EKSPERTUTVALGET FOR NASJONAL KONTROLL MED KRITISK DIGITAL KOMMUNIKASJONSINFRASTRUKTUR – EKOMSIKKERHETSUTVALGET

Nasjonal kontroll med kritisk digital kommunikasjons-infrastruktur – målbilde og virkemidler

2025

EKSPERTUTVALGET FOR NASJONAL KONTROLL MED
KRITISK DIGITAL KOMMUNIKASJONSINFRASTRUKTUR
– EKOMSIKKERHETSUTVALGET

Nasjonal kontroll med kritisk digital kommunikasjons-infrastruktur – målbilde og virkemidler

2025

Foto: Adobestock

Innhold

Foto: Anders Martinsen (Nkom)

I

Innledning

”

De aller fleste samfunnsfunksjoner av betydning for nasjonal sikkerhet eller for samfunnssikkerhet er avhengige av velfungerende digital kommunikasjon. De infrastrukturene som muliggjør slik digital kommunikasjon er spesielt kritiske, fordi konsekvensene dersom de ikke fungerer som forutsatt, er omfattende.

Foto: David Becker (Unsplash)

01

Sammendrag

De aller fleste samfunnsfunksjoner av betydning for nasjonal sikkerhet og samfunnssikkerhet er avhengige av velfungerende digital kommunikasjon. De infrastrukturene som muliggjør slik digital kommunikasjon er spesielt kritiske, fordi konsekvensene dersom de ikke fungerer som forutsatt, er omfattende. Det er derfor viktig at staten har nødvendig grad av nasjonal kontroll med hvordan kritisk digital kommunikasjonsinfrastruktur utvikles, driftes og vedlikeholdes. Denne kontrollen må brukes til å sikre og beskytte kritiske digitale kommunikasjonstjenester gjennom hele krisespennet fra fred til krise og krig.

Krisespennet har blitt langt mer relevant i spørsmål knyttet til nasjonal kontroll enn hva som var tilfelle for bare få år siden. Russland sin fullskalainvasjon av Ukraina har ført til at norske myndigheter med større alvor må tenke igjennom hva den øvre delen av krisespennet krever av tiltak. Internasjonale spenninger øker behovet for kontroll over kritisk teknologi og kritisk digital infrastruktur, noe som er tydeliggjort i Totalberedskapskommisjonens[1] rapport, og i den etterfølgende Totalberedskapsmeldingen[2]. Hos våre samarbeidspartnere EU og USA har det de siste årene blitt gjort mye for å styrke kontrollen og sikkerheten, særlig med utenlandske investeringer og viktige verdikjeder. Dette utvalgsarbeidet inngår derfor i en internasjonal trend for økt nasjonal kontroll med kritiske innsatsfaktorer.

Utvalget har sett på digital kommunikasjonsinfrastruktur som er viktig for statssikkerheten, har betydning for samfunnssikkerheten og som bærer tjenester

[1] NOU 2023: 17 *Nå er det alvor – Rustet for en usikker fremtid*

[2] Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen – Forberedt på kriser og krig*

som har høy betydning for kritiske samfunnsfunksjoner. Sikkerhetsloven gir hjemler som understøtter nasjonal kontroll innenfor deler av dette spennet, herunder eierskapskontroll, men utvalgets arbeid har omfattet et bredere spekter enn lovens nåværende rekkevidde. Utvalgets rapport må tolkes i lys av denne brede tilnærmingen.

I utvalgets kartlegging av dagens situasjon knyttet til eierskap av kritisk digital infrastruktur, er det ikke avdekket eierforhold som i seg selv fremstår som spesielt problematiske. Riktignok er utenlandsk eierskap svært utbredt, men eierskapet er i all hovedsak knyttet til land vi har et sikkerhetspolitisk samarbeid med. Videre er det stor transparens i eierforholdene i den forstand at eierskap kan spores direkte tilbake til norsk eierskap eller kjent utenlandsk offentlig eller privat eierskap. Likevel er det slik at eierskapstransaksjoner knyttet til kritisk digital infrastruktur påvirker statens kontroll med de samme infrastrukturene. Slike transaksjoner kan i noen sammenhenger gi en betydelig fordel ved at kapital blir gjort tilgjengelig for videreutvikling av den norske infrastrukturen. De er på den måten ønsket. Samtidig kan slike transaksjoner også utfordre statens mulighet til å ha nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur.

Eierskapstransaksjoner er imidlertid bare én type økonomisk aktivitet som kan utfordre nasjonal kontroll. Et annet eksempel kan være at tjenester som er avgjørende for å drifte eller vedlikeholde kritisk digital kommunikasjonsinfrastruktur, settes ut til utenlandske aktører. Et tredje eksempel kan være avhengighet av arbeidskraft som ikke har tilknytning til landet, slik at man risikerer at arbeidskraften ikke er tilgjengelig under en internasjonal krise.

Krise- og krigssituasjoner er generelt svært uforutsigbare i sin natur. Tilgang til innsatsfaktorer som deles selv mellom nære geografiske og allierte land kan bli vanskeliggjort dersom innsatsfaktorene kun er dimensjonert for fredstid. Utvalget mener derfor at staten bør ha oppmerksomhet både på å identifisere direkte sikkerhetstruende økonomiske aktiviteter, og på virkningen av økonomiske aktiviteter som ikke anses å være direkte sikkerhetstruende, men som utilsiktet kan få en kontrollsvekkende effekt i en internasjonal krisesituasjon.

En særlig kategori av utfordringer for nasjonal kontroll er knyttet til avhengighet til digitale infrastrukturer som på grunn av sin funksjon helt eller delvis befinner seg utenfor Norges grenser. Et eksempel er satellittbaserte systemer som blant annet benyttes til tidssynkronisering av kommunikasjonsnett. Mange slike internasjonale strukturer inngår som en integrert del av vår nasjonale kritiske digitale kommunikasjonsinfrastruktur. For slike strukturer må norske interesser ivaretas gjennom deltakelse og innflytelse i internasjonalt samarbeid. Nasjonal kontroll handler derfor langt på vei også om internasjonalt samarbeid.

I dialogen med aktørene har det kommet fram et ønske om økt nordisk samarbeid på sikkerhetsområdet. Utvalget mener at det er viktig å benytte de nordiske landenes samlede ressurser på best mulig måte. Samarbeid mellom myndighetene i de nordiske landene kan styrke situasjonen for ekomtilbydere knyttet til teknologisk utvikling, tilgang på personell og økende krav til robusthet i infrastrukturen.

Etter utvalgets syn gir det ikke mening å gi en statisk tilstandsbeskrivelse av hva som er nødvendig nasjonal kontroll med kritisk digital infrastruktur. Endringshastigheten i de digitale infrastrukturene i seg selv, hvordan de blir brukt og hva de blir brukt til, er for stor

til at en slik beskrivelse vil gi mening over tid. Likeledes vil endringer i selskapsstrukturer føre til at de mekanismene som gir nasjonal kontroll over hver enkelt infrastruktur også vil kunne endres over tid.

Utvalget har derfor konsentrert seg om å foreslå tiltak knyttet til hvordan staten bør innrette sitt kontinuerlige arbeid med å opparbeide og opprettholde nødvendig nasjonal kontroll med kritisk digital infrastruktur. Disse tiltakene er i noen grad generiske og ikke direkte knyttet til egenskaper ved kritisk digital infrastruktur. De kan derfor vurderes til å ha overføringsverdi også til andre sektorer.

Et nødvendig utgangspunkt for et slikt kontinuerlig arbeid er en presis definisjon av begrepet nasjonal kontroll. Utvalget har lagt følgende definisjon til grunn for sine forslag til tiltak:

Nasjonal kontroll innebærer at staten, knyttet til kritisk digital kommunikasjonsinfrastruktur, har
1. **styringsevne** til å ta effektive beslutninger gjennom for eksempel regulering, eierskap eller avtaler
2. **handlefrihet** til å gjennomføre beslutningene mest mulig uavhengig av utenlandske aktører og innsatsfaktorer.

Nedenfor gis en kort gjennomgang av de mest sentrale tiltakene som utvalget foreslår. Utvalget vil presisere at det å etablere nødvendig nasjonal kontroll, og å forvalte denne kontrollen, er et langsiktig arbeid som krever proaktiv handling. Når en krise-, konflikt- eller krigssituasjon oppstår, må den nødvendige nasjonale styringsevnen og handlefriheten allerede være etablert.

1.1 Et kontinuerlig arbeid for å etablere og vedlikeholde et målbilde av nasjonal kontroll med kritisk digital infrastruktur

Utvalget har identifisert at det ikke finnes noen enhetlig definisjon eller samlet organisert oversikt over hva som utgjør kritisk digital infrastruktur som er av betydning for nasjonal sikkerhet eller for samfunnssikkerhet. Dette kan forklares ved at det er et dynamisk bilde som stadig endrer seg. I relevante departementer og underliggende etater, foreligger det samlet sett mye informasjon om infrastruktur, kritikalitet, eierforhold og så videre. Likevel er det etter utvalgets syn vanskelig å arbeide systematisk med nasjonal kontroll over kritisk digital infrastruktur, uten at det foreligger en omforent forståelse av hva infrastrukturen består av og hvem som kontrollerer den. Utvalget foreslår derfor at Digitaliserings- og forvaltningsdepartementet (DFD) definerer og vedlikeholder en helhetlig oversikt over kritisk digital kommunikasjonsinfrastruktur og selskapene som eier denne. Dette arbeidet kan integreres som del av departementets arbeid med å identifisere og holde vedlikeholde oversikt over virksomheter i henhold til sikkerhetsloven § 2-1.

Det er også avgjørende at sektormyndighetene har tilgang til nødvendig informasjon om hvem som eier eller kontrollerer kritisk digital infrastruktur. Finansdepartementet (FIN) bør derfor utrede muligheten for større åpenhet i register over reelle rettighetshavere slik at departementer med sektoransvar etter sikkerhetsloven får tilgang til informasjon fra registeret.

Et kontinuerlig arbeid med nasjonal kontroll vil kreve at det finnes et målbilde over hva staten skal anse som nødvendig nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur. Dette målbildet må jevnlig vedlikeholdes og oppdateres i tråd med både teknisk og kommersiell utvikling på området. Utvalget mener at DFD bør etablere og vedlikeholde et målbilde for nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur. Målbildet bør omfatte nærmere definerte infrastrukturkategorier og funksjoner, og beskrive statens behov for styringsevne og handlefrihet i fred, krise og krig, innenfor disse kategoriene. Utvalget beskriver i kapittel 11 hvordan målbildet kan struktureres, og gir et eksempel på hvordan et målbilde kan formuleres i form av styringsevne og handlefrihet for en kategori av digital infrastruktur.

Et målbilde vil danne utgangspunkt for å vurdere nåsituasjonen, og et grunnlag for å vurdere om situasjonen er av en slik art at staten må kompensere med tiltak. Slike vurderinger må gjøres jevnlig i tråd med endringer i tekniske og organisasjonsmessige forhold. Utvalget mener derfor at DFD må sikre at det utvikles og løpende vedlikeholdes en analyse av nasjonal kontroll over alle kategorier av kritisk digital kommunikasjonsinfrastruktur. Dette innebærer å vurdere i hvilken grad statens tilgjengelige virkemidler gir den nødvendige styringsevne og handlefrihet som er definert i målbildet for den aktuelle kategorien av infrastrukturer. Slike analyser vil identifisere mulige gap mellom målbildet og realitetene. Utvalget mener at staten ved DFD må arbeide proaktivt med å identifisere gapene og risikoen med dem, planlegge og gjennomføre tiltak for å lukke gapene eller eventuelt akseptere risikoen.

Utvalget ser et tydelig samsvar mellom det proaktive arbeidet som må gjøres for å identifisere og redusere gap mellom målbildet og realitetene, og det arbeidet som må gjøres for å håndtere potensielt kontrollsvekkende endringer i sektoren. Når eksempelvis en eierandel i et selskap som kontrollerer kritisk infrastruktur vurderes solgt til utlandet, vil DFD måtte analysere hva situasjonen vil være etter et mulig salg, opp mot det etablerte målbildet for nasjonal kontroll. En slik analyse vil tydeliggjøre i hvilken grad salget kan svekke den ønskede styringsevnen eller handlefriheten. Om svekkelsen er vesentlig kan avbøtende tiltak identifiseres gjennom analysen, eller salget kan stanses i tilfeller der lovverket åpner for dette. Det kontinuerlige arbeidet med å vedlikeholde et bilde av vår nasjonale kontroll med kritisk digital kommunikasjonsinfrastruktur, vil således også sette myndighetene bedre i stand til å vurdere de mest egnede tiltakene i slike situasjoner.

1.2 Tiltak som setter myndighetene bedre i stand til å identifisere situasjoner som potensielt kan svekke nasjonal kontroll

Den omfattende dynamikken i sektoren for elektronisk kommunikasjon gjør at det ofte oppstår teknologiske eller markedsmessige endringer som kan påvirke den nasjonale kontrollen, og der myndighetene må vurdere hvorvidt det er nødvendig å gripe inn med tiltak. Dette kan være situasjoner der en eierandel i et selskap som kontrollerer kritisk digital kommunikasjonsinfrastruktur, skal selges til utenlandske aktører, eller der sentrale kontrakter for utvikling, drift og vedlikehold av kritisk digital infrastruktur skal inngås. I slike situasjoner er det avgjørende at informasjon om den forestående hendelsen når frem til de relevante myndigheter tidsnok. Dette krever et regelverk som sikrer rettidig informasjon til myndighetene. Kravene til eierskapskontroll i sikkerhetsloven er et

eksempel på dette. Utvalget mener i tillegg at DFD bør avklare om det sektorspesifikke regelverket er i stand til å også identifisere andre typer situasjoner der man står overfor kontrollsvekkende aktivitet i ekomsektoren.

En egenart ved ekomsektoren er at de anvendelsene som underbygger kritikaliteten til infrastrukturene ofte avhenger av innsatsfaktorer som ligger utenfor norsk jurisdiksjon. Utvalget observerer at selv om hver enkeltstående avhengighet isolert sett kan være uproblematisk, kan de samlet sett utgjøre et uønsket tap av nasjonal kontroll. For installasjoner og anvendelser som er avhengige av tilgang til infrastrukturer utenfor Norge, vil dette kunne være kritisk, særlig i den høye enden av krisespennet. Utvalget mener derfor at DFD bør vedlikeholde et faktagrunnlag knyttet til nasjonale avhengigheter av utenlandske innsatsfaktorer. Dette faktagrunnlaget bør danne basis for utvikling og vedlikehold av målbilde og virkemidler for nasjonal kontroll, herunder hvordan nasjonale beredskapstiltak og internasjonale beredskapsavtaler kan kompensere for kritiske avhengigheter til infrastruktur og innsatsfaktorer som ligger utenfor norsk jurisdiksjon.

1.3 Tiltak som bedrer nåsituasjonen knyttet til nasjonal kontroll

I eierskapsmeldingen fra 2022 angir Nærings- og fiskeridepartementet (NFD) seks ulike begrunnelser for statlig eierskap i selskaper, hvorav ett er «Samfunnssikkerhet og beredskap». Denne begrunnelsen benyttes for flere av statens eierskap i selskaper som eier kritisk digital kommunikasjonsinfrastruktur. Eierskap i selskaper fremstår språklig sett som et svært sterkt virkemiddel for nasjonal kontroll med slike strukturer. Utvalget har imidlertid en klar oppfatning om at staten ved NFD i forvaltningen av eierskapet bør være tydeligere på hvordan hensynet til samfunnssikkerhet og beredskap veies mot hensynet til avkastning, andre aksjonærer og for eksempel statsstøtteregler.

Det har over lengre tid pågått et arbeid for å vurdere og forberede opprettelsen av en nasjonal skytjeneste i Norge. I totalberedskapsmeldingen sier regjeringen at de vil planlegge en nasjonal skytjeneste for å sikre økt nasjonal kontroll med kritisk digital infrastruktur, viktige samfunnsfunksjoner og digitale verdier, og de har valgt et konsept for en slik tjeneste. Utvalget ser behov for etablering av nasjonal skyløsning ut fra behovet for nasjonal kontroll, og mener at dette arbeidet bør gis høy prioritet. Det anbefales at Justis- og beredskapsdepartement (JD) tydeliggjør videre ambisjonsnivå og plan, og stiller nødvendige ressurser tilgjengelig for arbeidet.

1.4 Tiltak som sikrer forutsigbarhet for aktørene

I dialogen med aktører fra bransjen har utvalget fra flere fått innspill om at statens arbeid med nasjonal kontroll må foregå på en måte som ikke fremstår som uforutsigbar for aktørene. En slik uforutsigbarhet kan i neste instans føre til at aktørene nøler med å initiere økonomisk sunne omstruktureringer, da det er vanskelig å forutse hvordan staten vil reagere. I den grad statens målbilde for nasjonal kontroll blir kommunisert til aktørene, vil et slikt målbilde i seg selv bidra betydelig til øket forutsigbarhet. Det er imidlertid også andre tiltak som vil kunne fremme forutsigbarhet, og som vi omtaler under.

Når en aktør vurderer erverv av eierandel i et norsk selskap, må man normalt legge til grunn at det er sunne bedriftsøkonomiske vurderinger som ligger bak. Et slikt oppkjøp kan føre til at kapital blir tilgjengelig for videreutvikling av norsk infrastruktur. Derfor bør myndighetenes arbeid for å sikre nasjonal kontroll med kritisk digital infrastruktur i så liten grad som mulig forstyrre aktørenes evne og vilje til slike investeringer.

Sikkerhetsloven § 10-3 gir staten mulighet til å fatte vedtak om stans i erverv av eierandeler i virksomheter dersom nasjonale sikkerhetsinteresser blir truet. Bestemmelsen er et viktig virkemiddel for å sikre nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur. Utvalget merker seg imidlertid at det er juridisk uenighet om hvorvidt bestemmelsen står seg mot de forpliktelsene Norge har i henhold til EØS-avtalen. JD bør derfor klarlegge om sikkerhetsloven § 10-3 kan være i strid med EØS-avtalens forpliktelser.

Dersom vi ønsker tilgang til utenlandsk kapital til norsk digital kommunikasjonsinfrastruktur, vil det være viktig at Norge fremstår som et forutsigbart og gjenkjennelig marked for potensielle investorer. Det arbeidet som skal gjøres i Norge for å sikre nasjonal kontroll over virksomheter som forvalter kritisk digital kommunikasjonsinfrastruktur bør derfor gjøres tett harmonisert med hva sammenlignbare land gjør på området. DFD og JD bør i den utstrekning det er mulig og relevant se til at Norge gjennomfører EØS-relevant regelverk knyttet til digital kommunikasjonsinfrastruktur. Nytt regelverk bør innføres i så nær tid som mulig med tilsvarende regulering i EU.

1.5 Rapportens oppbygging

Utvalget har skrevet en omfattende rapport som omhandler mange aspekter av problemstillingen nasjonal kontroll med digital kommunikasjonsinfrastruktur. Rapporten er delt opp i fire hoveddeler. Nedenfor i del I redegjøres det nærmere for utvalgets mandat og sammensetning. Del II inneholder beskrivende kapitler som utgjør bakgrunnsfakta for utvalgets diskusjoner og forslag til tiltak. Del III er dedikert til det virkemiddelapparatet staten rår over, og som er relevant for å forstå statens kontroll med kritisk digital infrastruktur. Del IV gir en nærmere beskrivelse av på hvilken måte staten bør arbeide systematisk og målrettet med nasjonal kontroll, kritikalitet til infrastruktur utenfor norsk jurisdiksjon, samt beskrivelse av økonomiske og administrative konsekvenser for de tiltakene utvalget foreslår. En samlet oversikt over utvalgets forslag til tiltak er inntatt i vedlegg 1.

Alle sektorer er i økende grad avhengig av digitale tjenester. Dette innebærer at den digitale infrastrukturen bærer stadig større verdier og mer kritiske tjenester for det norske samfunnet.

Foto: Glenn Carstens Peters (Unsplash)

02

Utvalgets mandat, sammensetning og arbeid

2.1 Utvalgets oppnevning og sammensetning

Utvalget ble oppnevnt av regjeringen i januar 2024 med oppdrag om å gi konkrete forslag til hvordan staten kan ivareta nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur.

