuters, 2022). Dette har som konsekvens at eksisterende datasentre ikke nødvendigvis har et så stort konkurransefortrinn ovenfor nye datasentre for å støtte KI-applikasjoner.

Norge kan være et attraktivt sted å etablere neste generasjons datasentre. Dette skyldes blant annet at vi har tilgang på regulert grønn energi, kaldt klima og god forbindelse til utlandet. Derfor kan det tenkes at flere aktører vil velge å etablere datasentre som understøtter KI i Norge i fremtiden.

Videre har vi allerede nevnt at en mulig trend er at det vil bli økt etterspørsel etter lokal prosessering og lagring lengere ute i nettene. Her ser vi at telekomoperatører inngår i samarbeid med skyleverandører om å tilby lagring og prosessering av data i deres nett.

Til sist er det mange virksomheter som ikke ønsker å benytte kommersielle skytjenester grunnet regulatoriske krav, behov for mer kontroll over egne data eller av økonomiske grunner. De drifter enten datasentre i egenregi eller benytter leverandører av datasentertjenester. Enkelte aktører kan også spesialisere seg på å skreddersy skyløsninger som passer med europeiske eller nasjonale reguleringer eller krav pålagt fra kunder gjennom leverandørkjeder.

4.6 Rimelig satellitteknologi komplementerer den digitale infrastrukturen på jorda

Satellitter er en voksende del av den digitale infrastrukturen. Dette er særlig drevet av teknologiske fremskritt som har gjort størrelsen på

satellittene mindre. Det amerikanske selskapet SpaceX, med sine Falcon 9-raketter og Starship-programmet, har gjort oppskytninger mer kostnadseffektive og hyppigere gjennom gjenbrukbare raketter (McKinsey & Company, 2023).

Over de siste årene har det vært en rask utvikling i tilbudet av bredbånd fra lavbanesatellitter. I dag er ikke bredbånd et fullverdig alternativ til bakkebasert bredbånd. Vi forventer heller ikke at satellitter vil konkurrere med bakkebasert infrastruktur i bebygde områder i nær fremtid. Derimot vil lavbanesatellitter kunne være et supplement til bakkebaserte bredbåndsnett i områder uten mobildekning, og i situasjoner med utfall i mobilnettene.

Lavbanesatellitter har også mulighet til å koble seg direkte til mobiltelefoner og IoT-instrumenter (direct-to-device). Fremfor å måtte bruke dedikerte satellittelefoner vil det derfor være mulig for mobiltelefoner og IoT-instrumenter å koble seg til satellitt i områder uten mobildekning. Dette vil bedre mulighetene for å innhente data fra sensorer utenfor dekning. Eksempler på dette kan være temperaturmålinger, overvåkningsinstrumenter eller sporingsinstrumenter på redningsvester langt til havs. Videre samarbeider lavbanesatellitt-selskaper med både telekomoperatører og mobiltelefonprodusenter om å kunne levere tjenester i områder uten dekning. Blant annet har Apple lansert en SOS-funksjon på alle modeller nyere enn iPhone14 som gjør det mulig for brukere å sende tekstmelding til nødetater i områder utenfor mobildekning.

Vi ser en utvikling hvor selskapene som tilbyr satellitt-tjenester blir en del av den digitale kommunikasjonsinfrastrukturen ved å inngå strategiske samarbeid med enten teleselskaper, eller skyleverandører. For eksempel har Space X både samarbeid med T-Mobile om å tilby 5G mobildekning i områder med dårlig tilkobling, og samarbeid med Microsoft Azure om å tilby skytjenester via satellitttilkobling (Satari, 2024b). Flere liknede partnerskap mellom satelittselskaper, telekomselskaper og hyperscalers har blitt annonsert de siste årene.

Veksten i satellittmarkedet drives først og fremst av det private markedet og noen privateide selskaper hjemmehørende USA. I USA kjøper det offentlige tjenester av flere leverandører i satellittmarkedet, og bidrar slik sett til veksten i etterspørselen. Det globale markedet for satellittkommunikasjon nådde en verdi på over 41 milliarder dollar i 2023, og markedet forventes å vokse med 50 prosent til over 60 milliarder dollar i 2028. Veksten forventes særlig innen markedet for mobilt satellittbasert internett

til områder uten fiber, samt internett til maritim sektor og til luftfarten (Research and Markets, 2024).

I Europa har det vært en politisk målsetting å bidra til en europeisk romindustri og et nettverk av satellitter som reduserer avhengigheten av amerikanske privateide selskaper, og den amerikanske staten. Dette har motivert mer direkte offentlig finansiering av satellittmarkedet.

Kina er det landet som etter USA skyter opp flest, og kontrollerer flest satellitter i bane rundt jorden. Det er imidlertid lite samarbeid mellom kinesiske og vestlige leverandører, og lite integrasjon i verdikjedene for satellitter i de to økosystemene.

4.7 Oppsummering

Ettersom vår avhengighet av digitale tjenester og produkter øker, blir også den digitale infrastrukturen mer verdifull. Næringslivets verdikjeder er avhengig av de digitale verdikjedene. Den digitale infrastrukturen er derfor viktig for hele samfunnet. Myndigheter på nasjonalt og flernasjonalt nivå anser god tilkobling og høy hastighet som en forutsetning for konkurransekraft i næringslivet og gode tjenester til innbyggerne. Denne avhengigheten gjør at den digitale infrastrukturen må tåle stadig mer, og nå ut til stadig flere. For å tåle den økte etterspørselen, og nå ut til flere ser vi tre trender som vi vil beskrive i dette kapitlet.