Utvalget har bestått av ni medlemmer, sammensatt av et bredt utvalg av eksperter fra akademia og privat og offentlig sektor:

- Olav Lysne (leder). Direktør for Simula Metropolitan Center for Digital Engineering (SimulaMet) og professor ved OsloMet.
- Alexander Iversen. Sjefkonsulent for digital sikkerhet i DNV Cyber, DNV AS.
- Anna Grinaker. Direktør for finansiell infrastruktur i Norges Bank.
- Bente Hoff. Avdelingsdirektør i Nasjonal sikkerhetsmyndighet.
- Hanne Tangen Nilsen. Direktør for Sykehuspartner HF.
- Hilde Walmestad. Leder for kunde og nettdrift i nettselskapet Lede
- Kenneth Fjell. Professor ved Norges Handelshøyskole
- Toril Nag. Seniorpartner i HitecVision.
- Camilla Ongre. Seniorrådgiver i Nasjonal kommunikasjonsmyndighet.

Camilla Ongre erstattet Pål Wien Espen som medlem i utvalget etter at han gikk av som direktør for Nasjonal kommunikasjonsmyndighet i mars 2024.

Utvalgets sekretariat har bestått av følgende personer: Irene Åmot (sekretariatsleder og spesialrådgiver i Nasjonal kommunikasjonsmyndighet), Hans Jørgen Enger (underdirektør i Nasjonal kommunikasjonsmyndighet) og Andreas Løhren (seniorrådgiver i Digitaliserings- og forvaltningsdepartementet).

2.2 Utvalgets mandat

Mandat for ekspertutvalg

Nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur (ekomsikkerhetsutvalget)

1. Sammendrag
Norge er et av verdens mest digitaliserte land, og alle sektorer er i økende grad avhengig av digitale tjenester. Dette innebærer at den digitale infrastrukturen bærer stadig større verdier og mer kritiske tjenester for det norske samfunnet. Det er et klart budskap i Hurdalsplattformen at regjeringen skal vurdere i hvilke tilfeller staten bør ta eierskap til digital infrastruktur for å sikre disse verdiene. Den skjerpede sikkerhetspolitiske situasjonen i Europa aktualiserer dette ytterligere. Regjeringen setter derfor ned et ekspertutvalg for å vurdere hvordan staten kan ivareta nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur.

Utvalget skal på et overordnet nivå identifisere kritisk digital kommunikasjonsinfrastruktur. Utvalget skal også identifisere selskaper som eier eller råder over slik infrastruktur og deres bakenforliggende eierforhold. I tillegg skal selskaper som er av avgjørende betydning for utbygging, drift og vedlikehold av infrastrukturen, og deres eiere, identifiseres.

Ekspertutvalget skal videre vurdere i hvilken grad dagens regulering og øvrige virkemidler er tilstrekkelig til å ivareta nasjonal kontroll og forsvarlig sikkerhet. Utvalget skal identifisere eventuelle restbehov eller restrisiko, og foreslå løsninger for å redusere denne ytterligere, blant annet gjennom reguleringer, nasjonalt eierskap og andre virkemidler, og hvordan ulike virkemidler i så fall bør innrettes.

2. Mål med arbeidet
Arbeidet deles inn i tre delmål:
- Identifisere kritisk infrastruktur på et overordnet nivå
- Status for nasjonal kontroll og dagens virkemidler
- Vurdere tiltak for styrket nasjonal kontroll

2.1 Identifisere kritisk infrastruktur
Ekspertutvalget skal til eget formål og på overordnet nivå lage en oversikt over kritisk digital kommunikasjonsinfrastruktur, av regional eller nasjonal betydning som:
- Er viktig for statssikkerheten
- Er av betydning for samfunnssikkerheten
- Bærer tjenester av høy betydning for kritiske samfunnsfunksjoner

DFD vil dele vurderinger som er relevante for dette arbeidet.

I tillegg skal ekspertutvalget identifisere selskaper av betydning for denne infrastrukturen, blant annet selskaper som:
- Helt eller delvis eier eller råder over slik infrastruktur
- Har en viktig eller kritisk rolle for utbygging, drift og vedlikehold av infrastrukturen.

I tillegg skal leverandører, underleverandører og entreprenører som er avgjørende betydning for utbygging, drift og vedlikehold av infrastrukturen, herunder utstyr og software, identifiseres. Behovet for reservedels-, beredskapslagre og beredskapsutstyr skal inngå i vurderingene.

Oversikten skal inkludere en vurdering av følgende typer infrastruktur (både hardware og software):
- mobil- og bredbåndsnett
- transportnett
- undersjøiske fiberkabler
- datasentre
- satellittkommunikasjonssystemer
- særlig viktige anlegg som er viktig for hele krisespennet, blant annet fortifikatoriske anlegg/fjellanlegg

Utvalget skal legge til grunn samfunnets avhengighet til digitale tjenester i dag, og vurdere utviklingen av denne frem mot 2030, herunder etableringen av en sikker skyløsning for staten. Utvalget skal tydeliggjøre hvilke kriterier og definisjoner som er lagt til grunn for dette arbeidet

2.2 Status for nasjonal kontroll og dagens virkemidler

Utvalget skal beskrive hvilke virkemidler myndighetene har for å ivareta nasjonal kontroll over digital infrastruktur, og i hvilken grad dagens virkemidler ivaretar behovet. Regulering og nasjonalt eierskap skal inngå i denne vurderingen.

Dagens eierstrukturer skal beskrives for selskapene som eier eller råder over kritisk infrastruktur. Det er viktig at ulike sider ved utenlandsk eierskap belyses, blant annet de markedsmessige, økonomiske, juridiske og sikkerhetsmessige. Utvalget skal vurdere hvilken innvirkning de ulike formene for eierskap (nasjonalt, statlig, offentlig og privat) har for nasjonal kontroll.

Ekspertutvalget skal belyse ulike eierformer og transaksjoner, og vurdere hvordan disse kan utfordre nasjonal kontroll, blant annet:
- oppkjøp av andeler eller hele selskaper
- oppkjøp av mindre andeler av et selskap i flere omganger
- oppstykking og oppkjøp av verdiene i ulike selskaper
- hvilken innflytelse et selskap og dets eiere har over forvaltningen av selskapet ved ulike eierstrukturer,
- komplekse eierkjeder og endret eierskap; dersom det er flere selskaper i eierstrukturen, eierskifte bakover i eierstrukturen
- styringsstrukturer

Digitale kommunikasjonsnett bygger på internasjonale standarder og et sterkt globalt økosystem med rask teknologisk utvikling. Innovasjon i bransjen er viktig, og Norge ligger langt fremme med digitalisering og utbygging av slik infrastruktur, med høy grad av dekning og kapasitet i mobil- og bredbåndsnettene. Utvalget skal vurdere hvilken effekt virkemidlene for nasjonal kontroll kan ha for videre utvikling og innovasjon. Forslagene fra utvalget skal ta hensyn til behovet for videre utvikling og innovasjon, og skal i størst mulig grad legge til rette for dette. Utvalget skal også ta hensyn til sikkerhetssidene ved lange, komplekse og internasjonale digitale verdikjeder.

Utvalget skal beskrive hvordan reguleringsregimer eller andre hensyn til nasjonal kontroll er ivaretatt i nordiske land.

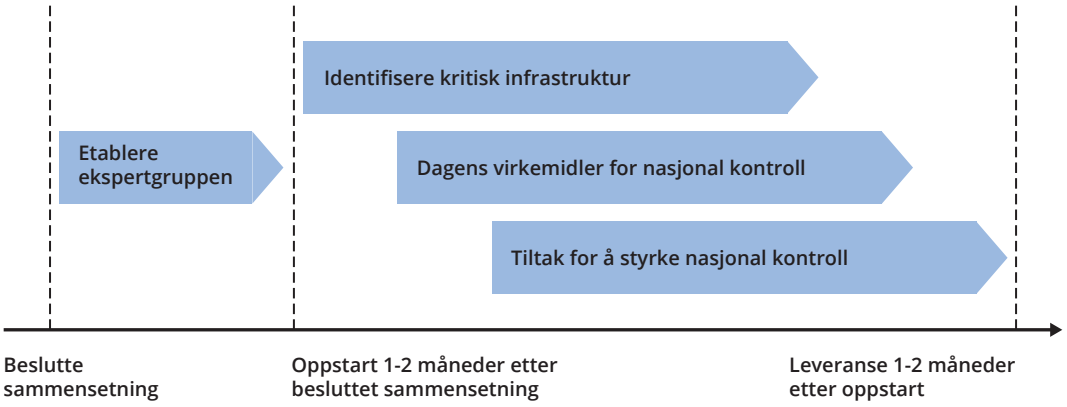
2.3 Vurdere tiltak for styrket nasjonal kontroll

Utvalget skal foreslå konkrete tiltak for videre arbeid med nasjonal kontroll over kritisk infrastruktur. Tiltakene som foreslås skal begrunnes og være konkrete. Konsekvensene av tiltakene, herunder kostnader, nyttevirkninger og konsekvenser for videre utvikling og innovasjon, skal belyses.

Utvalget oppfordres til å gjøre seg kjent med relevante deler av Investeringskontrollutvalgets rapport, som ble levert i desember 2023. Utvalget ble oppnevnt av NFD om eierskapskontroll i virksomheter som ikke er underlagt sikkerhetsloven. I tillegg oppfordres utvalget til å gjøre seg kjent med lov om endringer i sikkerhetsloven (eierskapskontroll og lovens virkeområde) av 20. juni 2023.

3. Tidsplan for arbeidet

Ekspertgruppen etableres 1-2 måneder etter besluttet sammensetning. Arbeidet er omfattende, og har en ambisiøs tidsplan på 12 måneder, med en muntlig rapportering i form av «forankringsmøter» med departementet etter 3, 5 og 9 måneder. Ekspertgruppen skal levere utkast til rapport etter 9 måneder og endelig rapport 12 måneder etter oppstart, som skissert i tidsplanen. Leveranse av endelig rapport blir 1. februar 2025[3]:



Eventuelle spørsmål kan avklares med departementet underveis i arbeidet.

4. Leveranse:

Arbeidet skal resultere i en rapport, der resultatene fra alle tre delmålene beskrives:
- Identifisere kritisk infrastruktur på et overordnet nivå
- Status for nasjonal kontroll og dagens virkemidler
- Vurdere tiltak for styrket nasjonal kontroll

Materiale som er gradert utarbeides i separat(e) vedlegg.

[3] Ny frist ble i dialog med departementet (DFD) satt til 28. februar 2025.

Utredningsinstruksen skal legges til grunn for arbeidet til ekspertutvalget: Utredningsinstruksen – regjeringen.no.

Det vises videre til Meld. St. 6 (2022–2023) eierskapsmeldingen: Meld. St. 6 (2022–2023) – regjeringen.no. Videre vises det til Meld. St. 9 (2022–2023) om nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet. Meld. St. 9 (2022–2023) – regjeringen.no

2.3 Utvalgets tolkning av mandatet

Utvalget har fått et meget omfattende mandat som i sin videste tolkning vil overskride rammene for et utvalgsarbeid. Det har derfor vært nødvendig å gjøre avgrensninger og prioriteringer for å kunne ferdigstille arbeidet innenfor de rammene som var til rådighet. I denne seksjonen beskrives de mest sentrale av disse avgrensningene og prioriteringene.

På overordnet nivå sier mandatet at utvalget skal vurdere hvordan staten kan ivareta nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur. Utvalget har på denne bakgrunn valgt å konsentrere seg om hva som gir staten nasjonal kontroll, og avgrense mot hva den nasjonale kontrollen skal benyttes til. Utvalget ser her på nasjonal kontroll som statens evne til å skaffe beslutningsgrunnlag, evne til å ta eller påvirke beslutninger, og handlefrihet til å sette beslutninger ut i live.

Eksempelvis tar utvalget ikke stilling til hvorvidt enkelte grupper av selskaper skal pålegges å opprette beredskapslager for en gitt type komponenter. Statens evne til å identifisere behovet for et slikt lager, påvirke en beslutning om at et beredskapslager skal opprettes, samt evne til å sørge for at en slik beslutning får effekt, tolkes imidlertid å ligge innenfor utvalgets mandat. I noen tilfeller er det krevende å trekke en klar grense mellom grep som gir nasjonal kontroll, og hva staten i en gitt situasjon kan ønske å benytte den nasjonale kontrollen til. Når det har oppstått tvilstilfeller har utvalget søkt å legge seg på en restriktiv linje. Tiltak som ikke i vesentlig grad påvirker statens kontroll har vi derfor latt ligge, selv om de isolert sett kan være gode i et sikkerhetsperspektiv.

Utvalget har også fått i oppgave å identifisere kritisk digital kommunikasjonsinfrastruktur og å identifisere selskaper som eier eller råder over slik infrastruktur. Vi har sett denne delen av oppgaven i lys av mandatets to andre hovedoppgaver, som er å redegjøre for status for nasjonal kontroll og vurdere tiltak for styrket nasjonal kontroll. Vi har ansett disse to siste oppgavene som viktigst i vårt mandat.

Heller enn å gi en fullt utarbeidet og begrunnet oversikt over hva som kan karakteriseres som kritisk infrastruktur, har utvalget konsentrert seg om å lage en oversikt som danner et hensiktsmessig grunnlag for vårt eget arbeid med tiltak for nasjonal kontroll. Vi har derfor på et overordnet nivå definert kategorier av infrastruktur som er viktig for statssikkerheten, av betydning for samfunnssikkerheten eller som bærer tjenester av høy betydning for kritiske samfunnsfunksjoner. Videre har vi identifisert virksomheter av betydning for disse klassene av infrastrukturer. Med utgangspunkt i disse virksomhetene har vi analysert dagens nasjonale kontroll med de kritiske delene av selskapenes virksomhet. Denne generiske analysen danner grunnlag for våre forslag til tiltak for styrket nasjonal kontroll.

En sentral begrunnelse for at utvalget ble opprettet, lå i et antall konkrete saker der salg av aksjeposter i enkeltselskaper ble vurdert. I disse sakene måtte norske myndigheter ta stilling til hvorvidt endringen i eierskapet ville utgjøre en risiko av betydning for samfunnssikkerheten og kritiske samfunnsfunksjoner. Disse sakene dreiet seg om eierskap, men den risikoen som oppstår gjennom sikkerhetstruende endringer i eierskap, er bare ett forhold som kan svekke nasjonal kontroll i kritisk digital kommunikasjonsinfrastruktur. Utvalget har derfor sett bredere på ulike forhold som kan svekke nasjonal kontroll, hvilken styringsevne og handlefrihet staten trenger for å opprettholde nasjonal kontroll og hvilke ulike virkemidler som kan brukes for å oppnå dette.

Utvalget har ikke gjort noen klare avgrensninger knyttet til krisespennet. De virkemidlene vi foreslår må i all hovedsak gjennomføres i fredstid, men effekten av dem vil være viktigst ved en eskalering oppover i krisespennet. Videre har vi ikke avgrenset oss mot noen deler av trusselbildet i den forstand at vi ser nasjonal kontroll som et virkemiddel for å bygge nasjonal sikkerhet i møte med alle relevante trusler. Likevel er det slik at de truslene som utfordrer nasjonal kontroll, står i en særstilling i vårt arbeid. Sikkerhetstruende økonomisk virksomhet som gir en grad av kontroll over selskaper som eier kritisk digital kommunikasjonsinfrastruktur, har derfor blitt viet spesiell oppmerksomhet.

En diskusjon om nasjonal kontroll med digital infrastruktur er ufullstendig uten en vurdering av det internasjonale bildet. Dette berøres i noen grad av mandatet ved at det omtaler internasjonalt samarbeid, et sterkt globalt økosystem og komplekse internasjonale verdikjeder. Det er et faktum at norske kritiske systemer og norsk kritisk infrastruktur er tett sammenvevd med internasjonale systemer som ikke er underlagt norsk jurisdiksjon. Nasjonal påvirkningsevne på disse systemene må skje gjennom internasjonalt samarbeid. Rapporten inneholder et eget kapittel som omhandler slike systemer.

2.4 Utredninger med grenseflater mot mandatet for dette utvalget

Utvalget har benyttet en rekke ulike kilder i sitt arbeid, både når det gjelder bakgrunnsinformasjon og vurderinger knyttet til nasjonal kontroll, eierskap og innflytelse i virksomheter og ulike trusler.

Som det fremgår av mandatet, ble utvalget oppfordret til å gjøre seg kjent med Investeringskontrollutvalgets rapport NOU 2023: 28 *Investeringskontroll – En åpen økonomi i usikre tider*. Flere av de vurderinger og beskrivelser av regelverk som fremkommer i NOU-en er relevant for dette utvalget

Andre relevante dokumenter har vært Meld. St. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – Så åpent som mulig, så sikkert som nødvendig*, Forsvarets forskningsinstitutt rapport 20/03149 *Utenlandske investeringer og andre økonomiske virkemidler – når truer de nasjonal sikkerhet?,* Totalberedskapskommisjonen NOU 2023: 17 *Nå er det alvor – rustet for en usikker fremtid* og Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen – Forberedt på kriser og krig*.

Når det gjelder Totalberedskapsmeldingen, ble denne meldingen ble lagt frem helt på tampen av utvalgets arbeid. Utvalget har derfor ikke hatt mulighet til å vurdere alt innholdet eller alle forslagene i meldingen.

2.5 Utvalgets møter og reiser

Utvalget startet arbeidet 2. februar 2024 og har avholdt 12 møter av en til to dagers varighet. Møtene har vært fysiske og avholdt i Oslo-området, men med mulighet for digital deltakelse. Det har i tillegg vært gjennomført digitale møter mellom enkelte utvalgsmedlemmer og utvalgsleder underveis i arbeidet.

Utvalget har i løpet av arbeidet hatt digitale møter med Telenor, Tampnet, Space Norway, Green Mountain, Helsenett og Nasjonal sikkerhetsmyndighet, Cyberforsvaret og Nkom.

2.6 Skriftlige innspill og utredninger bestilt av utvalget

Utvalget gjennomførte våren 2024 en informasjonsinnhenting for å få innsikt i hvordan ulike deler av ekomsektoren selv vurderer problemstillinger knyttet til eierskapstransaksjoner og da særlig knyttet til utenlandsk eierskap. Utvalget ba også om tilbakemeldinger om leverandører som ekomtilbyderne selv anser som viktige med tanke på utbygging, drift og vedlikehold av den kritiske digitale kommunikasjonsinfrastrukturen.

Spørreundersøkelsen er nærmere omtalt i vedlegg 5.

Utvalget har mottatt innspill fra Universitetet i Oslo som drifter et av samtrafikkpunktene for internettrafikk (NIX) i Norge, og Norsk Datasenterindustri. Innspillene omhandler temaer som omtales i denne rapporten, for eksempel utviklingen av datasentre i Norge, behov for infrastruktur knyttet til nøyaktig tid og synkronisering av frekvensbånd i mobilnett, forhold for å sikre basis internettjenester i Norge dersom deler av nettet er nede eller isolert, samt beredskap rundt fysisk infrastruktur.

Utvalget har underveis innhentet tre utredninger som benyttes aktivt i denne rapporten:

1. En fremtidsanalyse for utviklingstrekk og trender for kritisk digital infrastruktur frem mot 2030, gjennomført som et samarbeid mellom Oslo Economics og Norsk utenrikspolitisk institutt (NUPI).

Denne rapporten analyserer hvordan teknologiske- og markedsmessige trender og geopolitisk utvikling kan påvirke nasjonal kritisk infrastruktur i årene fremover, også i lys av samfunnets avhengigheter til digitale tjenester. Rapporten er behandlet i kapittel 7.

2. En eierskapsanalyse for å avdekke reelle (utenlandske) eiere til selskaper som eier kritisk digital kommunikasjonsinfrastruktur eller underleverandører til disse, gjennomført av Menon Economics.

I rapporten har det særlig vært fokus på å bringe på det rene utenlandsk eierskap gjennom flere ledd i eierskapskjeden, i tillegg til at det også for eksempel gjøres vurderinger av risiko knyttet til utenlandsk eierskap. Rapporten er behandlet i kapittel 6.

3. En juridisk vurdering av rettslige rammer for kontroll med kritisk digital infrastruktur, foretatt av professor Christoffer Conrad Eriksen ved Institutt for offentlig rett, Det juridiske fakultet, Universitetet i Oslo.

Utredningen tar for seg hvilke forutsetninger som må til for at norske myndigheter kan pålegge og håndheve vilkår som fastsettes overfor utenlandske selskaper som blir eier av eller får kontroll over kritisk digital kommunikasjonsinfrastruktur i Norge. Vurderinger fra rapporten er benyttet i kapittel 9 og 13.

I denne rapporten vil vi heretter referere til de tre utredningene som følger: OE/NUPI (2024), Menon (2024) og Eriksen (2024).

De tre utredningene er inntatt som vedlegg 2-4 i denne rapporten.

Foto: Pascal Debrunner (Unsplash)

II

Om kritisk digital kommunikasjonsinfrastruktur og nasjonal kontroll

”

I denne delen av rapporten gir vi en innføring i ekomsektoren for å vise på et helt overordnet nivå hvordan sektoren ser ut i dag, og hvordan den økende digitaliseringen av samfunnet vårt og ikke minst konkurranse om å levere ekomtjenester, har bidratt til å utvikle sektoren.

Foto: Globestock

03

Om ekomsektoren

3.1 Innledning

Den norske ekomsektoren leverer elektroniske kommunikasjonsnett og -tjenester til hele landet. Sammen med datasentre danner disse nettene og tjenestene det som gjerne omtales som *den digitale grunnmuren*.[4] Denne «grunnmuren» består av en rekke ulike tilbyderes infrastruktur, og de som leverer tjenestene sine via nettene, kan selv være eiere av nettene eller aktører som tilbyr tjenester basert på kjøp av tilgang til nett og tjenester fra andre.

I denne delen av rapporten gir vi en innføring i ekomsektoren for å vise på et helt overordnet nivå hvordan sektoren ser ut i dag, og hvordan den økende digitaliseringen av samfunnet vårt og ikke minst konkurranse om å levere ekomtjenester, har bidratt til å utvikle sektoren.

Utvalget har på ingen måte tatt mål av seg å gi en komplett beskrivelse av sektoren, da dette ikke er en del av mandatet, men heller sette sektoren inn i en ramme før vi ser nærmere på de ulike aktørene som i dag eier eller kontrollerer kritisk digital kommunikasjonsinfrastruktur.

[4] Se for eksempel Meld. St. 28 (2020–2021) *Vår felles digitale grunnmur, og Fremtidens digitale Norge*, *Nasjonal digitaliseringsstrategi* 2024-2030 utgitt av Digitaliserings- og forvaltningsdepartementet.

3.2 Noen korte fakta om ekomsektoren

Nasjonal kommunikasjonsmyndighet (Nkom) samler inn og offentliggjør årlig informasjon om utviklingen i ekomsektoren. I etterkant av liberaliseringen av det gamle telemonopolet siste halvdel av 1990-tallet, har den norske ekomsektoren utviklet seg med etablering av en rekke tjenestetilbud og tilbydere som konkurrerer om å tilby sine tjenester til offentlige og private kunder. Tidligere krav om konsesjon ble med ekomloven fra 2003 erstattet av en generell tillatelse gjennom det rettslige rammeverket, samt en registreringsplikt hos Nkom. Individuelle tillatelser ble begrenset til å omfatte frekvenstillatelser og nummer innenfor nasjonal nummerplan.

Ser vi på nøkkeltall for sektoren, viser disse at ekomsektoren i 2023 samlet omsatte for i underkant av 39 milliarder kroner. Tallene er hentet inn fra 150 større og mindre tilbydere og tar utgangspunkt i tilbydernes fakturering av egne kunder, men inkluderer for eksempel ikke TV-abonnement eller utleie eller salg av utstyr som for eksempel mobiltelefoner.

Den norske ekomsektoren har gjort betydelige investeringer for å bygge ut infrastruktur i hele landet. Investeringsandelen målt mot omsetning har i en årrekke ligget på over 1/3. Det er særlig investeringer i mobilnett (4G og 5G), samt fiberbredbånd som har bidratt til de høye investeringstallene i de senere årene. Det ble foretatt investeringer i varige driftsmidler for elektroniske kommunikasjonsnett og -tjenester på mer enn 12,6 milliarder kroner i 2023, og samlet rundt 63,6 milliarder kroner for årene 2019-2023.

I tillegg kommer investeringer i datasentre. Dette er tall Nkom foreløpig ikke har tilgang til, men i en rapport estimerer Norsk Datasenterindustri investeringer på 20-30 milliarder kroner per år i årene fremover.

Romindustrien er heller ikke inkludert i disse tallene. På dette området er særlig introduksjonen av lavbane-satellitter (LEO – Low Earth Orbit) interessant fordi de vil kunne gi konnektivitet i områder som ikke er dekket av eksisterende fastnett eller mobilnett.

Knyttet til vurderingen av kritisk digital kommunikasjonsinfrastruktur, er det viktig å påpeke at det ikke nødvendigvis er et én-til-én-forhold mellom de som eier eller kontrollerer infrastruktur og de som tilbyr tjenester som leveres over infrastrukturen. Ekomsektoren består av en rekke tilbydere som baserer sitt tilbud på grossisttilgang hos ulike infrastruktureiere og på den måten konkurrerer om offentlige og private kontrakter. Dette innebærer at en samfunnskritisk tjeneste kan leveres over infrastrukturen til en infrastruktureier uten at denne nødvendigvis er kjent med kritikaliteten til virksomheter som benytter tjenestene som leveres over infrastrukturen.

3.3 Markedsmessig utvikling – konsolidering og konvergens mellom nett og tjenester

Det norske ekommarkedet består i dag av en rekke ulike selskaper som tilbyr tilgang til digitale kommunikasjonsnett og -tjenester, og dette landskapet er stadig i endring etter hvert som selskaper kjøpes opp eller avvikles, eller nye selskaper etableres. Forretningsmodellene bak de enkelte selskapene kan variere, avhengig av om eier for

eksempel har en finansiell tilnærming til drift med ønske om fremtidig oppkjøp i tankene eller er en mer industriell og langsiktig eier.

Telenor har en solid markedsposisjon i det norske markedet, med utgangspunkt i selskapets landsdekkende mobil- og bredbåndsinfrastruktur. Denne posisjonen har i de senere årene blitt utfordret av både Telia og ice (nå Lyse Tele). Gjennom oppkjøp av andre selskap har Telia og Lyse Tele kontroll over infrastruktur som innebærer at de har både fastnett og mobilnett i Norge (dekningen er dog ikke nødvendigvis helt lik). Denne utviklingen bidrar for eksempel til at alle de tre selskapene kan tilby komplette løsninger i både bedriftsmarkedet og privatmarkedet, og er i ferd med å oppfylle den politiske målsettingen om å ha tre fullverdige mobilnett i Norge.

I markedet for fast bredbånd er Altibox-partnerne og GlobalConnect viktige aktører med utstrakt bredbåndsinfrastruktur som danner grunnlag for solide markedsposisjoner i privat- og bedriftsmarkedene.

Telenor er fortsatt den klart største aktøren i det norske markedet målt i total omsetning. Selskapets andel av samlet omsetning var på 43,8 prosent første halvår 2024, med Telia på andreplass med 23,5 prosent av samlet omsetning.

På tjeneste- og infrastruktursiden ser vi at det har vært en utvikling ved at flere tjenester som tidligere ble levert i ulike nett og med ulik teknologi, nå smelter sammen og leveres via internett-teknologi (pakke-svitsjede nett). Dette gir mulighet for sømløs overgang mellom ulike typer nett (fast/trådløst) for tjenester mange benytter seg av i det daglige. For arbeidslivets del er det for eksempel kan det være en fordel å kunne flytte samtaler på Teams mellom ulike enheter (PC til mobil) dersom man er nødt til å ta deler av et møte på farten.

3.4 Nye aktører med egen infrastruktur – en internasjonal sektor i stadig endring

Ekomsektoren er i sin natur internasjonal. Dette vises godt ved at flere aktører har etablert tjenestetilbud med egen infrastruktur i flere ulike land, men ikke minst fordi *innholdet* vi konsumerer og tjenestene vi benytter oss av, leveres av store internasjonale selskaper som Alphabet (Google), Amazon, Microsoft, Meta (Facebook) og ByteDance (TikTok) med opphav utenfor Europas grenser.

I Norden er Telenor, Telia og GlobalConnect eksempler på aktører som minst har et skandinavisk fotavtrykk for sine nettverk. I Europa for øvrig finnes flere eksempler på multinasjonale selskaper som drifter nett og tjenester i flere av medlemsstatene i EU og med forgreninger til andre deler av verden. Mens Telenor i en årrekke har hatt virksomhet i Asia, er for eksempel Deutsche Telekom blant de største mobilnettaktørene i USA, i tillegg til at selskapet har aktivitet i Canada.

Fremveksten av store internasjonale innholdsleverandører endrer måten bransjen og kundene tilnærmer seg tjenester og informasjon som leveres over ekomnettene, på. I Nkoms rapport «Internett i Norge – Årsrapport 2024» fremgår det for eksempel at man på et aggregert nivå har en årlig vekst i internettrafikken på om lag 20-30 prosent. Strømmetjenester er den største trafikkdriveren og står for omtrent 70 prosent av

trafikken i nettene. I et 10-15 års perspektiv går det derfor an å trekke frem spesielt to viktige trender – fremveksten av sjøkabler og etablering av en ny datasenternæring i Norge. Disse to trendene henger tett sammen. Kombinasjonen sjøkabler og lokale datasentre gir brukerne rask tilgang til data med lav responstid.

De siste 10 årene er det etablert eller under planlegging flere store sjøfiberkabler som knytter Norge til Europa og verden for øvrig. Denne type internasjonal konnektivitet bidrar til både redundante og diversifiserte internettforbindelser for datatrafikken innad samt til/fra Norge, men kan også sees i sammenheng med det politiske siktemålet om å gjøre Norge til et attraktivt land å investere og bygge datasenter i.[5] Altibox Carrier, Bulk og Tampnet er eksempler på aktører som har etablert internasjonale sjøfiberforbindelser til/fra Norge.

Flere regjeringer har vært pådrivere for å legge til rette for etablering av datasentre i Norge. Regjeringen Gahr Støre ved digitaliserings- og forvaltningsminister Karianne Oldernes Tung har varslet at det skal legges frem en ny datasenterstrategi våren 2025. Datasenternæringen er i fremvekst, og flere eksisterende datasenteraktører som for eksempel Bulk, Lefdal Mine Datacenter, Green Mountain og Stack er omtalt i denne rapporten.

I tillegg er det naturlig å se på en tredje trend innen teknologiutvikling, nemlig utviklingen innen satellittkommunikasjonstjenester. Fremveksten av lavbane-satellitter er med på å kunne gi gode bredbåndstjenester i områder som hittil ikke har vært dekket av annen teknologi. Satellittkommunikasjonsløsninger basert på geo-stasjonære satellitter som er posisjonert mye lengre ut i verdensrommet har sine klare begrensninger knyttet til ned- og opplastingshastighet, i tillegg til lang responstid, men dette bildet endres nå.[6] Både amerikanske Starlink og Project Kuiper (Amazon) er aktive her, men også europeiske Eutelsat OneWeb er eksempel på europeisk selskap. I tillegg kommer EUs IRIS-program[7] der man har avsatt 2,4 milliarder euro i perioden 2023-2027 for å skape et sikkert satellittbasert kommunikasjonsalternativ for i medlemslandene, men som også tar sikte på å kunne tilby kommersielle kommunikasjonstjenester.

[5] Regjeringen lanserte sin første datasenterstrategi i 2018, se https://www.regjeringen.no/globalassets/departementene/nfd/dokumenter/strategier/strategi-nfd-nett-uu.pdf En oppdatert datasenterstrategi ble gitt ut i august 2021, se https://www.regjeringen.no/contentassets/0eabdbcbfb2540699466a4a1a801d737/nn-no/pdfs/norske-datasenter.pdf

[6] Starlink sendte i første halvdel av oktober 2024 søknad til amerikanske myndigheter om å få gjøre endringer i oppsettet for deler av satellittene sine slik at de skal kunne levere Gigabit-hastigheter – se https://www.digi.no/artikler/starlink-vil-levere-1-gbit-s-fra-satellittene/551895

[7] Infrastructure for Resilience, Interconnection and Security by Satellite (IRIS)

Utvalget definerer i dette kapittelet «nasjonal kontroll» og ser nærmere på hvordan nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur vil være et viktig virkemiddel for å ivareta nasjonale sikkerhetsinteresser.

Foto: Anders Martinsen (Nkom)

04

Nasjonal kontroll med digital infrastruktur

4.1 Hva er nasjonal kontroll

4.1.1 Innledning

Problemstillinger rundt nasjonal kontroll ble for alvor satt på spissen i forbindelse med Russlands fullskala angrepskrig mot Ukraina. Kort tid etter invasjonen i 2022 ble Elon Musk-eide SpaceX sin satellittjeneste Starlink tilgjengeliggjort for Ukraina. Også en rekke satellitterminaler ble anskaffet og donert, slik at ukrainske myndigheter kunne opprettholde kommunikasjon når deres egen telekom- og kraftinfrastruktur ble angrepet. Det er rapportert at Ukraina hadde stor nytte av dette. I ettertid var Musk imidlertid involvert i flere kontroverser, blant annet ved å nekte Ukraina tilgang til Starlink for offensive militæroperasjoner.[8] I dette tilfellet manglet Ukraina egnede kommunikasjonstjenester under egen nasjonal kontroll og var prisgitt én enkelt aktør utenfor egen jurisdiksjon, og som kunne sette egne betingelser for tilgang på tjenesten.

Et motsatt eksempel var hvordan Ukraina håndterte sine offentlige data i forbindelse med invasjonen. Tidligere ble disse lagret på lokale servere i Ukraina, under nasjonal kontroll. Imidlertid ble disse datasentrene vurdert som mulige mål for militære angrep. Rett før invasjonen ble det åpnet for at kritiske offentlige data kunne migreres over på offentlige skytjenester, blant annet på Microsofts skyplattform[9], slik at dataene kunne

[8] Aftenposten 2023, https://www.aftenposten.no/verden/i/zE3RRq/starlink-systemet-gir-elon-musk-stor-makt-det-skaper-bekymring

[9] Microsoft blog 2022, https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

flyttes ut av Ukraina og spres på datasentre i Europa. I dette tilfellet var det fordelaktig å «redusere» den nasjonale kontrollen med dataene for å beskytte dem.

Konseptet med å kunne evakuere kritisk data ut av landet i forbindelse med krise og krig er ikke nytt. I 2017 signerte statsministrene i Estland og Luxembourg avtale om å etablere en estisk «data-ambassade» i Luxembourg, i form av datasentre, med tilsvarende juridisk beskyttelse som en fysisk ambassade.[10] Her lagrer Estland backup av viktige offentlige data, som eiendomsregistre, folkeregister osv.[11]

Innenfor elektronisk kommunikasjon vil ulike sikkerhetstiltak måtte tilpasses behovet for kommunikasjonens tilgjengelighet, integritet og konfidensialitet. For eksempel vil det i en ekstremværsituasjon være viktigere å sikre at mobilkommunikasjon er tilgjengelig for redningspersonell og innbyggere, enn at den er avlyttingssikker. Ved utveksling av informasjon som kan skade nasjonale sikkerhetsinteresser om den kommer på avveie, så vil det å sikre kommunikasjonens konfidensialitet som oftest være det viktigste behovet.

Ofte kan hensynene til elektronisk kommunikasjons tilgjengelighet, integritet og konfidensialitet komme i konflikt med hverandre. I tillegg må sikkerhet hele tiden avveies mot andre viktige samfunnshensyn. Digital infrastruktur er i hovedsak eid og driftet av private aktører i et fritt konkurransemarked, og en del av en teknologisk kompleks sektor som krever tunge investeringer. I et lite land som Norge er derfor utenlandske investeringer og partnerskap, samt tilgang til utenlandsk teknologi og kompetanse, avgjørende for å sikre konkurransekraft, innovasjon og utvikling.

Å legge til rette for konkurranse, innovasjon og teknologisk utvikling står ikke i motstrid med behovet for sikkerhet, heller tvert imot. For eksempel har norske myndigheter besluttet at dagens Nødnett, som er en separat og fullt ut statlig eid sambandsinfrastruktur for nød- og beredskapsetater, skal fases ut, og erstattes med nytt konsept for nød- og beredskapstjenester som kombinerer statlig eierskap med kjøp fra kommersielle mobiloperatører[12]:

> «Kombinasjonen utnytter styrkene fra offentlig og privat sektor. Staten vil benytte ulike virkemidler, som eierskap, sikkerhetsloven, regulering, tilsyn og avtaler for å oppnå tilstrekkelig grad av nasjonal kontroll og forsvarlig sikkerhet i nytt nødnett.»

Den sentrale utfordringen er derfor å vurdere behovet for sikkerhet og nasjonal kontroll sammen med hensynet til konkurranse, innovasjon og utvikling. Som for sikkerhetstiltak for øvrig, er nasjonal kontroll et virkemiddel som kan ha stor betydning for sikkerheten i noen tilfeller, men begrenset eller ingen effekt i andre tilfeller. I noen tilfeller kan det sågar være hensiktsmessig at infrastruktur eller tjenester er plassert utenfor Norge, for å ivareta nasjonale sikkerhetsinteresser.

[10] Journal officiel du Grand-Duche de Luxembourg 2017, https://legilux.public.lu/eli/etat/leg/loi/2017/12/01/a1029/jo

[11] e-estonia 2019, https://e-estonia.com/data-embassy-the-digital-continuity-of-a-state/

[12] Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen*

4.1.2 Ulike definisjoner og beskrivelser

Nasjonal kontroll er ett av flere virkemidler for å oppnå nasjonal sikkerhet. Meld. St. 9 (2022–2023) omtaler nasjonal kontroll sammen med en rekke andre virkemidler for å bygge digital motstandskraft. Andre virkemidler omfatter eksportkontroll, sikker teknisk design, hendelseshåndtering, spesialistkompetanse, veiledningsressurser mv. Dette kapitlet ser nærmere på begrepet nasjonal kontroll.

Nasjonal kontroll er ikke entydig definert. Siden ekomsikkerhetsutvalget har blitt nedsatt som et av tiltakene i Meld. St. 9 (2022–2023), er det naturlig å ta utgangspunkt i beskrivelsen av begrepet nasjonal kontroll i denne stortingsmeldingen. Her er begrepet knyttet til *evnen til å ivareta nasjonale sikkerhetsinteresser.* Nasjonale sikkerhetsinteresser er i sikkerhetsloven § 1-5 nr. 1 er definert som følger:

Boks 4.1

Definisjon av nasjonale sikkerhetsinteresser i sikkerhetsloven § 1-5 nr. 1.

1. nasjonale sikkerhetsinteresser: landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til
   a. de øverste statsorganers virksomhet, sikkerhet og handlefrihet
   b. forsvar, sikkerhet og beredskap
   c. forholdet til andre stater og internasjonale organisasjoner
   d. økonomisk stabilitet og handlefrihet

Det følger av Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet* at nasjonale sikkerhetsinteresser omfatter primært *statssikkerhet,* men også de deler av *samfunnssikkerheten* som har vesentlig betydning for Norges evne til å ivareta sikkerhetsinteressene. Loven fanger derfor i større grad enn tidligere lov opp samfunnssikkerhetsperspektivet i tillegg til statssikkerheten. Det uttales i den nevnte proposisjonen at det i dagens samfunn har blitt vanskeligere å trekke en klar linje mellom statssikkerhet og samfunnssikkerhet, gitt både det komplekse trusselbildet, og de komplekse og gjensidige avhengighetene på tvers av samfunnssektorer, privat og offentlig virksomhet, og sivil og militær virksomhet. På samme bakgrunn vurderer utvalget at også sektorreguleringen i ekomsektoren delvis griper inn i forhold som omhandler nasjonale sikkerhetsinteresser, ved at flere av kravene i ekomloven og forskriften er knyttet til å ivareta «nasjonal sikkerhet».

Ifølge mandatet skal utvalget se på digital kommunikasjonsinfrastruktur som er viktig både for statssikkerheten, har betydning for samfunnssikkerheten og som bærer tjenester som har betydning for kritiske samfunnsfunksjoner. Derfor vil utvalget i rapporten bruke begrepet *nasjonale sikkerhetsinteresser* i en bredere forstand, slik at det ikke bare er strengt avgrenset til definisjonen i sikkerhetsloven, men også kan omfatte nasjonal sikkerhet slik det omtalt i ekomloven. I utvalgets mandat er nasjonal kontroll tett knyttet til eierskap. Mandatet viser til Hurdalsplattformens budskap om at regjeringen skal vurdere i hvilke tilfeller staten bør ta eierskap til digital infrastruktur for å sikre verdiene som bæres over infrastrukturen. Her er kartlegging av dagens eierstrukturer til

gjeldende digital infrastruktur et sentralt moment. Videre skal utvalget vurdere hvordan nasjonal kontroll påvirkes av ulike eierformer og eierskapstransaksjoner.