For det **første** driver den økte bruken av infrastrukturen frem behov for investeringer i økt kapasitet. I Norge ligger det store investeringer bak oss og et kontinuerlig behov for vedlikehold og oppgraderinger. I Europa er det fremdeles store investeringsbehov med tilhørende kapitalbehov for enda ikke er finansiert. For å tåle investeringene peker flere på at telekomselskapene må få sterkere finansielle muskler, og at man må legge til rette for større europeiske telekomselskaper. Selv om det har vært noen konsolideringer på tvers av land, er markedsstrukturen i EU fremdeles preget av at det er mange nasjonale telekommarkeder heller enn ett felles telekommarked. På grunn av nasjonale reguleringer er det også begrensede gevinster å hente ved konsolideringer på tvers av land. Dette hindrer fremveksten av større europeiske teleselskaper. For å vokse ønsker enkelte selskaper derfor å gjennomføre fusjoner internt i de nasjonale markedene. Dette har blitt vurdert til å være i strid med europeisk konkurranselovgivning. Enkelte krefter ønsker å endre EUs konkurransepolitikk for å legge til rette for fremvekst av større europeiske teleselskaper.

En kompliserende faktor i denne sammenhengen er de geopolitiske spenningene mellom Vesten og Kina som har bidratt til konsentrasjon og svekket konkurranse i leverandørmarkedet for 5G-infrastruktur. De kinesiske leverandørene Huawei og ZTE har blitt utestengt fra USA, og sterkt begrenset i EU. Dette har ført til bekymring om leverandørene Nokia og Ericsson vil levere tilstrekkelig innovative produkter, og hvilken kostnad deres produkter eventuelt vil ha.

For det **andre** forventer vi at ny teknologi vil bidra til å optimalisere bruken av infrastrukturen og å redusere kostnadene ved utbygging av ny infrastruktur. Bruk av skyteknologi, kunstig intelligens og «edge computing» er sentrale teknologier for å bidra til å optimalisere bruken av nettet både for operatørene og for brukerne av nettet. Teknologier med åpen arkitektur som skiller software fra hardware øke konkurransen i utbyggingen av 5G-infrastrukturen, og driver frem innovasjon.

Vi ser at det vokser frem stadig flere strategiske samarbeid mellom tradisjonelle telekomaktører og leverandører av innovative teknologiske løsninger. Det er også strategiske samarbeid mellom telekomselskaper og amerikanske skytjenesteselskaper. De ulike landene har ulik tilnærming til bruken av ny teknologi i nettet, og samarbeidet med større teknologigiganter. USA fremmer åpen arkitektur i 5G-nettet, og subsidierer amerikanske selskaper som jobber for dette. EU ønsker å fremme sine europeiske verdikjeder, og

ønsker også å regulere bruken av skytjenester og lagring av europeiske data.

Et utviklingstrekk er at flere tjenester har behov for at data lagres og prosesseres nærmere sluttbruker. Blant annet er det en utvikling mot at deler av prosesseringen i store språkmodeller kan gjøres lokalt. Flere telekomoperatører har derfor inngått i samarbeidskonstellasjoner med innovative selskaper og skyleverandører for å tilby lagring og prosessering som understøtter KI-applikasjoner lenger ute i sine nett. Holdt sammen med de europeiske og nasjonale reguleringene for lagring av data ser vi at det vil vokse frem et marked for datalagring som består av en flora av ulike typer lagring og skytjenester i fremtiden. Vi ser også at etableringen av datasentre fører med seg investeringer i utenlandsforbindelser mellom datasentre i Norge og andre land, samt investeringer i mørk fiber mellom datasentre i Norge.

Den **tredje** og siste måten nettet kan avlastes på er ved hjelp av satellitteknologi. Ny teknologi har gjort satellittene mer kommersielt konkurransedyktige. I noen områder kan derfor satellitter konkurrere med kostnadene knyttet til utbygging av fiber eller 5G-nett. Bruk av satellitter kan derfor spare unødig store kostnader i nettutbygging og kan også fungere som beredskap i områder med sårbar tilgang. Satellittinfrastrukturen kan imidlertid ikke bære de store mengdene datatrafikk som utveksles i verden, og er et supplement og ikke en konkurrent til den øvrige digitale infrastrukturen.

5. Forventet markedsstruktur på mellomlang sikt

Basert på informasjonen vi har samlet og vår forståelse av de geopolitiske, teknologiske og markedsmessige trendene peker vi på hvordan vi forventer at eierskapsstrukturen i den digitale infrastrukturen vil utvikle seg. Det vil alltid være usikkerhet knyttet til hvordan markedsstrukturen vil se ut på mellomlang sikt.

5.1 Infrastruktur for 5G-nett

Infrastrukturen for 5G-nett er i dag godt utbygget i Norge sammen med andre land, med tre tilbydere flere steder. Med den videre utbyggingen av 5G-nettet forventer vi at Norge vil ha tre fullverdige 5G-nett med høy båndbredde på mellomlang sikt. Infrastrukturen driftes av Telenor, Telia og ICE, og eierskapet kontrolleres også av teleselskapene gjennom heleide eller majoritetsseide datterselskap. Telenor, Telia og ICE har henholdsvis staten som majoritetsseier, svenske stat som kontrollerende minoritetsseier og kraftselskapet Lyse, som igjen eies av kraftkommuner i Stavangerregionen, som eier. Det er med andre ord overveiende norsk eierskap, og for øvrig noe nordisk eierskap i 5G-infrastrukturen. Vi forventer at eierskapet i 5G-infrastrukturen vil forbli slik som beskrevet på mellomlang sikt.