Men utvalget skal ikke se utelukkende på eierskap som virkemiddel for nasjonal kontroll med digital infrastruktur. Det spesifiseres i mandatet at også andre virkemidler skal vurderes, som for eksempel regulering i lov og forskrift og nasjonalt eierskap (kommune, fylkeskommune og privat norsk eierskap). Stortingsmeldingen peker på ytterligere virkemidler, som offentlig-privat/sivil-militært og internasjonalt samarbeid, råd og veiledning, og det å ha tilstrekkelig oversikt over verdiene.

I «Konseptvalgutredning for nasjonal skytjeneste» (NSM, 2023), fremgår det at begrepet nasjonal kontroll brukes for å «*beskrive en tilstand der staten kan ivareta sin handlefrihet og styringsevne gjennom hele krisespekteret*», og at *«fravær av nasjonal kontroll kan kjennetegnes ved at staten står i et avhengighetsforhold til eksterne aktører utenfor norsk jurisdiksjon».*

Videre beskriver NSMs temarapport «Nasjonal kontroll av IKT-tjenester» (2023) at begrepet, i konteksten av IKT-tjenester, i praksis kan innebære at

> «[…] utvalgte norske data og tjenester er underlagt reell norsk teknisk og juridisk kontroll, og at man med høy sannsynlighet kan utelukke at utenlandske selskaper og andre land har teknisk tilgang til norske data og tjenester. Dette innebærer at det ikke skal være teknisk mulig for noen utenfor Norge (inkludert utenlandske leverandører og andre lands myndigheter) å lese, manipulere eller sabotere norske data og tjenester. […] Data og tjenester skal fungere godt i hele krisespekteret […].»

4.1.3 Tilstøtende begreper – autonomi og suverenitet

Det finnes også tilstøtende begreper til nasjonal kontroll som har dels overlappende betydning. Et slikt begrep er *nasjonal autonomi*. Autonomi betyr *selvstyre*, og brukes i mange ulike sammenhenger, fra et lands selvråderett, til tekniske systemer som tar beslutninger uten menneskelig intervensjon, og til et menneskes individualitet og evne til å ta egne beslutninger.

I kontekst av elektronisk kommunikasjon, er nasjonal autonomi omtalt i en egen bestemmelse, § 2-9, i forskrift om elektronisk kommunikasjon og elektroniske kommunikasjonstjenester (ekomforskriften):

> «Nasjonal kommunikasjonsmyndighet kan i krise- og beredskapssituasjon pålegge tilbyder å utføre drift og vedlikehold av tjenestetilbudet med personell og tekniske løsninger som er lokalisert på norsk territorium.»

Et annet tilstøtende begrep er *digital suverenitet.* Begrepet har blant annet blitt brukt i forbindelse med EUs felleseuropeiske visjon for digital omstilling «Det digitale tiåret 2030», hvor målet blant annet er å styrke europeisk konkurransekraft og Europas digitale suverenitet og digitale sikkerhet og slik gjøre seg mindre avhengig av USA og Asia.

For å bidra til å nå disse målene har EU blant annet etablert et investeringsprogram DIGITAL[13] [14], som har seks satsingsområder: 1) tungregning og superdatamaskiner, 2) skyteknologi, data og kunstig intelligens, 3) digital sikkerhet, 4) avansert digital kompetanse, 5) anvendelse av digitale teknologier, og 6) halvledere (mikrobrikker). Norge deltar i dette programmet.

I sammenheng med den store utbredelsen av skytjenester brukes suverenitets-begrepet også i formen «sovereign cloud». Med dette menes i de fleste sammenhenger en skytjeneste-infrastruktur som sikrer at data lagres og skytjenester prosesseres innenfor et lands grenser og jurisdiksjon.

4.1.4 Utvalgets definisjon av nasjonal kontroll med digital infrastruktur

Som angitt i mandatet skal eierskap være sentralt i utvalgets vurderinger av nasjonal kontroll. Samtidig er det helt avgjørende at eierskap som virkemiddel sees i sammenheng med øvrige virkemidler for å ivareta nasjonal kontroll, slik som regulering, avtaler, internasjonalt samarbeid osv.

På den ene side har utvalget dermed et *bredere* perspektiv enn for eksempel investeringskontrollutvalget, som ser utelukkende på screening av utenlandske investeringer. På en annen side har utvalget et *spissere* fokus, hva gjelder den sektorspesifikke avgrensningen til digital kommunikasjonsinfrastruktur.

Begrepene nasjonal kontroll, nasjonal autonomi og digital suverenitet tar opp i seg de samme momentene, er dels overlappende og ser også ut til å brukes om hverandre i ulike sammenhenger.

Digital suverenitet er et generisk begrep som kan brukes til å omtale alt fra en enkelt virksomhets kontroll med sin egen digitale infrastruktur og egne data, til EUs digitale suverenitet overfor andre stormakter.

Nasjonal autonomi i kontekst av digital kommunikasjonsinfrastruktur virker å være nærmere knyttet til en teknisk implementasjon, jf. § 2-9 om nasjonal autonomi i ekomforskriften. Det vil si, at drift og vedlikehold av infrastruktur/tjenester skal gjennomføres med personell og tekniske løsninger som er lokalisert på norsk territorium.

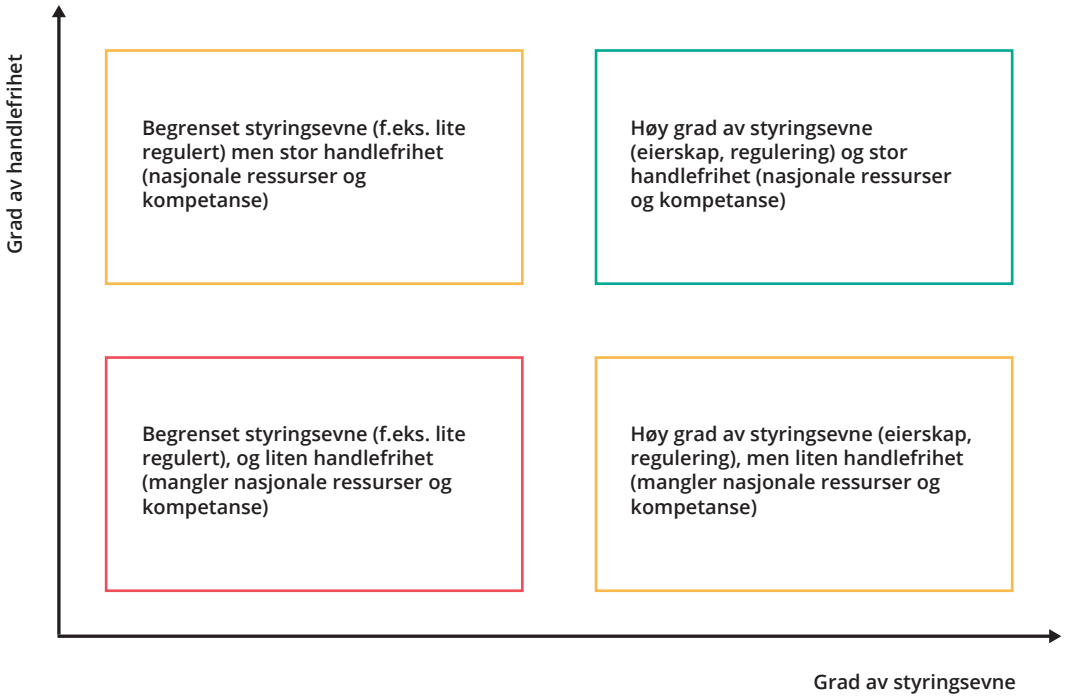
Slik utvalget vurderer det, omhandler nasjonal kontroll på sin side to sentrale aspekter; statens *styringsevne*, og statens *handlefrihet*. Styringsevne kan sees på som den myndigheten og det mandatet staten har til å fatte effektive beslutninger om digital infrastruktur gjennom for eksempel eierskap, regulering eller avtaler. Handlefrihet beskriver den fleksibiliteten og det handlingsrommet som staten har til å få implementert og gjennomført disse beslutningene uten å bli begrenset av utenlandske aktører eller andre eksterne faktorer.

[13] The Digital Europe Programme, https://digital-strategy.ec.europa.eu/en/activities/digital-programme

[14] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 EUR-Lex – 02021R0694-20230921 – EN – EU https://e-estonia.com/data-embassy-the-digital-continuity-of-a-state/R-Lex

Forholdet mellom styringsevne og handlefrihet kan illustreres i figur 4.1.

Figur 4.1 Nasjonal kontroll som produkt av styringsevne og handlefrihet



Forholdet mellom styringsevne og handlefrihet kan for eksempel illustreres med autonomi-bestemmelsen i ekomforskriften. Sett for eksempel at en norsk mobiloperatør i fremtiden etablerer produksjon av 5G-tjenester på en utenlandsk skyplattform. Autonomi-bestemmelsen er i seg selv ikke til hinder for dette, så lenge myndigheten ikke har gitt mobiloperatøren pålegg om å innføre nasjonal autonomi. Bestemmelsen gir derimot myndighetene nødvendig *styringsevne* til å kunne pålegge nasjonal autonomi dersom en krise- eller beredskapssituasjon inntreffer.

Hvis operatøren ikke på forhånd har forberedt drift av 5G-tjenestene med infrastruktur, ressurser og kompetanse i Norge, vil statens *handlefrihet* imidlertid være begrenset, og beslutningen om å innføre nasjonal autonomi vil ikke kunne gjennomføres i praksis. I dette tilfellet oppnås handlefrihet gjennom at det faktisk er forberedt tilgjengelige innsatsfaktorer på norsk jord som legger til rette for nasjonal drift av 5G-tjenestene i en krise- eller beredskapssituasjon. Dette kan være at skyplattformen er designet slik at den enkelt kan flyttes og kjøres fra norske datasentre, at mobiloperatøren har tilrettelagt for et nasjonalt operasjonssenter, og at det er sikret driftsressurser med nødvendig kompetanse i Norge. Eksemplet viser at både styringsevne og handlefrihet er nødvendig for å oppnå reell nasjonal kontroll.

Det er viktig å påpeke at det i alle beskrivelser av nasjonal kontroll (og autonomi og suverenitet) er en erkjennelse av at kontrollen ikke kan være fullstendig (100 %). Alle digitale infrastrukturer, produkter og tjenester vil ha visse avhengigheter til funksjoner

eller innsatsfaktorer, direkte eller i indirekte i leverandørkjeden, som reduserer den nasjonale kontrollen. Dette omtales nærmere i kap. 13.

Oppsummert legger utvalget derfor følgende definisjon av nasjonal kontroll i digital kommunikasjonsinfrastruktur til grunn:

Boks 4.2

Nasjonal kontroll innebærer at staten, i tilknytning til kritisk digital kommunikasjonsinfrastruktur, har

1) *styringsevne* til å ta effektive beslutninger gjennom for eksempel regulering, eierskap eller avtaler

2) *handlefrihet* til å gjennomføre beslutningene mest mulig uavhengig av utenlandske aktører og innsatsfaktorer.

4.2 Trussel- og risikobildet

Det er et stort spenn av farer og trusler som kan ramme sektoren for digital infrastruktur. Dette omfatter både utilsiktede hendelser som naturhendelser, menneskelige feil og programvarefeil, og tilsiktede hendelser som fysisk sabotasje, cyberangrep og spionasje. For utvalgets arbeid avgrenses omtalen til det som anses mest relevant i kontekst av nasjonal kontroll. Det vil si, aktiviteter som truer de nasjonale sikkerhetsinteressene gjennom å svekke statens styringsevne eller handlefrihet, eller hvor den sikkerhetstruende effekten av aktiviteten forsterkes av manglende nasjonal kontroll.

4.2.1 Sikkerhetsmyndighetens vurderinger

Etterretningstjenestens rapport «Fokus 2024»[15] peker på at Norge nå står overfor et mer alvorlig trusselbilde enn på flere tiår. Russlands militærmakt forblir den dimensjonerende militære trusselen mot Norges suverenitet, sentrale samfunnsfunksjoner og infrastruktur. E-tjenesten peker videre på både petroleums- og internettinfrastrukturene som særlig utsatt, herunder undersjøisk infrastruktur. Disse infrastrukturene har blitt kartlagt over flere år, og er potensielle mål for sabotasje. Russland har vist både vilje og evne til å ramme kritisk infrastruktur i konfliktsituasjoner.

Når det gjelder innpass i vestlige verdikjeder og kritisk infrastruktur så har imidlertid sanksjonsregimet overfor Russland etter Ukraina-krigen gjort det vanskeligere for Russland å slippe inn. Det er derfor først og fremst Kina som i dag har evne og vilje til å forfølge en slik strategi, ifølge Etterretningstjenesten. Den peker på at slik innpass har høy verdi for fremmede makter, ved at det kan gi tilgang til sensitiv informasjon, gi mulighet til å kartlegge sårbarheter, og utnyttes til å forstyrre eller sabotere forsyningskjeder enten digitalt eller fysisk.

[15] Fokus 2024 – Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer, https://www.etterretningstjenesten.no/publikasjoner/fokus/Fokus24_innhold

Politiets sikkerhetstjeneste (PST) vurderer i sin «Nasjonal trusselvurdering 2024»[16] at Russland og Kina vil fortsette å utgjøre de største truslene når det gjelder spionasje og sikkerhetstruende økonomisk virksomhet mot Norge. Russland og Kina forventes å bruke oppkjøp og investeringer i norske selskaper for strategiske fordeler. Selv om disse økonomiske tiltakene ofte er lovlige, kan de true nasjonale interesser når de utnyttes samlet sett. Russland fokuserer på å dekke militære og teknologiske behov, for eksempel gjennom oppkjøp av eiendom nær norske militære installasjoner. Kina søker kontroll over kritiske råvarer og verdikjeder, som sjeldne jordarter, som er viktige for høyteknologi og det grønne skiftet. Bruk av kinesisk teknologi i norsk infrastruktur kan også utgjøre en sikkerhetstrussel ved å åpne for skjulte bakdører, ifølge PST.

I tillegg til sikkerhetstruende økonomiske virkemidler, peker PST på at fremmede stater bruker en rekke andre metoder mot mål i Norge. Dette inkluderer cyberoperasjoner, rekruttering av menneskelige kilder, etterretning ved bruk av sivile fartøy, påvirkningsoperasjoner, sabotasje og fordekte anskaffelser.

NSM fremhever i sin «Risiko 2024»-rapport[17] at privat næringslivet har stor betydning for både nasjonal og internasjonal sikkerhet, og peker blant annet på den norske petroleumsnæringen, men også andre deler av næringslivet. Herunder sier NSM at endringer i eierstrukturer kan medføre risiko for at blant annet sikkerhetsgradert informasjon kan tilflyte uvedkommende. Videre er NSM bekymret for det kinesiske «fotavtrykket» i nasjonale kritiske verdikjeder, noe som gir et handels- eller sikkerhetspolitisk maktmiddel som kan unyttes til å ramme grunnleggende nasjonale funksjoner i Norge. De viser til at flere vestlige land nå fører en strategi for å redusere avhengigheten av Kina i kritiske sektorer som forsvar, elektronisk kommunikasjon og energi, for å minimere slik risiko.

4.2.2 Risiko- og sårbarhetsvurdering av ekomsektoren

Nkom gjennomfører jevnlig risiko- og sårbarhetsvurderinger for sektoren elektronisk kommunikasjon (EkomROS). Dette er sektorspesifikke vurderinger som bygger på de overordnede risiko- og trusselvurderingene til sikkerhetsmyndighetene. I EkomROS 2024[18] peker Nkom på syv områder som anses som de største utfordringene, hvor særlig fire har relevans for nasjonal kontroll. Dette er avhengigheter og konsentrasjon i verdi- og leverandørkjeder, cyberangrep, innsidetrusselen og sabotasje (herunder sjøfiberkabler).

Nkom advarer om at den forverrede sikkerhetspolitiske situasjonen kan redusere tilgang til kritisk utstyr samt utenlandsk arbeidskraft som tar tid å sikkerhetsklarere. Avhengigheten til få leverandører for sentralt utstyr og programvare øker risikoen for omfattende skade dersom sårbarhetene utnyttes. Dette utgjør en sikkerhetsutfordring særlig for norske ekomtilbydere som er under sikkerhetsloven.

16 Nasjonal trusselvurdering 2024, PST, https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2024/

17 Risiko 2024 – Nasjonal sikkerhet – et felles ansvar, NSM, https://nsm.no/getfile.php/1313477-1719434219/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf

18 Risiko og sårbarhetsanalyse for ekomsektoren (2024), Nkom, file:///C:/Users/DFD1112/Downloads/EkomROS%202024%20-%20offentlig%20versjon%20(1).pdf

Cyberangrep utgjør en konstant trussel mot ekomnett og -tjenester, og den geopolitiske og teknologiske utviklingen påvirker dette trusselbildet. Økt bruk av skytjenester gir i mange tilfeller sikkerhetsfordeler, men kan også introdusere nye sårbarheter. En utfordring er at skybaserte løsninger til dels innebærer å gi fra seg kontroll med hvor tjenester blir produsert og data lagret, hvem som har tilganger, og hvordan uønskede hendelser håndteres. Nkom er spesielt bekymret for destruktive angrep på styringssystemer, og viser blant annet til angrepet på den ukrainske mobiloperatøren Kievstar i 2023 som førte til at mer enn 24 millioner abonnenter ble rammet i over en uke.

Når det gjelder sabotasjetrusselen, viser Nkom blant annet til at flere sjøfiberkabler har blitt skadet som følge av menneskelig aktivitet de siste årene. I Norge gjelder dette blant annet Svalbardfiberen, som ble utsatt for skader gjennom tråling i 2022. Det har også vært flere tilfeller i Østersjøen den siste tiden. Skader på undersjøisk infrastruktur er ofte utilsiktet som følge av fiskeriaktivitet eller ankring. Samtidig peker Nkom på at tilsiktede handlinger kan skjules som uhell slik at attribusjon mot en spesifikk aktør blir vanskelig, og viser blant annet til Russlands hybride virkemiddelbruk. Slike kamuflerte uhell kan brukes blant annet for å kartlegge de berørte landenes rettekapasitet og avdekke svakheter ved disse.

4.2.3 Nærmere om sikkerhetstruende økonomiske aktivitet

Som omtalt i PSTs og NSMs trussel- og risikovurderinger over, så er oppkjøp og investeringer i norske virksomheter et virkemiddel som andre stater benytter for å opparbeide seg strategiske fordeler som kan true våre nasjonale sikkerhetsinteresser. Forsvarets forskningsinstitutt (FFI) har i en rapport[19] undersøkt hvordan andre staters økonomiske virkemidler kan true nasjonal sikkerhet og hvordan dette kan integreres i risiko- og sårbarhetsanalyser.

Begrepet *sikkerhetstruende økonomisk aktivitet* er beskrevet i NSMs veiledninger knyttet til bestemmelsene i sikkerhetslovens kapittel 10 om eierskapskontroll. I veiledningen[20] skriver NSM:

> «Flere stater bruker økonomiske virkemidler til andre formål enn forretninger. Utenlandske investeringer i og oppkjøp av norske virksomheter kan benyttes for å få innsikt i sensitiv informasjon og tilgang til teknologi og ressurser av strategisk betydning. Her benytter vi begrepet «sikkerhetstruende økonomisk virksomhet» om sikkerhetstruende investeringer og oppkjøp.
>
> Statens ønske om kontroll med eierskap i strategisk viktige sektorer kommer av økt bevissthet om at oppkjøp av norske virksomheter kan være sikkerhetstruende virksomhet.
>
> Med sikkerhetstruende virksomhet menes en tilsiktet handling som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Et eksempel kan være

[19] Utenlandske investeringer og andre økonomiske virkemidler – når truer de nasjonal sikkerhet? FFI-rapport 20/03149, https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2832/03149.pdf

[20] Hva er sikkerhetstruende økonomisk aktivitet? Veiledning NSM, https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/handtering-av-sikkerhetstruende-okonomisk-virksomhet/hva-er-sikkerhetstruende-okonomisk-virksomhet/

at virksomheten i forbindelse med et oppkjøp blir gjort kjent med at kjøper har koblinger til en trusselaktør, for eksempel et land som representerer en etterretningstrussel mot Norge.

Sikkerhetstruende økonomisk virksomhet kan omfatte mange ulike typer aktiviteter. Det kan blant annet dreie seg om informasjonsinnhenting, påvirkning og skadeverk som søkes oppnådd gjennom at eksisterende eierskap styres eller manipuleres inn i posisjon, eller gjennom oppkjøp og overdragelser av eierskap som allerede er i posisjon.

Strategiske investeringer og oppkjøp kan skje gjennom stråselskaper og komplekse selskapsstrukturer og kan dermed være vanskelig å avdekke. Videre kan det være vanskelig å skille strategiske oppkjøp med illegitime hensikter fra ordinær porteføljeforvaltning foretatt ut fra rene kommersielle hensyn. Det vil følgelig kunne være utfordrende å avdekke slik aktivitet, samt å vurdere risikoen knyttet til aktiviteten.»

FFI beskriver ulike typer økonomiske aktiviteter, både direkteinvesteringer i Norge som nyetableringer («greenfield»), sammenslåinger og oppkjøp, men også import/eksport, sanksjoner og økonomisk spionasje og korrupsjon. Videre beskriver de ulike typer målsetninger som kan ligge bak slike sikkerhetstruende økonomiske aktiviteter, og hvor det å sikre nasjonal kontroll blir viktig. Ett mål er å fremtvinge politisk endring gjennom å opparbeide seg en posisjon til å enten kortsiktig eller langsiktig kunne påvirke norske politiske prosesser og standpunkt. Et annet mål er å forsvare sin egen (militære) handlefrihet gjennom å få kontroll på kritiske innsatsfaktorer eller infrastruktur i Norge som man selv er avhengig av, for å opprettholde egen makt. Et tredje mål kan være å oppnå en strategisk fordel. Dette kan være gjennom tilgang på informasjon, teknologi eller andre ressurser, som igjen kan være springbrett for å gjennomføre alvorlige handlinger.

Når en trusselaktør har oppnådd en strategisk fordel overfor et annet land, er hensikten med dette å kunne «utløse» fordelen i situasjoner som gir maksimal gevinst for aktøren. Dette kan være gjennom handlinger av både politisk, økonomisk eller militær art – og dermed i ytterste konsekvens ved væpnet konflikt og krig.

4.2.4 Den ytterste enden av krisespekteret – konflikt og krig

Sikkerhetstruende økonomiske virkemidler som nevnt i kapittel 4.2.3 kan, sammen med en rekke andre sikkerhetstruende virkemidler, være motivert av å oppnå strategiske fordeler, som kan utløses i situasjoner der dette behøves. I ytterste konsekvens kan dette være i væpnet konflikt og krig. Når behovet for nasjonal kontroll skal vurderes i hele krisespekteret, er det derfor også viktig å se hen til scenarier i den ytterste enden av spekteret. Treffsikkerheten og effekten av angrep mot digital infrastruktur med både konvensjonelle og cyberbaserte våpen, kan da avhenge av hvilke etterretning og informasjon trusselaktøren sitter på. Dette informasjonstilfanget kan være opparbeidet over lang tid gjennom økonomiske eller andre typer virkemidler – enten rettet direkte mot den aktuelle infrastrukturen, eller indirekte via leverandør- og verdikjeder.

I 2024 publiserte FFI en rapport[21] som oppsummerer de viktigste erfaringene og læringspunktene fra krigen i Ukraina, og hvilken overføringsverdi dette har for det norske og vestlige lands forsvar. FFI tar blant annet opp Russlands hybridkrigføring, og på cyberangrep på ukrainske informasjonssystemer i forkant av invasjonen i 2022. Slike angrep må påregnes som en integrert del av en væpnet konflikt, hvor formålet kan være å ramme kommunikasjonen mellom militære og sivile myndigheter og mellom myndigheter og befolkningen, ramme beredskapstiltak og generelt slite ned tilliten i samfunnet.

Når det gjelder bruk av konvensjonelle våpen viser FFI til at Russland gjennom krigen i omfattende grad har brukt langtrekkende missiler og droner mot ukrainske mål, først militære mål, deretter forsvarsindustrimål, kommunikasjonsinfrastruktur, jernbane, drivstofflagre og raffinerier, og til slutt rene sivile mål og sivil infrastruktur. Det er også gjennomført cyberangrep mot mål i vestlige land som har sendt våpen og annen hjelp til Ukraina.

FFI mener at Russlands handlingsmønster om bruk av hybride og irregulære virkemidler sammen med væpnet konflikt har høy signifikans og overførbarhet til norske forhold. De mener derfor at Norge må bygge opp både en militær og sivil motstandsdyktighet mot slike sammensatte trusler. Når det gjelder informasjonssystemer uttrykker de:

> «Konsekvensen er at det må legges stor vekt på å beskytte de informasjonssystemene norske myndigheter er avhengige av i krig og konflikt, både ved å gjøre systemene robuste og sørge for redundans som muliggjør bruk av alternative kommunikasjonskanaler.»

Utvalget vil presisere at robusthet og redundans må sees på som komplementære strategier, og viser da henholdsvis til omtalen av nasjonale fortifikatoriske anlegg i kapittel 5, og eksempelet med å etablere redundante systemer for datalagring og prosessering i «data-ambassader» i utlandet, som nevnt i kapittel 4.1.1.

4.3 Økonomiske aktivitet som kan ha kontrollsvekkende effekt

For de aller fleste tilfeller av økonomiske aktiviteter knyttet til norsk digital infrastruktur som innebærer utenlandske aktører, må man anta at det ikke ligger noe direkte *sikkerhetstruende formål* bak. Den utenlandske aktøren vil som oftest ha et rent kommersielt motiv, eventuelt støttet opp under legitime handelspolitiske og innenrikspolitiske mål fra hjemstaten. Likevel, selv om den utenlandske aktørens motiv er legitimt, kan effekten av slike økonomiske aktiviteter samtidig svekke vår nasjonale styringsevne og handlefrihet. Dette kan typisk skje ved at det utilsiktet oppstår bortfall eller forstyrrelser i de utenlandske innsatsfaktorene man er avhengig av (f.eks. feilsituasjoner eller ressursknapphet). I slike situasjoner kan staten som kontrollerer innsatsfaktoren bli tvunget til å prioritere egne behov fremfor andre lands behov. Sågar kan endringer i det handelspolitiske eller sikkerhetspolitiske landskapet gjøre at den

[21] Erfaringer fra krigen i Ukraina – læringspunkter etter tusen dager med krig, FFI-rapport 24/01299, https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3313/24-01299.pdf

utenlandske staten finner grunnlag for å utnytte maktposisjonen også til andre formål. Dette peker også FFI på i sin rapport om sikkerhetstruende økonomiske virkemidler:

> «Samtidig kan det ikke utelukkes at selv om motivasjonen i utgangspunktet er ressurssikkerhet av innenrikspolitiske hensyn, så kan kontroll over selskaper og ressurser gi avsenderstaten makt som senere kan brukes også til andre formål.»

Utvalget vil i denne sammenheng peke på at den norske digitale kommunikasjonsinfrastrukturen både er kapitalkrevende, og avhengig av internasjonale innsatsfaktorer. Kapital, utstyr, teknologi, programvare og kompetanse må i stor grad skaffes til veie gjennom utenlandske investeringer, eller gjennom utenlandske leverandører og samarbeidspartnere. Nedenfor omtaler utvalget noen aktuelle typer økonomiske aktiviteter som observeres i sektoren for elektronisk kommunikasjon. Disse økonomiske aktivitetene kan i mange tilfeller bidra til å styrke sikkerheten, men kan også ha en kontrollsvekkende effekt, selv uten at det nødvendigvis ligger et sikkerhetstruende motiv bak.

4.3.1 Konsolideringer

Det er i økende grad diskusjoner om behov for europeiske konsolideringer innenfor den europeiske (og nordiske) telekomsektoren, for å styrke den europeiske konkurranse- og innovasjonskraften, i møte med de stadig sterkere amerikanske og asiatiske teknologimotorene. Dette kan innebære at det i fremtiden blir færre og større selskaper innenfor sektoren i Norden og innenfor EØS, og for Norges del mer utenlandsk eierskap i nasjonal digital kommunikasjonsinfrastruktur. Disse utviklingstrekkene er beskrevet i mer detalj i kapittel 7. Konsolideringer vil typisk skje gjennom oppkjøp eller fusjoner av selskaper, altså eierskapstransaksjoner. Eierskap samt regulering av eierskap (eierskapskontroll) er virkemidler for nasjonal kontroll som omtales i mer detalj i kapittel 8.

4.3.2 Nyetablering (greenfield)

En nyetablering (greenfield-investering) refererer til utbygging av helt ny infrastruktur fra grunnen av, i motsetning til brownfield-investeringer som involverer oppgradering eller utvidelse av eksisterende infrastruktur. I sammenheng med kritisk digital kommunikasjonsinfrastruktur har vi for eksempel sett en betydelig datasenteretablering i Norge de siste årene.

I forhold til nasjonal kontroll kan denne type etablering være tveegget. På den ene siden vil utenlandske aktørers etablering av datasenter i Norge bidra til å styrke den nasjonale kontrollen ved at tjenester produseres og data lagres på norsk jord. Regjeringens gjeldende politikk er også at Norge skal være attraktiv for datasenteretableringer som bidrar til verdiskaping i Norge.[22] Et konkret eksempel på en slik større utenlandsk greenfield-investering er Googles planlagte etablering av datasenter i Skien.[23]

[22] Fremtidens digitale Norge Nasjonal digitaliseringsstrategi 2024–2030, https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf

[23] NRK 2024 https://www.nrk.no/vestfoldogtelemark/google-bygger-enormt-datasenter-i-skien-1.16749861

På en annen side kan utenlandsk nyetablering sette nasjonale sikkerhets- eller samfunnsinteresser på prøve. De siste årene har det for eksempel vært flere eksempler på uønskede utenlandske datasenteretableringer, hovedsakelig knyttet til kryptoutvinning, noe som forsøkes å avbøtes blant annet gjennom krav i den nye ekomloven som ble vedtatt i 2024. Også TikToks etablering i Norge, via Green Mountains nyetablering av datasenter i Innlandet, var omstridt. Saken ble behandlet i det interdepartementale screeningnettverket, men det ble ikke funnet grunnlag for å stoppe prosessen.[24]

4.3.3 Strategiske partnerskap

Et strategisk partnerskap er et langsiktig samarbeid mellom selskaper som har kompetanse, ressurser og teknologi som utfyller hverandre. For selskaper som forvalter kritisk digital infrastruktur, som for eksempel mobiloperatører, kan et strategisk partnerskap med utenlandske teknologipartnere eller skytjenesteleverandører gi flere fordeler som tilgang til teknologi, ekspertise og innovasjon som kan hjelpe dem å holde tritt med den raske teknologiske utviklingen, utvikle nye tjenester og forretningsmodeller, styrke sikkerheten, effektivisere driften osv.

I Norge er det mange eksempler på strategiske partnerskap mellom operatører av digital infrastruktur og internasjonale teknologiselskaper. Dette inkluderer for eksempel Telenor og Google Cloud[25], Telenor og NVIDIA[26], Telia og Microsoft[27], og Tampnet og OneWeb.[28]

Hvordan det strategiske partnerskapet kan påvirke den nasjonale kontrollen med den digitale infrastrukturen varierer selvsagt, avhengig av hvordan partnerskapet er utformet og graden av operasjonell eller teknologisk integrasjon. Jo tettere den utenlandske aktøren er integrert i selskapets teknologi og drift, desto større kan deres innflytelse bli. Et partnerskap vil typisk være regulert gjennom en avtale, et virkemiddel for nasjonal kontroll som omtales i mer detalj i kapittel 9.

4.3.4 Fellesforetak og konsortium

Et fellesforetak («joint venture») er et samarbeid der to eller flere selskaper etablerer en egen juridisk enhet for å nå et felles mål, for eksempel utviklings- og investeringsprosjekter. Partnerne deler på finansiering, kompetanse, fortjeneste og risiko i det nye selskapet. Graden av nasjonal kontroll påvirkes da av fordelingen av eierskap i det nye selskapet, og selvsagt opprinnelseslandet til selskapene som har inngått samarbeidet. For eksempel signerte i 2019 den finske telekomaktøren Cinia og den russiske telekomaktøren Megafon en intensjonsavtale om å bygge ut ny sjøfiberkabel

[24] Regjeringen.no 2023, https://www.regjeringen.no/no/aktuelt/green-mountain-vert-underlagt-sikkerheitslova-og-far-etablere-datasenter-i-innlandet/id2989926/

[25] NTB 2021, https://kommunikasjon.ntb.no/pressemelding/17920407/telenor-og-google-cloud-inngar-strategisk-partnerskap?publisherId=4954260

[26] NTB 2024, https://kommunikasjon.ntb.no/pressemelding/18052346/telenor-group-announces-collaboration-with-nvidia-to-support-its-ai-first-ambition?publisherId=4954260

[27] Telia 2024, https://presse.telia.no/pressreleases/telia-tar-sitt-nordiske-partnerskap-med-microsoft-til-det-norske-markedet-forenkler-hverdagen-for-bedriftskundene-3357446

[28] Tampnet 2021, https://www.tampnet.com/press/tampnet-and-oneweb-sign-agreement-to-further-develop-the-next-generation-of-offshore-connectivity-capabilities

som skulle forbinde Europa med Asia gjennom Nordøstpassasjen gjennom selskapet «Arctic Link Development Oy». Senere koblet også et norsk selskap seg på prosjektet, et datterselskap av det offentlig eide selskapet Bredbåndsfylket, med tanke på ilandføring av kabelen i Nord-Norge. Utviklingsprosjektet ble imidlertid ikke gjennomført, og ble avsluttet i 2021.[29]

4.3.5 Salg av innhold i selskaper

Som del av teknologi- og markedsutviklingen har tradisjonelle vertikalt integrerte telekomselskaper, som for eksempel Telenor, gjennom ulike faser foretatt salg av innhold i selskapene. Ved å skille ut eierskap til slike eiendeler i egne selskaper og eventuelt selge hele eller deler av det nye selskapet, kan selskapene redusere sin gjeld, øke likviditeten og bruke midlene til å investere i nye vekstområder. Det etableres da gjerne samarbeidsmodeller med det nye selskapet for å sikre fortsatt tilgang til infrastrukturen, uten å binde opp like store ressurser som når man eide den selv. Samtidig skapes det også et avhengighetsforhold til det nye selskapet som da blir en, potensielt kritisk, del av leverandør-/verdikjeden. For eksempel har nå alle tre norske mobiloperatører, Telia, Telenor og Lyse Tele /Ice flyttet operasjon av mobiltårn, inkludert utstyrshytter, strøm og kjøling, ut i egne mobiltårnselskaper, henholdsvis Telia Towers, Telenor Towers og Tårnselskapet. I 2023 ble også Telenors fibernett skilt ut i eget selskap, Telenor Fiber, hvorpå 30 prosent av selskapet ble solgt til det globale investeringsselskapet KKR og Oslo Pensjonsforsikring.[30] Staten satte betingelser i forbindelse med denne transaksjonen, som omtales nærmere i kapittel 9.2.2.

4.3.6 Leverandørvalg og administrerte tjenester

Innenfor elektronisk kommunikasjon går også teknologiutviklingen svært raskt. Utvikling, innovasjon og effektiv drift krever mer og mer spesialisert kompetanse som norske aktører må innhente gjennom tettere integrert samarbeid med utenlandske utstyrsleverandører, som for eksempel Cisco, Juniper, Palo Alto, Nokia, Ericsson og Huawei. I økende grad drifter også leverandørene tjenestene i tilknytning til utstyret på vegne av kunden (administrerte tjenester – managed services). Dette er grunnet kompleksiteten i leveransene, og gjør det mer skalerbart og fleksibelt for kunden, som da kan fokusere på kjerneoppgaver. I norsk telekom-sammenheng er nok den mest omtalte leverandørvalgsaken knyttet til Telias og Telenors valg av leverandør for deres 5G mobilnett i perioden 2020-2021. Her satte sikkerhetskravene i ekomloven og sikkerhetsloven begrensninger for hvordan operatørene kunne benytte leverandører fra land som Norge ikke har sikkerhetsmessig samarbeid med.[31] Dette omtales også nærmere i kapittel 9.6.

[29] NRK 2022, https://www.nrk.no/tromsogfinnmark/rodt-krever-svar-etter-at-bredbandsfylket-avtalte-samarbeid-med-russiske-megafon-1.16183441

[30] NTB 2022, https://kommunikasjon.ntb.no/pressemelding/17942689/telenor-etablerer-fiberselskap-i-norge?publisherId=4954260

[31] Spørsmål til skriftlig besvarelse nr. 18 fra stortingsrepresentant Christian Tybring-Gjedde, https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qnid=67684

4.3.7 Utkontraktering og offshoring

Utkontraktering og offshoring av forretningsfunksjoner, som for eksempel IT utvikling og drift, IT-sikkerhetstjenester, nettverksovervåking, osv. er også en vanlig strategi for å optimalisere driften. Dette gjelder for stort sett alle typer virksomheter, inkludert operatører av kritisk digital infrastruktur. Slike leverandører har ofte spesialiserte ressurser som kan tilby kontinuerlig overvåking og en robust infrastruktur som møter høye sikkerhetsstandarder, geografisk spredning og redundans.

Avhengigheten til utenlandske leverandører av slike tjenester, og deres leverandørkjeder igjen, kan imidlertid også få negative konsekvenser for sikkerheten i den nasjonale digitale infrastrukturen. Utilsiktede feil i leverandørkjeder har potensiale til å spre seg raskt og få vidtrekkende konsekvenser gjennom at det kan ramme alle kunder som er avhengig av leverandøren samtidig, noe som forsterker omfanget og konsekvensene av avbruddet. Dette ble blant annet tydelig sommeren 2024 da en programvareoppdatering hos sikkerhetsleverandøren Crowdstrike førte til krasj av Windows-systemer, og som påvirket samfunnskritiske tjenester over hele verden[32] – dog med begrensede konsekvenser i Norge. Et annet eksempel er «Nødnett-saken» tilbake i 2016-2017, hvor det ble avdekket at IT-driftspersonell i India satt med uautoriserte tilganger til Nødnett gjennom Nødnetts sambandsleverandørkjede.[33] Tilgangene var i strid med sikkerhetslovens bestemmelser, medførte fare for tap av nasjonal kontroll gjennom at skjermingsverdig informasjon om kritisk digital infrastruktur kunne komme på avveie, og en evne til å kunne ramme driften av Nødnett i Norge, fra India.

4.4 Aktuelle myndighetsprosesser

Regjeringens digitaliseringsstrategi «Fremtidens digitale Norge – Nasjonal digitaliseringsstrategi 2024-2030»[34] viser til at den strategiske retningen for å ivareta digital sikkerhet er nedfelt i Meld. St. 9 (2022–2023). Under digitaliseringsstrategiens mål om en sikker og fremtidsrettet digital infrastruktur fremgår det blant annet at regjeringen vil «*sikre tilstrekkelig nasjonal kontroll med den delen av den digitale grunnmuren som understøtter kritiske samfunnsfunksjoner*». I den sammenheng har det de siste årene pågått flere myndighetsprosesser som har relevans i forhold til nasjonal kontroll med digital infrastruktur. Noen av disse omtales i det følgende.

4.4.1 Konseptvalgutredning om nasjonal sky

En konseptvalgutredning for nasjonal skytjeneste[35] ble gjennomført av NSM på oppdrag fra JD i perioden februar 2022 til januar 2023. Bakgrunnen for utredningen var erkjennelsen av at avhengigheten av utenlandske skytjenester kan utgjøre en sårbarhet

[32] Digi.no 2024, https://www.digi.no/artikler/nsm-etter-crowdstrike-still-kritiske-sporsmal-om-programvareutviklingen/549154

[33] Felles redegjørelse NSM og Nkom, https://www.regjeringen.no/contentassets/17dba73e91354368aad3d53d600a18b0/tilsyn-med-nodnett---felles-redegjorelse-nsm-nkom.pdf

[34] Fremtidens digitale Norge Nasjonal digitaliseringsstrategi 2024–2030, https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf

[35] Konseptvalgutredning for nasjonal skytjeneste 2023, NSM, https://nsm.no/getfile.php/1313330-1696430485/NSM/Filer/Dokumenter/Rapporter/Nasjonal%20skytjeneste%20-%20konseptvalgutredning%20-%20KVU%202023.pdf

for visse datatyper og IKT-systemer i statsforvaltningen, som er viktige å beskytte og ha kontroll på for å ivareta nasjonale sikkerhetsinteresser. Utredningen gjaldt ikke sikkerhetsgradert informasjon, men skjermingsverdig ugradert informasjon (iht. sikkerhetsloven) og annen ugradert beskyttelsesverdig informasjon. Dette kan typisk være statlige IT-systemer og data knyttet til valgsystemet, personregistre, helseregistre, eiendomsregistre, infrastruktur- og transportsystemer mv.