I Europa vil det antagelig foregå utbygging av 5G-nett i flere år før det er en infrastruktur på plass som er i tråd med de politiske målsettingene. Hvorvidt det vil bli gjennomført konsolideringer i markedet gjenstår å se, og vil blant annet avhenge av EU-kommisjonens vektlegging av konkurransen i markedet versus oppbygging av europeiske «champions». Antagelig vil det i leverandørkjeden for utbygging av 5G foregå mye innovasjon.

I flere land foregår dette gjennom pilotering og utprøving av Open-RAN-løsninger, og softwaredefinerte nettverk og forsøk med skybaserte løsninger for drift av kjernenett. Innovasjonen vil antagelig skje i samarbeid mellom etablerte leverandører i telekom, og teknologiselskaper i tilstøtende markeder. Samlet sett kan dette gjøre leverandørkjedene noe mer komplekse, og oppmerksomhet rettet mot leverandører kan være like relevant som fokus på eierskap av den fysiske infrastrukturen. I Norge

virker det som man er avventende til å ta i bruk enkelte av disse teknologiene.

5.2 Nasjonal og regional fiberinfrastruktur

I aksessmarkedet for fibernet i Norge er det i dag et stort antall aktører, delvis fordi regionale aktører har stått for utbyggingen av fiber i ulike områder av landet. Bak oss ligger en periode med utbygging og deretter oppkjøp og konsolideringer av små- og mellomstore aktører. Det kan fremdeles komme flere konsolideringer i markedet for aksessnettet..

Den grunnleggende fiberinfrastrukturen som utgjør transportnettet er også godt bygget ut, og dimensjonert for mer trafikk. Telenor har det mest omfattende transportnettverket. Også Global Connect, Telia og Lyse har utbygget kommersielle transportnett i Norge. Eierskapsstrukturen er organisert slik at det er norske eller nordiske aktører som kontrollerer mye av infrastrukturen, med innslag av private fondsinvestorer. Kun Global Connect er heleid av private aktører, med en svensk hovedeier og en minoritetsseier i Abu Dhabi. Eierskapet for denne eierandelen er underlagt vilkår fra regjeringen.

Vi forventer at eierskap til grunnleggende fiberinfrastruktur vil være en stor verdi i fremtiden, og forventer ikke at noen av markedsaktørene vil ønske å selge kontrollerende eiendeler i infrastrukturen. Videre viser eksempelet med salget av minoritetsseiendelen av Global Connect at store endringer i eierskapet i infrastruktur utløser stor oppmerksomhet. For selskapene er det risiko for at eventuelle transaksjoner kan bli stoppet med hjemmel i sikkerhetsloven. Dette begrenser hvilke transaksjoner vi kan forvente at selskapene vil ønske å forsøke å gjennomføre.

I Europa ser vi på samme måte at selskaper som eier og driver telekomvirksomhet også er eiere av grunnleggende fiberinfrastruktur, men at det er en trend mot synliggjøring av verdien av infrastrukturen gjennom deling av eierskap mellom telekomselskaper og finansielle investorer.

5.3 Internasjonal fiberinfrastruktur

I dag bygges det ut stadig flere undersjøiske fiberkabler som kobler ulike kontinenter og regioner sammen. Det er enkelte selskaper som er eiere av global fiberinfrastruktur som forbinder

både land og kontinenter. Europeiske aktører som kontrollerer slik global fiberinfrastruktur er blant annet Arelion (SW), Telecom Italia Sparkle (IT), Orange (FR), Telxius (ES) Deutsche Telekom (GE) og Liberty Global (NL).

En trend er at de store allmenne skyleverandørene står for en stor andel av utbyggingen av sjøfiberkabler mellom sine datasentre i ulike land. Det er også forventet at disse vil stå for hovedvekten av utbyggingen av nye sjøfiberkabler i fremtiden. Skytjenesteleverandørene har bygd ut nye fiberkabler alene, eller de har deltatt i konsortier hvor skyleverandører samarbeider med spesialiserte leverandører av internasjonal fiberinfrastruktur for bygging av infrastrukturen. Det er også en trend mot bruk av såkalt «Open Access» som gjør det mulig for investorer og tredjeparter å kjøpe seg tilgang til utvalgte fiberpar i undersjøiske kabler som legges av skyleverandører. Investeringer som gjøres av de store skyleverandørene kan derfor være med på å redusere terskelen for tredjeparter å etablere egne private nettverk og mørk fiber mellom kontinenter.

5.4 Bredbånd via satellitt

Markedet for kommersielle satellitter kontrolleres av private eiere i USA, men med staten som viktig kunde. Det største selskapet innen kommunikasjon via satellitter er Starlink (US) som er en del av selskapet SpaceX. Dette kontrolleres av den grunnleggeren Elon Musk. Den internasjonale skytjenesteleverandøren Amazon planlegger å ta opp konkurransen med Starlink gjennom sitt «Project Kuiper». Amazon (US) kontrolleres av grunnlegger Jeff Bezos. Det Europeiske selskapet OneWeb med base i Storbritannia, eies av franske Eutelsat Group. Selskapet er børsnotert og eies av private equity fond, den britiske staten og det indiske telekomselskapet Bharti Enterprises Ltd.

De neste årene forventer vi kraftig vekst i antall satellitter som blir tilgjengelige for kommunikasjonsformål. Veksten vil antagelig være drevet av selskaper som SpaceX og Amazon.

5.5 Lagring

I fremtiden tror vi at de allmenne skyleverandørene vil fortsette sin markedsdominans globalt, og at en stor mengde av data vil lagres i hyperscale datasentre rundt om i verden. De store allmenne skyleverandørene er også godt posisjonert for å etablere neste generasjons datasentre for å kunne kjøre treningsmodeller for store språkmodeller for generativ kunstig intelligens.