I analysen estimerer NSM at om dagens utviklingstrender knyttet til bruk av skytjenester fortsetter, så vil om ti år om lag 80 % av slike beskyttelsesverdige data og systemer ligge på skybaserte løsninger, de fleste helt eller delvis utenfor nasjonal jurisdiksjon. NSM mener derfor det er viktig å styrke den nasjonale kontrollen på disse løsningene for å sikre myndighetenes evne til å ivareta konfidensialiteten, tilgjengeligheten og integriteten i både fred, men også i krise og i væpnet konflikt. Konseptvalgutredningen vurderer ulike skybaserte løsningskonsepter som skal ivareta tilstrekkelig nasjonal kontroll, samtidig som de balanseres opp mot behovet for kostnadseffektivitet, funksjonalitet og innovasjon som følger av moderne (kommersielle) skyløsninger. NSM vurderer fem ulike konsepter hvor de anbefaler en harmonisering av regelverk og sterkere regulering av det offentliges bruk av skytjenester samt et kombinasjonskonsept bestående av 1) en statlig lukket skyløsning for de mest kritiske dataene og systemene, og 2) en lukket kommersiell sky for de øvrige data og systemer.

Det inngår i statens prosjektmodell at konseptvalgutredninger skal kvalitetssikres av eksterne rådgivere. I kvalitetssikringsrapporten konkluderes det med at konseptet med en lukket kommersiell sky kommer best ut på de prissatte virkningene. En statlig lukket skyløsning vurderes å ville både koste vesentlig mer og gi dårligere funksjonalitet og innovasjon, men vil samtidig gi større nasjonal kontroll. Imidlertid påpeker kvalitetssikrerne at det ikke nødvendigvis er en direkte sammenheng mellom økt nasjonal kontroll og økt sikkerhet, og at en lukket kommersiell sky kan komme like godt eller bedre ut enn en statlig lukket skyløsning. De mener derfor det er betydelig usikkerhet knyttet til nytteverdien for en statlig lukket skyløsning sett opp mot ekstrakostnadene som en slik løsning vil innebære. Oppsummert anbefaler kvalitetssikrerne at det gjennomføres supplerende analyser før endelig beslutning om konsept tas.

Regjeringen har deretter tatt beslutning om konsept og arbeidet er tatt videre.[36] Konseptet innebærer en lukket skytjeneste hvor det gjennom sikkerhetsgraderte anskaffelser inngås en avtale med en eller noen få leverandører som skal utvikle, drifte og forvalte en nasjonal skytjeneste. Videre er det presisert at det skal stilles krav til nasjonal kontroll i leveransen.

4.4.2 Langtidsplanen for Forsvaret og totalberedskapsmeldingen

I desember 2021 nedsatte regjeringen Forsvarskommisjonen av 2021. Kommisjonens mandat var å vurdere sikkerhets- og forsvarspolitiske veivalg for Norge i et 10-20-års perspektiv. I januar 2022 ble Totalberedskapskommisjonen nedsatt, som en parallell prosess for å vurdere samfunnets samlede beredskapsressurser. De to utredningene ble

[36] Stortinget, møte den 18. april 2024, https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2023-2024/refs-202324-04-18?m=3, Meld. St. 9 (2024 –2025) Totalberedskapsmeldingen, https://www.regjeringen.no/contentassets/c24e6978185f4a49a7d2689a4741a9b1/no/pdfs/stm202402250009000dddpdfs.pdf

avgitt i 2023, som henholdsvis NOU 2023: 14 *Forsvarskommisjonen av 2021 – Forsvar for fred og frihet* og NOU 2023: 17 *Nå er det alvor – Rustet for en usikker fremtid*. Til sammen gir utredningene en omfattende gjennomgang av Norges sikkerhet og beredskap i et stadig mer komplekst trusselbilde.

Forsvarskommisjonen tegner et alvorlig situasjonsbilde av dagens norske forsvarsevne. Etter en fredelig periode i vår del av verden etter den kalde krigen og frem til Russlands fullskala invasjon av Ukraina i 2022, så samsvarer ikke lenger dagens forsvarsevne med dagens sikkerhetspolitiske situasjon, og utviklingen som ventes de neste 10–20 årene. Kommisjonen peker derfor på tre sentrale erkjennelser som må ligge til grunn for videre politikkutforming: Norske myndigheter og befolkning må ta innover seg alvoret i situasjonen, myndighetene må handle raskt, og utfordringene stiller krav til en helhetlig politikk.

I tillegg til de rent forsvarsfaglige anbefalingene, understreker Forsvarskommisjonen at Norge ikke kan forsvares utelukkende med militære virkemidler. Blant annet skriver de:

> «Vårt totalforsvar er tilpasset en tid der trusselen om krig på eget territorium har vært ansett som liten. Reaksjonsevnen og utholdenheten er for dårlig til å møte dagens og fremtidens utfordringer. Norske myndigheter må systematisere arbeidet med nasjonalt og alliert planverk, slik at sivil og militær side baserer seg på de samme planforutsetningene. Næringslivets rolle og ansvar for å bidra til å gjøre landet vårt tryggere blir viktigere.»

Som del av dette mente Forsvarskommisjonen at den nasjonale kontrollen med digitale verdier bør styrkes, herunder i form av digital infrastruktur på norsk territorium, og at det bør etableres et minimumsnivå av tilgjengelighet og digital forsyningsevne.

5. april 2024 la regjeringen frem Prop. 87 S (2023–2024) *Forsvarsløftet – for Norges trygghet*. Denne langtidsplanen innebærer en betydelig styrking av forsvarssektoren fra 2025 og frem til 2036. Gjennom et bredt forlik på Stortinget ble den endelige langtidsplanen fastsatt i juni 2024. Planen innebærer både en utbedring av kritiske mangler i dagens forsvar, og betydelige satsinger på flere områder. Dette omfatter styrkinger både på det maritime området, i Hæren og Heimevernet, på styrket luftvern og styrket overvåkning og kontroll, herunder på satellittområdet. I forholdet til samhandlingen med sivil side, peker langtidsplanen blant annet på at Norden nå er samlet i NATO og at dette muliggjør videreutviklingen av et totalforsvar i en nordisk kontekst. Videre legger planen vekt på å styrke samarbeidet med sivile myndigheter og sivilt næringsliv, og viser blant annet til de positive erfaringene med gjensidig støtte for å kartlegge og beskytte undersjøisk infrastruktur på norsk sokkel etter sabotasjen på Nord Stream-ledningene.[37] Også når det gjelder forsvarets virksomhet i cyberdomenet, herunder beskyttelse og videreutvikling av forsvarets IKT-systemer, så påpekes behovet for å samarbeide tett med sivile aktører.

På sivil side går Totalberedskapskommisjonens rapport nærmere inn på temaet nasjonal kontroll med digital infrastruktur. De peker på at ekomnett og -tjenester er bygget opp og dimensjonert for fredstid, og at sektoren er sårbar for langvarige forstyrrelser

[37] Økt sikkerhet for kritisk infrastruktur på norsk sokkel -https://www.regjeringen.no/contentassets/c24e6978185f4a49a7d2689a4741a9b1/no/pdfs/stm202420250009000dddpdfs.pdf regjeringen.no

i internasjonale forsyningskjeder. Videre peker de på et underskudd av tilgang på teknologi- og sikkerhetskompetanse i Norge:

> «Gitt den sikkerhetspolitiske situasjonen i Europa og erfaringene vi har med koronapandemi og større globale hendelser, mener kommisjonen at det må utarbeides operasjonelle krav til nasjonal egenevne til produksjon, vedlikehold og gjenoppretting. Ved en større internasjonal krise vil utenlandske ressurser måtte benyttes i landet de befinner seg i. Det må derfor fastsettes hvilken grunnleggende kompetanse, hvilke funksjoner og hvilket utstyr som skal være tilgjengelig innenfor Norges grenser. Det vil ta tid for sektoren å tilpasse seg, og arbeidet må derfor sette i gang så raskt som mulig.»

Blant annet anbefaler Totalberedskapskommisjonen at kravene til nasjonal autonomi operasjonaliseres, men også at man vurderer hvordan et styrket nordisk samarbeid kan styrke robustheten og motstandsdyktigheten i sektoren.

Blant annet med grunnlag i NOU 2023: 17 la regjeringen 10. januar 2025 frem Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen*. Stortingsmeldingen identifiserer tre hovedmål for regjeringens arbeid med å styrke totalberedskapen. Dette er å sikre et sivilt samfunn som 1) er forberedt på krise og krig, 2) motstår sammensatte trusler, og 3) understøtter militær innsats. For å nå målene legger regjeringen frem syv strategiske retninger, hvor ett av de er å «*styrke digital motstandskraft og nasjonal kontroll over kritisk infrastruktur og strategisk viktige virksomheter, naturressurser, eiendom og verdie*r». Regjeringen påpeker i meldingen at den nasjonale kontrollen skal innrettes slik at den ivaretar forutsigbarhet for næringslivet, og som bevarer Norge som en åpen økonomi.

4.4.3 Proaktive og reaktive myndighetstiltak relatert til nasjonal kontroll

Myndighetene har de siste årene håndtert flere konkrete saker relatert til digital kommunikasjonsinfrastruktur hvor nasjonal kontroll er et sentralt moment. Noen av disse aktivitetene er proaktive prosjekter initiert av myndighetene, andre er reaktive kontroller og tiltak av for eksempel utenlandsinvesteringer.

Av proaktive grep så er kanskje satsingen innenfor norsk romvirksomhet det mest fremtredende. Romteknologi og satellitter er sentrale for kommunikasjon så vel som andre viktige samfunnsfunksjoner innenfor transport, energiforsyning, overvåking og værvarsling. Satellittjenestene spiller også en viktig rolle for Norge i suverenitetshevdelse, militær beredskap og etterretning. Viktige milepæler som styrker nasjonal kontroll i kommunikasjonssammenheng ble nådd i 2024. I august ble to norske bredbåndssatellitter i Arctic Satellite Broadband Mission fra statlig eide Space Norway skutt opp fra California i USA. I desember ble systemet satt i drift, og sikrer nå at Norge har kontroll over strategisk viktige kommunikasjonstjenester for blant annet Forsvaret i store områder i Arktis som før har vært uten dekning.[38] Tidlig i 2024 gjennomførte også Space Norway oppkjøp av selskapet Telenor Satellite AS. Oppkjøpet forutsatte en kapitaltilførsel til Space Norway på 2,36 milliarder kroner, som ble godkjent av Stortinget like før jul 2023. Oppkjøpet ble av myndighetene vurdert både strategisk

[38] https://spacenorway.com/news/space-norway-delivery-enhances-the-armed-forces-operational-capability-in-the-high-north/

og markedsmessig fornuftig, samtidig som det bidrar til å sikre nasjonal kontroll over satellitter som er viktig for samfunnsviktige funksjoner.[39]

Innenfor ekomsektoren har det de siste årene også vært flere reaktive saker knyttet til screening av utenlandsinvesteringer og kontroll av andre typer økonomiske aktiviteter. Flere av disse omtales ulike steder i rapporten, og inkluderer blant annet myndighetenes presiseringer av begrensninger i valg av utstyrsleverandører til 5G-mobilnettene[40], screening av Telenors salg av en minoritetseierandel av Telenor Fiber AS[41], screening av GlobalConnects salg av kvalifisert eierandel til Mubadala[42], og vurderinger av Green Mountains etablering av datasenter i Innlandet med TikTok som kunde.[43]

4.5 Oppsummering

Utvalget har beskrevet hvordan nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur vil være et viktig virkemiddel for å ivareta nasjonale sikkerhetsinteresser. Nasjonal kontroll handler da om at staten er posisjonert til å kunne opprettholde en selvstendig styringsevne til å ta effektive beslutninger om kritisk digital kommunikasjonsinfrastruktur, og handlefrihet til å operere mest mulig uavhengig av utenlandske innsatsfaktorer, ressurser og kompetanse.

Sikkerhetsmyndighetenes trussel- og risikovurderinger, Forsvarskommisjonen og Totalberedskapskommisjonens analyser, og analysene til FFI, tegner et alvorlig bilde av den sikkerhetspolitiske situasjon i dag og i fremtiden. Disse vurderingene gir et tydelig signal om at denne styringsevnen og handlefriheten bør dimensjoneres etter scenarioer som befinner seg i den ytre enden av krisespekteret, som væpnet konflikt og krig.

Sikkerhetstruende økonomisk virksomhet er det som kanskje oftest knyttes til temaet nasjonal kontroll, og som kan svekke handlefriheten og styringsevnen. Dette inkluderer utenlandske investeringer i Norge hvor det kan ligge en skjult intensjon bak som kan true nasjonale sikkerhetsinteresser. Samlet vurderer utvalget at det er tre hovedmålsetninger som vil kunne ligge bak sikkerhetstruende økonomisk virksomhet fra utenlandske aktører. Det ene er makt og innflytelse over norsk kritisk digital infrastruktur for å kunne påvirke beslutningsprosesser som fremmer egen nasjons interesser. Det andre er å få tilgang på informasjon om for eksempel teknologi, infrastrukturtopologi, driftsforhold, beredskapstiltak, nøkkelpersonell osv. som har etterretningsverdi for den fremmede staten. Det tredje er å etablere evne til å kunne sabotere, hindre eller legge betingelser for norsk tilgang på kritisk digital infrastruktur i en krise- eller krigssituasjon.

Utvalget anser at ettersom elektronisk kommunikasjon er en kritisk innsatsfaktor for nær alle andre samfunnsfunksjoner, vil det at andre stater opparbeider seg en posisjon

[39] https://www.regjeringen.no/no/aktuelt/space-norway-med-avtale-om-kjop-av-telenor-satellite/id3014624/?expand=factbox3014627

[40] https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qnid=67684

[41] https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2023-2024/inns-202324-008s/?m=1&s=Telenor+Fiber#match_1

[42] https://www.regjeringen.no/no/aktuelt/regjeringen-setter-vilkar-knyttet-til-kjop-av-eierandel-i-globalconnect/id2970605/

[43] https://www.regjeringen.no/no/aktuelt/green-mountain-vert-underlagt-sikkerheitslova-og-far-etablere-datasenter-i-innlandet/id2989926/

til å kunne forsinke, nekte eller legge betingelser på vår egen tilgang til elektronisk kommunikasjon, være et kraftfullt virkemiddel for å svekke Norges evne i krise og krig.

For de aller fleste økonomiske aktiviteter som innebærer investeringer eller innflytelse fra utenlandske aktører, ligger det imidlertid ikke en skjult intensjon bak, men rene forretningsmessige motiver. Effekten av slike aktiviteter kan på den ene siden være at den styrker den nasjonale sikkerheten, for eksempel ved at det investeres mer i norsk digital infrastruktur som for eksempel bidrar til å bygge ut en sterkere og mer robust nasjonal infrastruktur som ellers ikke ville ha blitt bygd ut.

På den andre siden kan en utilsiktet effekt av slike aktiviteter være en svekkelse av den nasjonale kontrollen, enten direkte eller indirekte, og på kort sikt eller lang sikt. For det første, kan aktører som etablerer en større og større maktposisjon i norsk digital infrastruktur, senere finne grunnlag for å utnytte denne maktposisjonen til formål som kan true nasjonale sikkerhetsinteresser. Dette er også poengtert av FFI i rapporten om sikkerhetstruende økonomiske virkemidler. For det andre vil utvalget understreke at en utenlandsk maktposisjon også *utilsiktet* kan ramme våre nasjonale sikkerhetsinteresser, ved at Norge får redusert handlefrihet. Selv der norsk digital infrastruktur har avhengigheter til kritiske innsatsfaktorer i allierte og vennligsinnede land, så kan det i en krise- og krigssituasjon for eksempel oppstå ressursunderskudd. Siste års hendelser og konflikter har illustrert hvor sårbare de globale verdikjedene er. Dette viser at tilgang til for eksempel reserveutstyr og materiell for digital infrastruktur etter just-in-time-prinsippet, ikke lenger kan tas for gitt.

Tilgang til felles innsatsfaktorer som deles mellom nære geografiske og allierte land kan også bli utilgjengelige, særlig dersom innsatsfaktorene kun er dimensjonert for «fredstid». Dersom det oppstår hendelser som skaper underskudd på for eksempel kompetanse, utstyr eller rettekapasitet, kan man ikke se bort fra at landet som har førstehånds kontroll på ressursene, vil måtte prioritere å ivareta egne nasjonale behov fremfor andres. Dette påpekes også av totalberedskapskommisjonen.

Krise- og krigssituasjoner er generelt svært uforutsigbare i sin natur, noe som gjør at en må ta høyde for at uventede virkninger kan oppstå. Utvalget mener derfor det er avgjørende at staten har oppmerksomhet *både* på å identifisere sikkerhetstruende økonomiske aktiviteter, men *også* virkningen av økonomiske aktiviteter som ikke anses å være direkte sikkerhetstruende, men som utilsiktet kan få en kontrollsvekkende effekt på kortere eller lengre sikt.

”

Dette kapittelet redegjør for hvilke infrastrukturkategorier utvalget har lagt til grunn som kritiske, og gir et øyeblikksbilde over selskaper som eier kritisk infrastruktur i Norge.

Foto: Gunnstein Myhre (Nkom)

05

Selskaper som forvalter digital kommunikasjons-infrastruktur

5.1 Innledning

Utvalget er bedt om å beskrive dagens eierskapsstrukturer i selskapene som eier eller råder over kritisk digital kommunikasjonsinfrastruktur. I tillegg skal selskaper som er av avgjørende betydning for utbygging, drift og vedlikehold av infrastrukturen, og deres eiere, identifiseres.

Dette kapittelet redegjør for hvilke infrastrukturkategorier utvalget har lagt til grunn som kritiske, og selskaper som eier kritisk infrastruktur innen disse kategoriene er identifisert. Hvilke underleverandører[44] utvalget har sett nærmere på, samt beskrivelsen av eierskapsstrukturene i de identifiserte selskapene i dette kapittel og utvalgte underleverandører, fremgår av kapittel 6.

Formålet med dette kapittelet er i første rekke å etablere rammene for den oversikt og status på eierskap som utvalget skal legge til grunn i sitt arbeid. Identifiserte infrastrukturkategorier og selskaper viser naturlig nok et øyeblikksbilde, og oversikten ville sett annerledes ut for 10 år siden, og vil se annerledes ut 10 år frem i tid.

[44] Selskaper som er av avgjørende betydning for utbygging, drift og vedlikehold av infrastrukturen

5.2 Vurdering av kritisk digital kommunikasjonsinfrastruktur

Utvalget skal, til eget formål og på overordnet nivå, utarbeide en oversikt over kritisk digital kommunikasjonsinfrastruktur, av regional eller nasjonal betydning som:
- er viktig for statssikkerheten
- er av betydning for samfunnssikkerheten
- bærer tjenester av høy betydning for kritiske samfunnsfunksjoner

I denne vurderingen vil arbeidet med grunnleggende nasjonale funksjoner etter sikkerhetsloven være sentralt. Grunnleggende nasjonale funksjoner (GNF) er i loven definert som *«tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser».*[45] I ekomsektoren vil kritisk digital kommunikasjons-infrastruktur være avgjørende for å opprettholde følgende grunnleggende nasjonale funksjoner:
- Evne til å ivareta talekommunikasjonstjenester basert på norsk nummerplan
- Evne til å ivareta tekstbaserte meldingstjenester basert på norsk nummerplan
- Evne til å ivareta grunnleggende internettilgang
- Evne til å ivareta datalagring og prosesseringskapasitet i Norge
- Satellittbasert kommunikasjon

I tillegg til rammeverket som definerer kritikalitet med bakgrunn i nasjonale sikkerhetsinteresser etter sikkerhetsloven, skal utvalget også inkludere infrastruktur som har betydning for samfunnssikkerhet og samfunnskritiske funksjoner. Etter utvalgets oppfatning omfatter dette de følgende to dimensjoner: betydningen av elektronisk kommunikasjon som en samfunnskritisk funksjon i seg selv[46] og andre samfunnskritiske funksjoners avhengighet til elektronisk kommunikasjon.

Det gjeldende rammeverket for vurderinger knyttet til samfunnssikkerhet finnes i Direktoratet for samfunnssikkerhet og beredskap (DSB) sin rapport fra 2016 «Samfunnets kritiske funksjoner».[47] Av rapporten fremgår det at *med kritisk samfunnsfunksjon menes «en funksjon som samfunnet ikke kan klare seg uten i syv døgn eller kortere, uten at dette truer befolkningens sikkerhet og/eller trygghet».* Det er identifisert 14 kritiske samfunnsfunksjoner hvor ekomnett og -tjenester og satellittbaserte tjenester[48] er inkludert.

I det første vedlegget til DSBs rapport fremgår en oversikt over ulike infrastrukturer de identifiserte samfunnsfunksjonene er avhengig av. Angitte infrastrukturer for elektronisk kommunikasjon er «kjernenett, regionalnett, aksessnett og svitsjer». For satellittbaserte tjenester nevnes satellitter og bakkestasjoner. I det andre vedlegget til DSBs rapport redegjøres det for kritiske innsatsfaktorer og her fremkommer det at elektronisk kommunikasjon er «*avgjørende for en rekke samfunnsfunksjoner: helse, redningstjenester, lov og orden, finans, transport osv.»* Videre at: *«De fleste innsatsfaktorene er avhengig av*

[45] Jf. sikkerhetsloven § 1-5, nr. 2

[46] Eksempelvis kritikaliteten av at befolkningen har mulighet for å kunne kommunisere under en krise

[47] https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

[48] Satellittbasert kommunikasjon er en av flere satellittbaserte tjenester

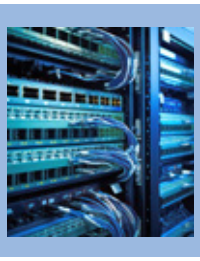
elektrisk energi og fungerende ekomtjenester som slik sett fremstår som enda viktigere i et samfunnsmessig perspektiv enn de øvrige».

I kontekst av nasjonal kontroll kan det være hensiktsmessig å illustrere hvordan ulike kategorier av digital kommunikasjonsinfrastruktur hører til i et «økosystem», jf. figur 5.1.

Figur 5.1 Et økosystem for digital kommunikasjonsinfrastruktur, som viser kategorier av infrastrukturelementer gruppert som passiv infrastruktur, støtteinfrastruktur og tjenesteproduksjonsinfrastruktur. Innenfor alle kategoriene vil det være behov for personellressurser og kompetanse for planlegging og drift.

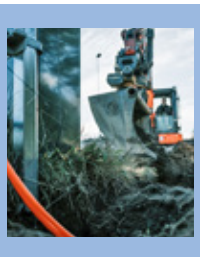
Tjenesteproduksjonsinfrastruktur (aktive elektroniske kommunikasjonsnett)

- Transportnett og bredbåndsnett
- Internett infrastruktur (DNS, ruting, samtrafikk, mv.)
- Mobilnett (mobilkjernenett og basestasjoner)
- VHF/maritim kommunikasjonsinfrastruktur
- Satellittkommunikasjonsinfrastruktur



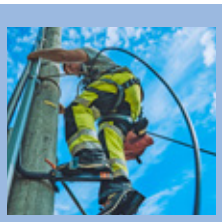
Støtteinfrastruktur (strøm, kjøling, fysisk sikring, støttefunksjoner)

- Datasentre og fortifikatoriske anlegg
- Mobiltårn m/noderom
- Satellitt jordstasjoner
- Klokkeinfrastruktur for nøyaktig tid og synkronisering
- Infrastruktur for nummerportering og opprinnelsesmarkering



Passiv infrastruktur (fysiske innsatsfaktorer uten aktive elementer)

- Eiendom
- Kabelkanaler, utstyrsskap
- Stolper og mastekonstruksjoner
- Fiberkabler (mørk fiber), herunder sjøfiberkabler



Planlegging og drift (personellressurser og kompetanse)

- Design og konfigurasjon
- Overvåking og drift
- Entreprenører – utbygging og feilretting
- Vakt og sikring

I økosystemet som vist i figuren vil det være avhengigheter på kryss og tvers. For eksempel vil produksjon av 5G mobiltjenester i et mobilnett være avhengig av både infrastrukturelementer som transportnettjenester, datasentertjenester, mobiltårn, klokkeinfrastruktur og fysiske fiberkabler, men også tilgang til personellressurser og kompetanse til drift, overvåkning, feilretting osv. Noen enkeltselskaper, som Telenor, forvalter infrastrukturelementer og ressurser i flere deler av dette økosystemet. Andre selskaper forvalter typisk én type infrastruktur eller funksjon, f.eks. fiberselskaper, datasenterselskaper, tårnselskaper og entreprenørselskaper.

Utvalget har i sitt arbeid ikke funnet det hensiktsmessig å utarbeide en komplett liste over infrastrukturelementer som er kritiske, men snarere trukket ut noen kategorier av infrastrukturelementer. Utvalget har derfor tatt utgangspunkt i følgende kategorier:

- Mobilnett
- Bredbåndsnett
- Transportnett
- Fiberkabler som forbinder oss til sokkelen og til utlandet, herunder undersjøiske fiberkabler
- Datasentre
- Satellittkommunikasjonssystemer
- Fortifikatoriske anlegg
- Infrastruktur knyttet kritiske basalfunksjoner som DNS og NRDB[49]
- Samtrafikkpunkter

Kritisk digital kommunikasjonsinfrastruktur vil i utvalgsarbeidet således omfatte enhver struktur som faller inn under en av kategoriene over, og som er, eller snart vil bli, av vesentlig, kritisk eller avgjørende betydning for en eller flere av de overnevnte grunnleggende nasjonale funksjonene, eller for en funksjon som samfunnet ikke kan klare seg uten i syv døgn eller kortere, uten at det truer befolkningens sikkerhet eller trygghet. En struktur som kun har betydning innenfor et mindre geografisk område, faller utenfor mandatet.

5.3 Identifiserte selskaper

Utvalget har ikke tatt mål av seg til å identifisere alle selskaper som eier infrastruktur som omfattes av kategoriene over. Oversikten er derfor ikke uttømmende, men utvalget mener at de identifiserte selskapene utgjør et representativt utvalg som er dekkende for formålet.

Etter avklaring med DFD har utvalget avgrenset sitt arbeid mot offentlig eide tjenestenett og deres infrastrukturer[50] da eierskapsproblemstillinger i mindre grad er direkte relevant når det gjelder disse aktørene. Utvalget har imidlertid hatt dialog og fått innspill til sitt arbeid også fra slike aktører.

I sikkerhetsloven er det et skille mellom virksomheter som råder over kritisk infrastruktur som har henholdsvis *avgjørende* og *vesentlig* betydning for grunnleggende nasjonale funksjoner og nasjonale sikkerhetsinteresser.

Det er den første kategorien som ved vedtak fattet av relevant sektordepartement underlegges sikkerhetslovens bestemmelser.[51] Selskapene dette gjelder innen ekomsektoren er det naturlige utgangspunkt når man skal identifiserte aktører som eier eller råder over kritisk digital kommunikasjonsinfrastruktur. Disse er følgelig inkludert i oversikten under.

[49] DNS og NRDB forklares i kapittel 5.3.

[50] Norsk helsenett, Sikt, Nødnett, Avinor, Bane NOR, Statnett, Cyberforsvaret

[51] Jf. sikkerhetsloven § 1-3 første ledd

Når det gjelder virksomheter som råder over infrastruktur med «vesentlig betydning», finnes det på nåværende tidspunkt ikke informasjon som utvalget kan benytte i sitt arbeid. Det fremgår av sikkerhetsloven[52] at sektordepartementet skal identifisere og holde oversikt over virksomheter med «vesentlig betydning». Dette er ment å være en dynamisk prosess, hvor oversikten oppdateres ved behov. Virksomheter av «vesentlig betydning» er i utgangspunktet ikke underlagt sikkerhetslovens bestemmelser. Sektormyndigheten har imidlertid mulighet til å fatte vedtak om at sikkerhetsloven kapittel 10 om eierskapskontroll, skal gjelde for den enkelte virksomhet. DFD har hittil prioritert arbeidet med å definere sektorspesifikke grunnleggende nasjonale funksjoner, og utpeking og oppfølging knyttet til virksomheter med «avgjørende betydning». Arbeidet med kartlegging av virksomheter med «vesentlig betydning» er derfor ikke igangsatt.

Utvalget har, i tillegg til selskapene som i dag er utpekt etter sikkerhetsloven, inkludert aktører for å sikre tilstrekkelig representativitet og bredde til også å ivareta samfunnssikkerhetsperspektivet. Videre er seleksjonen basert på aktørenes størrelse, betydning innenfor angjeldende infrastrukturkategori og regional betydning.

Utvalget har inkludert alle de tre mobiloperatørene med egne nettverk i Norge.[53] Siden alle disse har organisert sin passive infrastruktur i egne selskaper er også disse selskapene tatt med. I kategorien **mobilnett** er derfor følgende selskap inkludert: Telenor ASA, Telenor Towers Norway AS, Telia Norge AS, Telia Towers Norway AS, Lyse Tele AS[54] og Tårnselskapet AS.

Utvalgte selskaper som eier **bredbåndsinfrastruktur** er: Telenor ASA, Telia Norge AS, Lyse Tele AS, GlobalConnect AS, Eidsiva Bredbånd AS, Eviny Digital AS, NTE Telekom AS, Viken Fiber AS, Bredbåndsfylket AS og Ishavslink AS.

Transportnett er infrastruktur som forbinder ulike regionale og lokale nettverk sammen. I denne kategorien har utvalget tatt utgangspunkt i følgende selskaper: Bredbåndsfylket AS, Bulk Infrastructure Holding AS, Eviny Digital AS, GlobalConnect AS, KystTele AS, Lyse Tele AS, N0r5ke Fibre AS, NTE Telekom AS, Tampnet AS, Telenor ASA, Telia Norge AS, Viken Fiber AS og Stamfiber AS.

Når det gjelder infrastruktur som anvendes til internasjonal samtrafikk har utvalget definert kategorien «**fiberkabler til utlandet**[55], inkludert undersjøiske fiberkabler» Identifiserte selskaper er: Arelion Norway AS, Bredbåndsfylket AS, Bulk Infrastructure Holding AS, GlobalConnect AS, De-Cix Management GmbH, Lumen Technologies Norway AS, Lyse Tele AS, Space Norway AS, Tampnet AS, Telenor ASA og Telia Norge AS.

Datasenter er også en identifisert infrastrukturkategori. En datasentertjeneste er en tjeneste som legger til rette for innplassering, tilkobling og drift av IT – og nettverksutstyr for datalagring, dataprosessering og dataoverføring. Tjenesten omfatter i tillegg fysisk sikkerhet, strøm og kjøling, og kan inkludere andre relaterte tjenester.[56] Når det gjelder

[52] Jf. sikkerhetsloven § 2-1 første ledd, bokstav b

[53] Unntatt mobilnett offshore

[54] Eier merkevaren ice

[55] Fra Fastland-Norge og på norsk sokkel

[56] § 1-5 nr. 37 i ny ekomlov, jf. Prop. 93 LS (2023–2024)

selskaper som eier infrastruktur som anvendes til datasentertjenester har utvalget identifisert: Bulk Infrastructure Holding AS, Eidsiva Bredbånd AS, Green Mountain AS, Lefdal Mine Datacenter AS, Infrastructure Nordics 4 AS (Stack) og Orange Business Digital Norway AS.

Satellittbasert kommunikasjon understøtter kommunikasjon på en rekke områder hvor andre ekomnett ikke har dekning. På et overordnet nivå blir satellittkommunikasjon i Norge brukt til kringkasting og datakommunikasjon. Utvalget har lagt til grunn et representativt utvalg av aktører som eier slik infrastruktur/tilbyr slik konnektivitet. Disse er: Inmarsat Solutions AS, Kongsberg Satellite Services AS, OneWeb Norway AS, Space Norway AS, Space Norway Satcom AS og Starlink Norway AS.

Fortifikatoriske anlegg forstås som et anlegg som i tillegg til naturlig fjelloverdekning eller armert betong (bunker), har beskyttelsestiltak mot CBR-elementer (kjemisk, biologisk og radioaktivt). Slike anlegg benyttes til innplassering og eventuelt samlokalisering av kjerneinfrastruktur for å kunne drifte ekomtjenester også i situasjoner høyt oppe i krisespennet. Det er kun Telenor som har slike anlegg innen sektoren og infrastrukturen eies av Telenor Towers Norway AS.

Norid AS og Nasjonal Referansedatabase AS (NRDB) er identifisert som selskaper som eier infrastruktur knyttet til kategorien «**kritiske basalfunksjoner**».

Norid AS er registerenhet for de norske landkodetoppdomenene[57] og drifter navnetjenesten og registreringstjenesten for .no. Domenenavnsystemet (DNS) knytter IP-adresser til unike domenenavn. Når en bruker forsøker å kontakte en tjeneste på internett (nettsider, e-post mv.) utløser det en rekke oppslag i DNS for å finne den aktuelle IP-adressen. Navnetjenesten som Norid drifter er en nødvendig del av denne DNS-infrastrukturen under .no.

NRDB leverer tekniske fellesløsninger til ekomtilbydere, eksempelvis er NRDB mellomledd i prosessen med å portere kunders telefonnummer over til ny tilbyder ved tilbyderbytter. NRDB leverer også geografisk lokalisering og overføring av abonnementsinformasjon ved anrop til nødetatene (opprinnelsesmarkering). Ved bortfall av NRDB sine tjenester vil man fortsatt kunne ringe og motta samtaler. Man mister imidlertid mulighet for å gjennomføre nummerportering og på kort sikt også automatisk støtte til opprinnelsesmarkering.

Et **samtrafikkpunkt** er et fysisk eller virtuelt knutepunkt i telenettene hvor ulike operatører kobler seg sammen for å utveksle nasjonal og internasjonal trafikk mellom ulike nettverk. Identifiserte selskaper i denne kategorien er: Bulk Infrastructure Holding AS, De-Cix Management GmbH, GlobalConnect AS, Infrastructure Nordics 4 AS (Stack), Lyse Tele AS, Orange Business Digital Norway AS, Telenor ASA, Telia Norge AS og Norwegian Internet Exchange (NIX).

[57] .no, .sj og .bv. Det er kun .no-domenet som er åpent for bruk.

Tabell 5.1 Oversikt over relevante virksomheter kategorisert etter infrastrukturtype

Selskap / infrastruktur	Mobilnett	Bredbåndsinfrastruktur	Transportnett	Fiberkabler til utlandet (inkl. sjøfiber)	Datasenter	Satellittbasert kommunikasjon	Fortifikatoriske anlegg	Kritiske basalfunksjoner	Samtrafikkpunkter
Telenor	X	X	X	X					X
Telenor Towers Norway	X						X		
Telia Norge	X	X	X	X					X
Telia Towers Norway	X								
Lyse Tele	X	X	X	X					X
Tårnselskapet	X								
GlobalConnect		X	X	X					X
Eidsiva bredbånd		X			X				
Eviny Digital		X	X						
NTE Telekom		X	X						
Viken fiber		X	X						
Bredbåndsfylket		X	X	X					
Ishavslink		X							
Bulk Infrastructure Holding			X	X	X				X
Kyst Tele			X						
N0r5ke Fibre			X						
Tampnet			X	X					
Stamfiber			X						
Arelion Norway				X					
De-Cix Management				X					X
Lumen Technologies Norway				X					
Green Mountain					X				
Lefdal Mine Datacenter					X				
Infrastructure Nordics 4 (Stack)					X				X
Orange Business Digital Norway					X				X

Space Norway				X		X			
Space Norway Satcom						X			
Kongsberg Satellite Services						X			
OneWeb Norway						X			
Inmarsat Solutions						X			
Starlink Norway						X			
Norid								X	
NRDB								X	
Norwegian Internet Exchange (IX)									X

5.4 Innspill fra relevante sektormyndigheter

Utvalget har forelagt tilnærmingen beskrevet over for NSM, DSB og Nkom. Utvalget har bedt om synspunkt på om infrastrukturkategoriene og identifiserte virksomheter er dekkende for formålet etter deres syn, eventuelt om de har forslag til endringer.

NSM og DSB mener begge at infrastrukturkategoriene og identifiserte virksomheter virker hensiktsmessig for formålet.

Når det gjelder infrastrukturkategorier påpeker Nkom at utvalget kunne supplert denne listen med tjenester som autentiserer og sikrer transaksjoner, såkalte tillitstjenester. Utvalget mener at dette er viktige tjenester, men at de ligger utenfor rammen av utvalgtes definisjon av kritisk digital kommunikasjonsinfrastruktur. Utvalget omtaler likevel disse tjenestene i kapittel 13.4. Videre påpeker Nkom kritikaliteten knyttet til tidssynkronisering av ekomnett som en sentral funksjon for stabil tjenesteproduksjon. Utvalget ser nærmere på tidssynkronisering i kapittel 11.6, og også i kapittel 13.5.

Nkom har også supplerende forslag til aktører som eier infrastruktur i kategoriene utvalget har lagt til grunn, men sier samtidig at: «*Listen over selskaper ser ut til å omfatte en stor andel av aktører som det vil være naturlig for utvalget å ha dialog med, gitt mandatets formulering. En kan alltids utvide til flere aktører, men Nkom antar at det er trukket en grense ut fra hva som er praktisk mulig å håndtere innenfor utvalgets tidsrammer, samt hva en definerer som digital samfunnskritisk infrastruktur.*»

Utvalget oppfatter på denne bakgrunn at relevante sektormyndigheter i stor grad støtter utvalgtes tilnærming og at de identifiserte selskapene gir tilstrekkelig representativitet, selv om listen ikke er uttømmende.

Utvalget har videre ønsket å klargjøre sektormyndighetenes eventuelle rolle knyttet til å definere og vedlikeholde oversikt over kritisk digital kommunikasjonsinfrastruktur i dag, utover arbeidet med grunnleggende nasjonale funksjoner etter sikkerhetsloven. Utvalget ønsket også synspunkter på om det er behov for at noen har et slikt dedikert ansvar, dersom dette ikke er tilfelle i dag.

På bakgrunn av tilbakemeldingene legger utvalget til grunn at ingen av de relevante sektormyndighetene har et dedikert ansvar for å definere og vedlikeholde en helhetlig oversikt over all kritisk digital kommunikasjonsinfrastruktur i dag. Når det gjelder behovet for dette påpeker DSB at når nye EØS-relevante regelverk som CER[58]- og NIS2[59]-direktivet er implementert i norsk rett, kan dette gi føringer for offentlige myndigheter når det gjelder å definere og vedlikeholde oversikt over kritisk digital kommunikasjonsinfrastruktur.

Nkom påpeker at de som sektormyndighet har bred oversikt over aktørbildet, herunder også viktige aktører som ikke er utpekt etter sikkerhetsloven. De beskriver et sett med tilsynsoppgaver og regelverk som til sammen gjør at tilsynet mener å ha tilstrekkelig oversikt og informasjonstilgang knyttet til kritisk digital kommunikasjonsinfrastruktur. Samtidig påpeker de at en sammenstilling av eksisterende informasjon i et eventuelt register vil gi en høyere informasjonsrisiko, og også merarbeid med vedlikehold av informasjonen. Nkom mener derfor at det ikke er hensiktsmessig å etablere en egen samlet oversikt over kritisk infrastruktur, utover det som nå blir registrert.

Ingen av de relevante sektormyndighetene har i dag et dedikert ansvar for å definere og vedlikeholde helhetlig oversikt over kritisk digital kommunikasjonsinfrastruktur og selskapene som eier denne. Utvalget oppfatter at relevant informasjon i stor grad allerede finnes og fortløpende blir generert gjennom Nkoms gjennomføring av tilsynets samfunnsoppdrag. Eksisterende informasjon og oppdatering av denne er imidlertid ikke strukturert slik at den er egnet til å gi en slik helhetlig oversikt. Utvalget kommer tilbake til behovet for en slik oversikt i kapittel 11.