Det er flere forhold som kan tale for at Norge kan være egnet for etablering av neste generasjons datasentre. Blant annet har vi tilgang på regulerbar grønn energi, kaldt klima og god forbindelse til utlandet. Videre vil det fortsatt være behov for colocation datasentre i fremtiden for å dekke behov til kunder som ønsker mer kontroll over egne data. Innenfor dette segmentet er det i dag flere aktører som tilbyr tjenester i Norge, hvor de fleste er hel- eller deleid av utenlandske investorer. Dette taler for at det vil etableres flere datasentre i Norge i årene som kommer. Det krever store investeringer og kompetanse for å etablere og drifte datasentre. I Nkoms årsrapport for internett i Norge i 2024 pekes det også på at utfordringer knyttet til byggetillatelse og tilgang på strøm kan kjøre det krevende for utenlandske aktører å etablere datasentre i Norge (Nkom, 2024). Derfor tror vi at eventuelle nye datasentre vil etableres av eksisterende aktører i markedet. Samtidig kan det være at disse aktørene kjøpes opp helt eller delvis av utenlandske investorer.

Innenfor edge er det en trend mot at telekomoperatører samarbeider med skyleverandører om å etablere lagring og prosessering av data langt ute i deres nettverk. Videre er det flere skyleverandører som tilbyr distribuerte skyløsninger hvor data og prosessorkapasitet kan innplasseres on-premise hos sluttbruker.

5.6 Nærmere om skyleverandørene sine rolle

De store amerikanske skyleverandørene bygger som nevnt ovenfor i økende grad ut egen infrastruktur mellom datasentre. Videre har de over de siste årene blitt store aktører av CDN-tjenester, og Amazon vil også kunne tilby bredbånd fra satellitt direkte til sluttbrukere. Det har derfor vært et spørsmål om skyleverandører vil konkurrere mot etablerte mobil- fibernettleverandører. Trenden er derimot at skyleverandørene inngår samarbeid med de mer tradisjonelle telekomoperatørene. Skyleverandørene kjøper transporttjenester ut til sluttkunde, mens telekomoperatørene kjøper skytjenester for mindre kritiske data. Videre samarbeider de om å kunne levere prosessering og lagring av data lenger ut i nettene, forskning på utvikling av applikasjoner som kan forbedre nettverkene og utforsker hvordan de kan bundle tjenester som kan selges til telekomoperatørens sluttkunder.

6. Oppsummering om risiko og behov for nasjonal kontroll

Verdi: vår avhengighet av digitale tjenester

Norge har en befolkning med høy digital kompetanse, og som raskt tar i bruk nye digitale tjenester. Teknologiske fremskritt over de siste 30 årene har ført til at vi i dag er ett av de mest digitaliserte samfunnene i verden. Mange av verdikjedene i samfunnet er direkte eller indirekte avhengige av digitale tjenester, og vi har en av de mest digitaliserte offentlige sektorene i verden. Vi som samfunn blir derfor i økende grad avhengige av den underliggende digitale infrastrukturen.

I årene som kommer forventer vi at vårt samfunn vil bli stadig mer digitalisert. Regjeringens digitaliseringsstrategi legger klare mål for at Norge skal bli det mest digitaliserte samfunnet i verden innen 2030 (Digitaliserings- og forvaltningsdepartementet, 2024). Teknologiske trender som bruk av kunstig intelligens, skytjenester, virtuell virkelighet og en fortsatt økning i antall IoT-enheter vil være med å øke bruk av internett, og at digitale tjenester blir en stadig mer integrert del av verdikjeder i samfunnet.

Samtidig er det viktig å påpeke at den digitale infrastrukturen ikke er en enkeltstående enhet, men bestående av flere aktører og systemer. Over de siste årene har vi hatt en trend mot mer diversifisering i enkelte deler av infrastrukturen, blant annet ved at vi har fått flere transportnett og flere utenlandsforbindelser. Det er også en trend mot at sluttbrukere i økende grad er opptatt av sikker kommunikasjon, og implementerer tiltak for å spre trafikk og data geografisk og hos flere tilbydere. Disse trendene bidrar til at verdier spres på ulike deler av infrastrukturen, som er med på å begrense de negative konsekvensene av sikkerhetsbrudd hos enkeltstående aktører eller systemer.

På tross av dette er det allikevel vår vurdering at verdien som bæres over infrastrukturen vil være økende i årene som kommer, som isolert sett er med på å øke risikoen for sikkerhetsbrudd.

Trussel: det geopolitiske bakteppet

Det er mer uro i verden, og spenninger internasjonalt dreier seg i økende grad om kontroll over kritisk teknologi og teknologisk infrastruktur. Der teknologiutvikling globalt lenge var preget av relativt samarbeid og sterke gjensidige avhengigheter, har sikkerhetsbekymringer rundt

disse avhengighetene skapt et økende behov for sterkere nasjonal kontroll.

I våre samarbeidspartnere EU og USA har det de siste årene blitt gjort mye for å styrke kontrollen og sikkerheten med økonomiske avhengigheter, særlig med utenlandske investeringer og viktige verdikjeder. For Norges del peker den globale utviklingen mot et behov for å øke nasjonal kontroll også her hjemme, samtidig som tiltakene må være balanserte og i harmoni med tiltakene i andre land.

Norge som en liten åpen økonomi er avhengige av samarbeid med leverandører og land som vi har et sikkerhetspolitisk samarbeid for å kunne levere trygge og gode digitale tjenester. Dermed vil behovet for nasjonal kontroll bli påvirket av arbeidet i EU og USA med å bygge opp mer robuste og autonome verdikjeder. Over de neste 5-10 årene er det sannsynlig at verdikjeder i EU og USA blir mindre avhengige av leverandører fra land som vi ikke har et sikkerhetspolitisk samarbeid med. Økt robusthet hos våre samarbeidspartnere vil da være med på å øke vår egen robusthet.

Gitt en slik utvikling, vil tiltakene for nasjonal kontroll kunne være mer begrensede og målrettede mot risikoer forbundet med for eksempel investeringer og eierskap.

Sårbarhet: teknologiske og marked for tilbud av kritisk digital infrastruktur

I Norge er både fiberinfrastrukturen og 5G-nettet godt bygget ut, og eies og driftes i dag av kjente selskap med nordiske eiere. Dette reduserer sårbarheten for denne infrastrukturen. Samtidig er vi at det foregår mye teknologisk innovasjon i hvordan 5G-nettet vil driftes i fremtiden. Teknologiske innovasjoner og samarbeid med utenlandske aktører som for eksempel bidrar til å drifte kjernenettet kan føre til mer kompleksitet i verdikjedene. Vi forventer ikke at norske aktører vil inngå i samarbeid som medfører at de mister kontroll med kritisk infrastruktur. På den annen side kan for stor grad av alenegang gjøre infrastrukturen mer sårbar fordi norsk teknologiutvikling ikke vil være tilstrekkelig til å henge med på den internasjonale utviklingen. Vi er avhengig av å være integrert med utenlandske verdikjeder.

Innen datalagring ser vi at det kan bli økende interesse for å investere i datalagringscentre i Norge. Utenlandske investeringer i datasentre i

Norge er med på å gjøre infrastrukturen mer robust, fordi økt lagringskapasitet, flere utenlandsforbindelser og mer mørk fiber diversifiserer infrastrukturen ytterligere. På den annen side vil eierskapet til datalagringscentrene antagelig forbli på utenlandske hender, og det kan være utfordrende for norske myndigheter å ha kontroll med det reelle eierskapet i sentrene.

Satellitteknologi kan avhjelpe brudd i informasjonsinfrastrukturen i en beredskapssammenheng som følge av naturkatastrofer eller liknende, men det er usikkert om det er tilstrekkelig tilbud av satellitter til å tilby Norge nødvendig kapasitet i en konfliktsituasjon.

Samlet risiko

Det er ambisiøst å skulle si noe overordnet om den samlede risikoen i den kritiske digitale infrastrukturen. Med vårt analyseapparat har vi imidlertid noen perspektiver som kan være verdt å avslutte med.

For det første ser vi ikke noen samlet økt risiko knyttet til eierskap av kritisk digital infrastruktur. Systemet som helhet fremstår robust. For det andre er hovedvekten av den underliggende infrastrukturen kontrollert av norske eller nordisk eide selskaper som er kontrollert av statlige eller kommunale foretak i sine respektive land. For det tredje er systemet diversifisert, slik at verdiene som bæres over infrastrukturen er fordelt på flere aktører og systemer. Vi er for eksempel ikke avhengig av ett datasenter, ett mobilnett, én utenlandskabel eller liknende. Den siste årsaken er at verdien av den digitale infrastrukturen er så stor

at det vil være krevende å eie tilstrekkelig til å true systemet.

Dette betyr imidlertid ikke at det ikke er elementer i systemet det kan være verdt å ha ekstra oppmerksomhet rettet mot. Her vil vi trekke frem eierskap i datasentre i Norge. Per nå er dette spredt på ulike aktører, men dersom det oppstår konsentrasjon på eiersiden vil det være relevant for myndighetene å ha oppsyn med hvem som er de reelle eierne av datasentrene.

Som vi har drøftet vil også mer komplekse verdikjeder kunne gjøre at det bli uoversiktlig å ha kontroll med hvem som tilbyr innsatsfaktorer som inngår i infrastrukturen. Dette kan gjøre det vanskelig å ha tilstrekkelig informasjon om alle underleverandørene, og man kan stå ovenfor ukjente risikoer i verdikjeden. På den annen side bidrar et høyere antall leverandører til at man diversifiserer avhengigheten, og blir mindre avhengig av en enkelt aktør. Dette reduserer risikoen i verdikjeden.

Til sist kan det legges til at utfordringer knyttet til kritisk digital infrastruktur ikke er unike for Norge. Mange allierte land er opptatt av dette, og internasjonalt samarbeid bidrar til å utvikle teknologi, senke risiko i verdikjeder og kontrollere eierskap.

Den største risikoen for Norge vil være – på dette området som på flere andre områder – å bli stående utenfor et fellesskap av likesinnede land som sammen blir sterkere ved å dele ressurser, teknologi og kompetanse.

7. Referanser

A2, 2021. *Kartlegging av drift og forvaltning av IKT-løsninger i statlige virksomheter*, s.l.: A-2 Norge AS.

Amazon, 2024. *What is Network Latency?*.

[Internett]

Available at: <https://aws.amazon.com/what-is/latency/>

[Funnet 11.10.2024].

BEREC, 2023. *BEREC Report on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation*, Riga: BEREC.

BEREC, 2024. *BEREC Report on Cloud and Edge Computing Services*, Riga: BEREC.

Berr, J., 2017. "WannaCry" ransomware attack loses could reach \$4 billion. [Internett]

Available at:

<https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>

[Funnet September 2024].

Bicheno, S., 2024. *Global RAN market declined by 11% in 2023*. [Internett]

Available at: <https://www.telecoms.com/wireless-networking/global-ran-market-declined-by-11-in-2023>

[Funnet September 2024].

Braverman, B., Browne, M. T. & Mark, J., 2021. *Let Her Rip! FCC Adopts Remove-and-Replace Rules*.

[Internett]

Available at:

<https://www.dwt.com/insights/2021/01/fcc-huawei-zte-rip-and-replace-rules>

[Funnet September 2024].

Bremmer, I., 2021. *The Technopolar Moment: How digital powers will reshape the global order*. *Foreign Affairs*.

Bøhn, E. D. et al., 2024. *Generativ kunstig intelligens i Norge*, s.l.: Forskningsrådet.

Coe, N. M. & Yeung, H. W.-c., 2015. *Global Production Networks: Theorizing Economic Development in an Interconnected World*. Oxford: Oxford University Press.

Danzman, S. B. & Meunier, S., 2024. *The EU's Geoeconomic Turn: From Policy Laggard to Institutional Innovator*. *Journal of Common Market Studies*, 3 Mars, pp. 1097-1115.

Datatilsynet, 2018. *Skytjenester*. [Internett]

Available at:

<https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/>

[Funnet September 2024].

Deloitte, 2024. *2024 Telecommunications industry outlook*, s.l.: Deloitte .

DeNardis, L. & Raymond, M., 2013. *Thinking Clearly About Multistakeholder Internet Governance. GigaNet: Global Internet Governance Academic Network*, 14 November.

Digital Norway, 2021. *VR & AR: Slik tar bedrifter det i bruk*. [Internett]

Available at: <https://digitalnorway.com/vr-og-ar-slik-tar-bedrifter-det-i-bruk/>

[Funnet 15 Mars 2023].

Digitaliserings- og forvaltningsdepartementet, 2024. *Fremtidens digitale Norge*. [Internett]

Available at:

<https://www.regjeringen.no/no/dokumenter/fremtidens-digitale-norge/id3054645/>

[Funnet 30 September 2024].

Direktoratet for sikkerhet og beredskap, 2019.

Risikoanalyse på samfunnsnivå, Tønsberg:

Direktoratet for sikkerhet og beredskap.

Draghi, M., 2024. *The future of European competitiveness - A competitiveness strategy for Europe*, Brussels: European Commission.

Edmonstone, G., 2024. *Economic security policies compared: The United States, its allies and partners*. [Internett]

Available at: <https://www.ussc.edu.au/economic-security-policies-compared-the-united-states-its-allies-and-partners>

[Funnet September 2024].

European Commission, 2023. *2030 Digital Decade - Report on the state of the Digital Decade 2023*.

[Internett]

Available at: <https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade>

[Funnet 26 September 2024].

European Commission, 2024. *White Paper: How to master Europe's digital infrastructure needs?*, Brussels: European Union.

Finansdepartementet, 2024. *Perspektivmeldingen 2024*, Oslo: Regjeringen.

Geelen, A., 2023. *Deutsche Telekom, Google Cloud, and Ericsson Demonstrate Network*

Transformation Milestone with 5G Cloud-Native Network Pilot. [Internett]
Available at:
<https://www.telekom.com/en/media/media-information/archive/5g-cloud-native-pilot-shows-efficiency-1026992>
[Funnet September 2024].

Gereffi, G., Humphrey, J. & Sturgeon, T., 2005. The Governance of Global Value Chains. *Review of International Political Economy*, Februar, pp. 78-104.

Gerstle, G., 2022. *The Rise and Fall of the Neoliberal Order: America and the World in the Free Market Era*. New York: Oxford University Press.

Gertz, G. & Evers, M. M., 2020. Geoeconomic Competition: Will State Capitalism Win?. *The Washington Quarterly*, 16 Juni, pp. 117-136.

Greenberg, A., 2018. *The Untold Story of NotPetya, the most Devastating Cyberattack in History*. [Internett]
Available at: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
[Funnet September 2024].

Helsedirektoratet, 2023. *Digitale helsetjenester (e-helse/telemedisin)*. [Internett]
Available at: <https://www.helsedirektoratet.no>
[Funnet August 2024].

Helsedirektoratet, 2024a. *Helsenorge*. [Internett]
Available at: <https://www.ehelse.no/strategi/e-helsemonitor/aktiv-medvirkning-i-egen-og-n%C3%A6res-helse/helsenorge>
[Funnet September 2024].

Helsedirektoratet, 2024. *Bruk av digitale helsetjenester*. [Internett]
Available at: <http://www.helsedirektoratet.no>
[Funnet August 2024].

Hu, K., 2023. *ChatGPT sets record for fastest-growing user base - analyst note*, s.l.: Reuters.

IBM, 2020. *Introducing IBM Cloud for Telecommunications with 35+ Partners Committed to Join IBM's Ecosystem and Help Drive Business Transformation*. [Internett]
Available at:
<https://newsroom.ibm.com/Introducing-IBM-Cloud-for-Telecommunications-with-35-Partners-Committed-to-Join-IBMs-Ecosystem-and-Help-Drive-Business-Transformation>
[Funnet September 2024].

Inkster, N., 2016. *China's Cyber Power*. 1 red. London: Routledge.

Inkster, N., 2019. The Huawei Affair and China's Technology Ambitions. *Survival*, 29 Januar, pp. 105-111.

Justis- og Beredskapsdepartementet, 2022. *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet*, Oslo: Regjeringen.

Kano, L. & Oh, C. H., 2020. Global Value Chains in the Post-COVID World: Governance for Reliability. *Journal of Management Studies*, 15 September, pp. 1773-1777.

Kommunal- og moderniseringsdepartementet, 2016. *Digital agenda for Norge*, Oslo: Regjeringen.

Kommunal- og moderniseringsdepartementet, 2020. *Strategi for kunstig intelligens*. [Internett]
Available at:
<https://www.regjeringen.no/no/dokumenter/nasjon-al-strategi-for-kunstig-intelligens/id2685594/>
[Funnet September 2024].

Lenninghan, M., 2024. *Global telecoms kit market slides as carriers stop spending*. [Internett]
Available at: <https://www.telecoms.com/5g-6g/global-telecoms-kit-market-slides-as-carriers-stop-spending#close-modal>
[Funnet September 2024].

Lenninghan, M., 2024. *US and India announce joint Open RAN plans. Again*. [Internett]
Available at: <https://www.telecoms.com/open-ran/us-and-india-announce-joint-open-ran-plans-again>
[Funnet September 2024].

Letta, E., 2024. *Much More Than a Market: Speed, Security, Solidarity*, Brussels: European Council .

Lysne, O., 2018. *The Huawei and Snowden Questions. Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?*. s.l.:Springer International Publishing.

McKinsey & Company, 2023. *Space Launch: Are we heading for oversupply or a shortfall?*. [Internett]
Available at:
<https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/space-launch-are-we-heading-for-oversupply-or-a-shortfall>
[Funnet September 2024].

McNamara, K. R. & Newman, A. L., 2020. The Big Reveal: COVID-19 and Globalization's Great Transformations. *International Organization*, 14 September, pp. E59-E77.

Methri, G., 2022. *4 popular Payment Gateways in Norway*, s.l.: IBS intelligence.

Microsoft, u.d. *Hva er offentlige, private og hybride skyer?*, s.l.: Microsoft.

Monsees, L. & Lambach, D., 2022. Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, 9 September, pp. 377-394.

Morris, I., 2024. *Huawei amid sanctions beats Ericsson and Nokia on every measure*. [Internett] Available at: <https://www.lightreading.com/5g/huawei-amid-sanctions-beats-ericsson-and-nokia-on-every-measure> [Funnet September 2024].

Mubadala, 2022. *EQT infrastructure broadens investor base in Global Connect*. [Internett] Available at: <https://www.mubadala.com/en/news/eqt-infrastructure-broadens-investor-base-globalconnect> [Funnet 17 okotber 2024].

Munday, B., 2023. *Deploy and Run LLMs at the Edge*. [Internett] Available at: <https://medium.com/getmodzy/deploy-and-run-llms-at-the-edge-90b8523f6d85> [Funnet September 2024].

National Telecommunications and Information Administration, 2024. *Public Wireless Supply Chain Fund*. [Internett] Available at: <https://www.ntia.gov/funding-programs/public-wireless-supply-chain-innovation-fund> [Funnet September 2024].

NAV, 2023. *NAVs omverdensanalyse 2023-2035*, s.l.: NAV.

Newman, A. & Farrell, H., 2023. *The New Economic Security State: How Derisking Will Remake Geopolitics*. [Internett] Available at: <https://www.foreignaffairs.com/united-states/economic-security-state-farrell-newman> [Funnet September 2024].

Nkom, 2023. *Bredbåndsdekning*. [Internett] Available at: <https://nkom.no/statistikk/nokkeltall-og-interaktive-dashbord/bredbandsdekning> [Funnet September 2024].

Nkom, 2024. *Internett i Norge - Årsrapport 2024*. [Internett] Available at: <https://nkom.no/rapporter-og-dokumenter/internett-i-norge-arsrapport-2024> [Funnet September 2024].

Nocetti, J., 2015. Contest and conquest: Russia and global internet governance. *International Affairs*, 15 Januar, pp. 111-130.

Norges Bank, 2024 (1). *Norges Bank Memo - Kunderetta betalingsformidling 2023*, Oslo: Norges Bank.

NSM, 2022. *Typer av datasenter*. [Internett] Available at: <https://nsm.no/regelverk-og-hjelp/rapporter/temarapport-om-norske-datasentre-og-digital-autonomi/typer-av-datasenter/> [Funnet September 2024].

Nye, J. S., 2020. Power and Interdependence with China. *The Washington Quarterly*, 19 Mars, pp. 7-21.

Oracle, 2024. *Internet of things*. [Internett] Available at: <https://www.oracle.com/internet-of-things/> [Funnet 1 10 2024].

Oslo Economics, 2023. *En gjennomgang av sårbarheten i globale forsyningskjeder for matvarer*, Oslo: Oslo Economics.

Oslo Economics, 2023. *Omstillingsbarometeret*, Oslo: Oslo Economics.

Powers, S. M. & Jablonski, M., 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. s.l.:University of Illinois Press.

Regjeringen, 2021. *Hurdalsplattformen*, Oslo: Regjeringen.

Regjeringen, 2023. *Regjeringen setter vilkår knyttet til kjøp av eierandel i GlobalConnect*. [Internett] Available at: <https://www.regjeringen.no/no/aktuelt/regjeringen-setter-vilkar-knyttet-til-kjop-av-eierandel-i-globalconnect/id2970605/> [Funnet 17 oktober 2024].

Research and Markets, 2024. *Satellite Telecommunications Global Market Report 2024*. [Internett] Available at: <https://www.globenewswire.com/news-release/2024/02/07/2825377/0/en/Satellite-Telecommunications-Global-Market-Report-2024.html> [Funnet September 2024].

Reuters, 2022. *Meta halts construction of two data centres in Denmark*. [Internett] Available at: <https://www.reuters.com/technology/meta-halts-construction-two-data-centres-denmark-2022-12->

[Funnet September 2024].

Roberts, A., Choer Moraes, H. & Ferguson, V., 2019. Toward a Geoeconomic Order in International Trade and Investment. *Journal of International Economic Law*, pp. 655-676.

Samarbeidsportalen, 2024. *ID-porten*. [Internett]
Available at: <https://samarbeid.digdir.no/id-porten/id-porten/40>
[Funnet September 2024].

Satari, A., 2024a. *Global Open RAN market share by 2027 revised downward*. [Internett]
Available at: <https://www.telecoms.com/open-ran/global-open-ran-market-share-by-2027-revised-downward>
[Funnet September 2024].

Satari, A., 2024b. *Satellite disruption: how LEO and D2D are impacting telecoms*. [Internett]
Available at:
<https://www.telecoms.com/satellite/satellite-disruption-how-leo-and-d2d-are-impacting-telecoms>
[Funnet September 2024].

SNL, 2023. *Skytjeneste*. [Internett]
Available at: <https://snl.no/skytjeneste>
[Funnet September 2024].

SSB, 2017. *Norge i Europatoppen på digitale ferdigheter*. [Internett]
Available at: <https://www.ssb.no>
[Funnet August 2024].

SSB, 2023. *Bruk av IKT i husholdningene*. [Internett]
Available at: <https://www.ssb.no>
[Funnet August 2024].

SSB, 2023. *Fakta om internett og mobiltelefon*. [Internett]
Available at: <https://www.ssb.no>
[Funnet August 2024].

SSB, 2023. *IKT i næringslivet*. [Internett]
Available at: <https://www.ssb.no>
[Funnet August 2024].

SSB, 2024. *Digitalisering og IKT i offentlig sektor*. [Internett]
Available at: <https://www.ssb.no>
[Funnet August 2024].

STL Partners, 2020. *Telco edge computing: How to partner with hyperscalers*. [Internett]
Available at: <https://stlpartners.com/research/telco-edge-computing-how-to-partner-with-hyperscalers/>
[Funnet September 2024].

SØA, 2023. *Kunstig intelligens i Norge - nytte, muligheter og barrierer*, Oslo: NHO.

Teknologirådet, 2023. *Årsrapport til Teknologirådet for 2023*, s.l.: Teknologirådet.

Telenor Towers, 2024. *Telenor Towers - About*. [Internett]
Available at: www.telenortowers.com
[Funnet 17 oktober 2024].

Telenor, 2022. *Telenor etablerer fiberselskap i Norge*. [Internett]
Available at:
<https://www.telenor.com/media/nyheter/pressemeldinger/telenor-etablerer-fiberselskap-i-norge.page>
[Funnet 17 oktober 2024].

Telenor, 2023. *Internet of Things enkelt forklart*. [Internett]
Available at: <https://www.telenor.no/bedrift/iot/hva-er-iot/>
[Funnet 14 Mars 2023].

Telenor, 2024. *Telenor Årsrapport 2023*, Oslo: Telenor.

Telia Company, 2021. *Telia Company reaches agreement to sell part of its tower business in Norway and Finland to Brookfield and Alecta*. [Internett]
Available at:
<https://www.teliacompany.com/en/press-releases/telia-company-reaches-agreement-to-sell-part-of-its-tower-business-in-norway-finland-to-brookfield-alecta-2021-06-30-07-30-00>

T-Mobile, 2024. *T-Mobile Announces Technology Partnership with NVIDIA, Ericsson and Nokia to Advance the Future of Mobile Networking with AI at the Center*. [Internett]
Available at: <https://www.t-mobile.com/news/business/t-mobile-launches-ai-ran-innovation-center-with-nvidia>
[Funnet September 2024].

US Department of Justice, 2024. *The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector - Frequently Asked Questions*. [Internett]
Available at:
<https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector#1.%20checked%20on%201/10/2024>
[Funnet September 2024].

US Treasury, 2020. *Treasury Releases Final Regulations to Reform National Security Reviews for Certain Foreign Investments and Other*

Transactions in the United States. [Internett]
Available at: <https://home.treasury.gov/news/press-releases/sm872>
[Funnet September 2024].

US White House, 2019. *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. [Internett]
Available at:
<https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>
[Funnet September 2024].

US White House, 2021. *Building resilient supply chains, revitalizing american manufacturing, and fostering broad-based growth. 100-Day Reviews under Executive Order 14017*. [Internett]
Available at: <https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf>
[Funnet September 2024].

US White House, 2022. *Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States*. [Internett]
Available at: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/>
[Funnet September 2024].

US White House, 2024. *White House Office of Science and Technology Policy Releases Updated Critical and Emerging Technologies List*. [Internett]
Available at:
<https://www.whitehouse.gov/ostp/news-updates/2024/02/12/white-house-office-of-science-and-technology-policy-releases-updated-critical-and-emerging-technologies-list/>
[Funnet September 2024].

Wooden, A., 2023. *A guide to Open RAN*. [Internett]
Available at: <https://www.telecoms.com/open-ran/a-guide-to-open-ran>
[Funnet September 2024].

Zhou, Z. C. X., Liekang Zeng, E. L., Luo, K. & Zhang, J., 2019. Edge Intelligens: Paving the Last Mile of Artificial Intelligence With Edge Computing. *Proceedings of the IEEE*, August, pp. 1738-1762.

Zondag, M. H. W. & Tollersrud, T., 2019. *Vraker Huawei i 5G-utbyggingen: -Vi har hatt en dialog om sikkerhet*. [Internett]
Available at: <https://www.nrk.no/norge/vraker-huawei-i-5g-utbyggingen--vi-har-hatt-en-dialog-om-sikkerhet-1.14733807>
[Funnet September 2024].

Åmås, T., 2021. *Husholdningenes betalingsvaner*, s.l.: Norges Bank.

oslo**economics**

www.osloeconomics.no

E-post og telefon:
post@osloeconomics.no
+47 21 99 28 00

Besøksadresse:
Klingenberggata 7A
0161 Oslo

Postadresse:
Postboks 1562 Vika
0118 Oslo