[58] Direktiv (EU) 2022/2557 om kritiske enheters motstandsdyktighet (CER-direktivet)

[59] Direktiv (EU) 2022/2555 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer

”

Kapittel 6 gir en overordnet oversikt over dagens eierforhold og eierstrukturer i selskaper som eier eller kontrollerer kritisk digital kommunikasjonsinfrastruktur i Norge, eller selskaper som er av avgjørende betydning for utbygging, vedlikehold eller drift av infrastrukturen.

Foto: Anders Martinsen (Nkom)

06

Dagens eierstrukturer

6.1 Om kapittelet

Kapittel 6 gir en overordnet oversikt over dagens eierforhold og eierstrukturer i selskaper som eier eller kontrollerer kritisk digital kommunikasjonsinfrastruktur i Norge, eller selskaper som er av avgjørende betydning for utbygging, vedlikehold eller drift av infrastrukturen.

Listen av kartlagte selskaper er utarbeidet på bakgrunn av utvalgets kjennskap til ekomsektoren og innspill fra Nkom. Dette er de samme selskapene utvalget har identifisert og omtalt i kapittel 5 over. Utvelgelse av underleverandører er basert på tilbakemeldinger utvalget mottok i forbindelse med en spørreundersøkelse utvalget gjennomførte våren 2024. Her ble aktørene bedt om å navngi noen sentrale leverandører i ekomsektoren, hvorpå utvalget har plukket ut noen som er gjenstand for kartlegging. Utvalget ga et oppdrag til Menon Economics (Menon) om å lage en oversikt over eierstrukturer og eierforhold i selskaper som utvalget har identifisert.

Informasjonen som gjengis i dette kapittelet er i hovedsak et konsentrat av informasjon Menon har skaffet til veie for utvalget. Kartleggingen gir et øyeblikksbilde av eierforhold og eierstrukturer i disse virksomhetene og kan brukes til å identifisere potensielle problemområder knyttet til utenlandskdominerte eierforhold.

6.2 Status for nasjonal kontroll gjennom eierskap

6.2.1 Ulike eierformer og typer eiere

Menons kartlegging viser at det er en betydelig variasjon i selskapene som eier og forvalter kritisk digital kommunikasjonsinfrastruktur i Norge i dag. Selskapene som undersøkes er alt fra mindre lokale aktører til store internasjonale konsern. Det er eiere av satellitter som Kongsberg Satellite Services AS, datasentre som Green Mountain AS, og virksomheter som Telenor ASA som omsetter for titalls milliarder kroner hvert år. Mindre virksomheter som KystTele AS som omsetter for under 20 millioner kroner er også omfattet av undersøkelsen. Samtlige kartlagte selskaper er aksjeselskap, med unntak av Telenor ASA som er allmennaksjeselskap og De-Cix Management GmbH, som er et tysk selskap som tilsvarer den norske selskapsformen aksjeselskap, og som i Norge er registrert som et NUF.

Majoriteten av selskapene har enten norske offentlige eiere som stat, fylke og kommune (for eksempel Lyse, Telenor) eller utenlandske eiere (for eksempel Telia, GlobalConnect). Omfanget av norsk personlig eierskap og øvrige småaksjonærer (aksjonærer med mindre enn 5 prosent eierskap), er begrenset.[60]

6.2.2 Kartlagte selskaper

Menon har i sin analyse kartlagt eierskapet i totalt 50 selskaper som eier kritisk digital kommunikasjonsinfrastruktur eller som er viktige underleverandører til disse. Underleverandører inkluderer både entreprenører og leverandører som er av avgjørende betydning for utbygging, drift og vedlikehold av infrastrukturen, samt enkelte viktige utstyrsleverandører.

De to tabellene nedenfor gir en oversikt over selskapene Menon har kartlagt, med en kort beskrivelse av den enkelte virksomhet. Den første tabellen under, tabell 6.1, gir oversikt over infrastruktureiere, mens tabell 6.2 inneholder informasjon om viktige underleverandører for kritisk digital kommunikasjonsinfrastruktur. For underleverandører fremgår det i tillegg hvilke selskaper som har vært gjenstand for enten en begrenset kartlegging av eierskapet (kun norske aksjonærregistre) og de selskapene der man har kartlagt eierskap så langt som mulig for å avdekke ultimat eier (på samme måte for infrastruktureierne).

Selskapsbeskrivelsene i begge tabellene er offentlig tilgjengelig og hentet fra Brønnøysundregistrene og lignende.

[60] Personlig eierskap omfatter både familieeide bedrifter der flere fra familien eier sammen, enkeltpersoners bedrifter og bedrifter med flere private eiere som ikke er i slekt.

Tabell 6.1 Oversikt over eiere og forvaltere av kritisk digital infrastruktur

Selskap	Beskrivelse
Arelion Norway AS	Selskapet etablerer og driver telenett, både jordbundne og eterbaserte. Selskapet tilbyr også transmisjonstjenester og andre telekommunikasjonstjenester. Kilde: Brønnøysundregistrene
Bredbåndsfylket AS	Selskapet eier og drifter nettverk for kommunene i Troms og Finnmark, og yter tilknyttede tjenester. Kilde: Bredbåndsfylket
Bulk Infrastructure Holding AS	Selskapet etablerer, utvikler og drifter datasentre, fibernettverk og industrirelatert eiendom. Kilde: Bulk Infrastructure
De-Cix Management GmbH	Selskapet er en internasjonal plattform som tilbyr operatør- og datasenternøytrale internett-utvekslinger. Kilde: De-Cix
Eidsiva Bredbånd AS	Selskapet bygger, selger og drifter bredbåndstjenester på Østlandet. Kilde: Eidsiva
Eviny Digital AS	Selskapets formål er å etablere og drifte bredbåndsinfrastruktur, samt drive virksomhet knyttet til dette. Kilde: Brønnøysundregistrene
Exa Infrastructure Norge AS	Exa Infrastructure er et internasjonalt konsern som forvalter digitale infrastrukturtjenester, inkludert fiberoptiske nettverk som støtter kommunikasjon på tvers av kontinenter. Selskapet forvalter blant annet infrastruktur som benyttes av De-Cix i Norge. Kilde: Exa Infrastructure / De-Cix
GlobalConnect AS	Selskapet eier og forvalter fibernettverk og tilbyr tilknyttede kommunikasjonsløsninger. Kilde: GlobalConnect
Green Mountain AS	Selskapet driver med datasentervirksomhet og relaterte aktiviteter. Kilde: Brønnøysundregistrene
Infrastructure Nordics 4 AS	Selskapet er morselskapet til de norske datasentrene som driftes av Stack Infrastructure. Kilde: Proff.no
Inmarsat Solutions AS	Selskapet tilbyr informasjons- og kommunikasjonsløsninger til skipsfartøy. Kilde: Brønnøysundregistrene
Ishavslink AS	Selskapet bygger ut, eier og drifter bredbåndsinfrastruktur i Finnmark, og driver virksomhet med naturlig tilknytning til dette. Kilde: Brønnøysundregistrene / Ishavslink
Kongsberg Satellite Services AS	Selskapet tilbyr bakkestasjonstjenester og infrastruktur for satellitter. Kilde: KSAT
KystTele AS	Selskapet eier, bygger og driver bredbåndsinfrastruktur og tilbyr tilknyttede tjenester. Kilde: Kysttele
Lefdal Mine Datacenter AS	Selskapet driver med datasentervirksomhet og relaterte aktiviteter. Kilde: Lefdal Mine
Lumen Technologies Norway AS	Selskapet tilbyr telekommunikasjonsløsninger og tilknyttede tjenester. Kilde: Brønnøysundregistrene
Lyse Tele AS	Selskapet representerer Lyse-konsernets televirksomhet. Selskapet har ansvar for utbygging av mobilnett, 5G og fiber, samt tilknyttede tjenester. Kilde: Lyse
N0r5ke Fibre AS	Selskapet investerer i, eier og leier ut optiske fiberkabler både nasjonalt og internasjonalt, og driver også investeringsvirksomhet ved å investere i og yte lån til selskaper innen disse virksomhetsområdene. Kilde: Brønnøysundregistrene

Nasjonal Referansedatabase AS	Selskapet driver med utvikling og drift av en nasjonal referansedatabase for porterte nummer, samt effektiviserende fellesløsninger for tilbydere og andre kunder innen eller med tilknytning til ekomnæringen. Kilde: Brønnøysundregistrene
Norid AS	Selskapet drifter registeret for norske domenenavn, og har ansvaret for toppdomenene .no, .sj, og .bv. Selskapet behandler søknader om abonnement på domenenavn. Kilde: Norid
NTE Telekom AS	Selskapet driver utbygging av fiberbredbånd og salg av fiberkapasitet og -innhold. Kilde: NTE
OneWeb Norway AS	Selskapet leverer satellittbaserte kommunikasjonstjenester. Kilde: OneWeb
Orange Business Digital Norway AS	Selskapet tilbyr digitale tjenester og tilknyttede konsulenttjenester til bedriftskunder. Kilde: Orange Business
Space Norway AS	Selskapet forvalter og videreutvikler sikkerhetskritisk og kostnadseffektiv romrelatert infrastruktur for å dekke viktige norske samfunnsbehov. Kilde: Brønnøysundregistrene
Space Norway Satcom AS	Selskapet driver med satellittbasert kommunikasjonsvirksomhet både i Norge og utlandet. Kilde: *Brønnøysundregistrene*
Stamfiber AS	Selskapet driver utleie av disposisjonsrett til mørk fiber og annet som står i naturlig forbindelse med dette. Kilde: Brønnøysundregistrene
Starlink Norway AS	Selskapet driver med satellittvirksomhet og tilknyttede aktiviteter. Kilde: Brønnøysundregistrene
Tampnet AS	Selskapet eier, opererer og utvikler kommunikasjonsnettverk, og tilbyr kommersielle kommunikasjonstjenester basert på sitt nettverk. Kilde: Brønnøysundregistrene
Telenor ASA	Selskapet er morselskapet i Telenor-konsernet, som tilbyr et bredt spekter av tjenester telekommunikasjonsvirksomhet og tilknyttede områder. Kilde: Brønnøysundregistrene / Telenor
Telenor Fiber AS	Selskapet driver med utbygging og utleie av fiberinfrastruktur og tilhørende virksomhet, men det skal ikke ha tilgang til informasjon om sluttbrukere eller annen skjermingsverdig informasjon om infrastrukturen. Kilde: Brønnøysundregistrene
Telenor Towers Norway AS	Selskapet forvalter og leier ut plass i master, tårn og annen passiv infrastruktur. Kilde: Telenor Towers
Telia Norge AS	Selskapet driver med elektronisk kommunikasjonsvirksomhet, inkludert utbygging, drift og vedlikehold av landsdekkende data-, tele- og TV-distribusjonsnett, samt produksjon og levering av lyd, bilder og elektroniske signaler, inkludert digital TV, og innholdsproduksjon for distribusjon i disse nettverkene, i tillegg til annen relatert virksomhet. Kilde: Brønnøysundregistrene
Telia Towers Norway AS	Selskapet driver med drift av og tilbyr plass i master, tårn og lignende strukturer for trådløs mobilteknologi. Kilde: Brønnøysundregistrene / Telia Towers
Tårnselskapet AS	Selskapet eier, drifter og leier ut plass i tårn og annen infrastruktur til mobiloperatører og andre selskaper som trenger tilgang til høydemaster for å bygge ut sine nettverk og tjenester. Selskapet er en del av Lyse-konsernet. Kilde: Lyse
Viken Fiber AS	Selskapet bygger og drifter fibernett på Østlandet. Kilde: Viken Fiber

Kilde: Menon Economics (2024), tabell 3-2.

Tabell 6.2 Oversikt over leverandører til kritisk digital infrastruktur

Selskap	Beskrivelse	Type kartlegging
Caverion Norge AS	Selskapet er en teknisk totalleverandør for bygg og industri, med fokus på smarte og bærekraftige løsninger. Kilde: Caverion	Fullstendig
Cisco Systems Norway AS	Selskapet tilbyr produkter og tjenester knyttet til datamaskiner (hardware og software). Kilde: Brønnøysundregistrene	Begrenset
Eltel Networks AS	Selskapet driver med bygg, drift og vedlikehold av kritisk infrastruktur innen energi og telekommunikasjon. Kilde: Eltel	Fullstendig
Ericsson AS	Selskapet leverer nettverksutstyr og -tjenester. Kilde: Ericsson	Begrenset
Huawei Technologies Norway AS	Selskapet leverer utstyr, løsninger og tjenester innen IT og telekommunikasjon. Kilde: Brønnøysundregistrene	Begrenset
Juniper Networks Norway AS	Selskapet driver med salg, markedsføring og tjenester innen IT, data og telekommunikasjon. Kilde: Brønnøysundregistrene	Begrenset
Netel AS	Selskapet bygger og vedlikeholder infrastruktur for tele- og datakommunikasjon. Kilde: Netel	Fullstendig
Nexans Norway AS	Selskapet driver med utvikling, produksjon og markedsføring av kabler og kablingssystemer, inkludert kraft- og telekabler. Kilde: Nexans	Fullstendig
Nokia Solutions and Networks Norge AS	Selskapet driver med telekommunikasjon og elektronisk industri, inkludert implementering av systemer og tjenester som nettverksplanlegging, vedlikehold, brukerstøtte og konsulenttjenester. Kilde: Brønnøysundregistrene	Begrenset
OneCo Networks AS	Selskapet driver med svakstrøm- og sterkstrøminstallasjon, prosjektering, samt forvaltning av andeler i selskaper med lignende formål. Kilde: Brønnøysundregistrene	Fullstendig
Palo Alto Networks (Norway) AS	Selskapet er en del av det internasjonale konsernet Palo Alto Networks, som tilbyr cybersikkerhetsprodukter og tilhørende tjenester. Kilde: Brønnøysundregistrene / Palo Alto Networks	Begrenset
Prysmian Group Norge AS	Selskapet utvikler og produserer kabler til en rekke segmenter, inkludert datakabler, telekom og fiber. Kilde: Prysmian	Fullstendig
Seaworks AS	Selskapet driver med bulktransport og sjøkabeltjenester. Kilde: Seaworks	Fullstendig
Seaworks Management AS	Selskapet forvalter personell hos Seaworks AS, som driver med bulktransport og sjøkabeltjenester. Kilde: Seaworks	Fullstendig
Site Service AS	Selskapet installerer, drifter og vedlikeholder fiber-, elektro-, tele- og kommunikasjonsnettverk. Kilde: Site Service	Fullstendig

Kilde: Menon Economics (2024), tabell 3-3.

6.2.3 Metode for kartlegging og eierkategorier

Menon har benyttet egne databaser (eierskapsdatabase og regnskapsdatabase), men også internasjonale kilder som Orbis, andre nasjonale eierskapsdatabaser, og årsrapporter mv. En mer utfyllende beskrivelse av metode og kilder fremgår av kapittel 2, 4 og Vedlegg A i Menons rapport.

Menon har kartlagt selskapenes *ultimate norske eierskap*, dvs. eierskap som kan spores tilbake til en ultimat norsk eier, eller til første utenlandske eierledd. I tillegg har de gjennomført en tilnærmet fullstendig kartlegging også av det utenlandske eierskapet i alle selskap der dette er relevant. I tekstboksen nedenfor forklares tre av begrepene som er benyttet i Menons rapport:

Boks 6.1

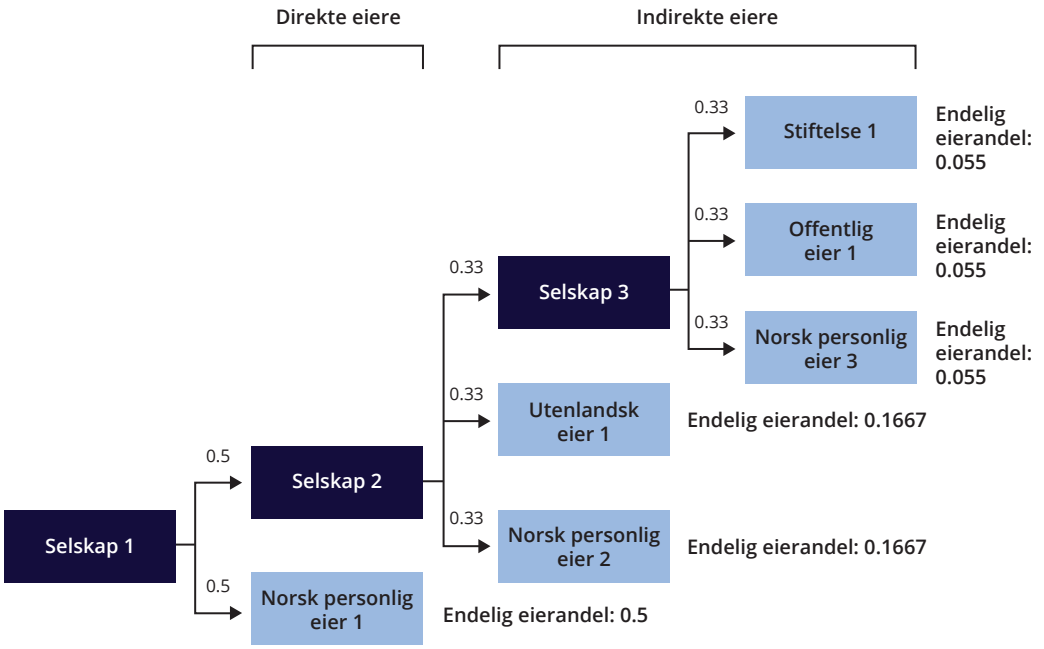
Definisjoner av viktige begreper benyttet i Menon (2024).

Effektivt eierskap: Det effektive eierskapet er den reelle eierandelen til en eier, som inkluderer både direkte og indirekte eierskap.

Ultimat eier: Ultimate eiere er de personene, stiftelsene/selveiende virksomheter eller det offentlige som er øverst i et eierskapshierarki og har en eierandel i virksomheten.

I figuren under gis en illustrasjon av hvordan eierdatabasen til Menon definerer ultimat eier.

Figur 6.1 Illustrasjon av hvordan eierskapsdatabasen definerer ultimat eier. Blå bokser indikerer ultimat eier



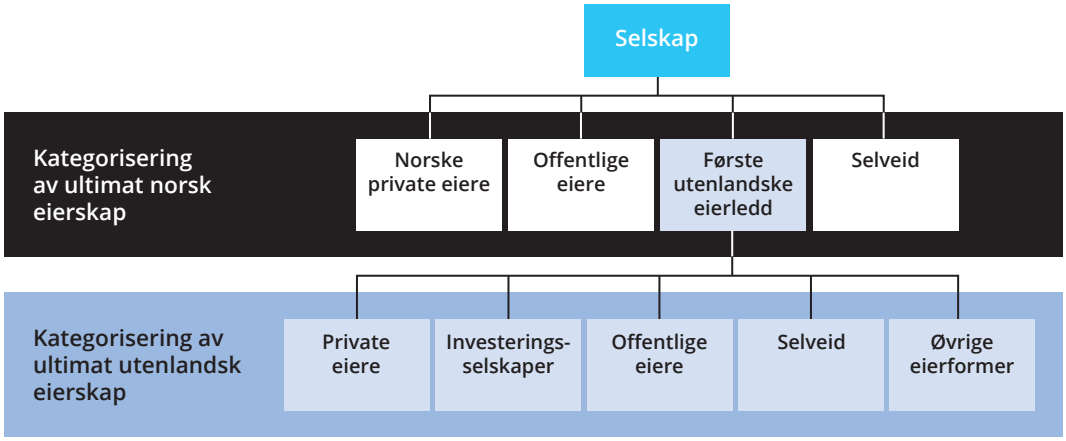
Kilde: Menon Economics (2024), figur V-1.

De aller fleste selskapene Menon har gjennomgått har transparente eierforhold der eierskap kan spores direkte tilbake til norsk eierskap eller kjent utenlandsk offentlig eller privat eierskap, eller børsnoterte selskaper der eierskapet er spredt på svært mange mindre aksjonærer.

Enkelte selskap har mer komplekse eierstrukturer som gjør eierforholdene vanskeligere å avdekke. Dette gjelder særlig eierskap som spores tilbake til land der det ikke lenger er mulig å hente ut eierskapsdata, eller til investeringsselskap uten kjente investorer.

En illustrasjon av ulike kategorier eierskap som er avdekket ved kartleggingen er inntatt nedenfor.

Figur 6.2 Illustrasjon av kategorisering av norsk og utenlandsk eierskap



Kilde: Menon Economics (2024), figur 4-1.

6.2.4 Usikkerhet

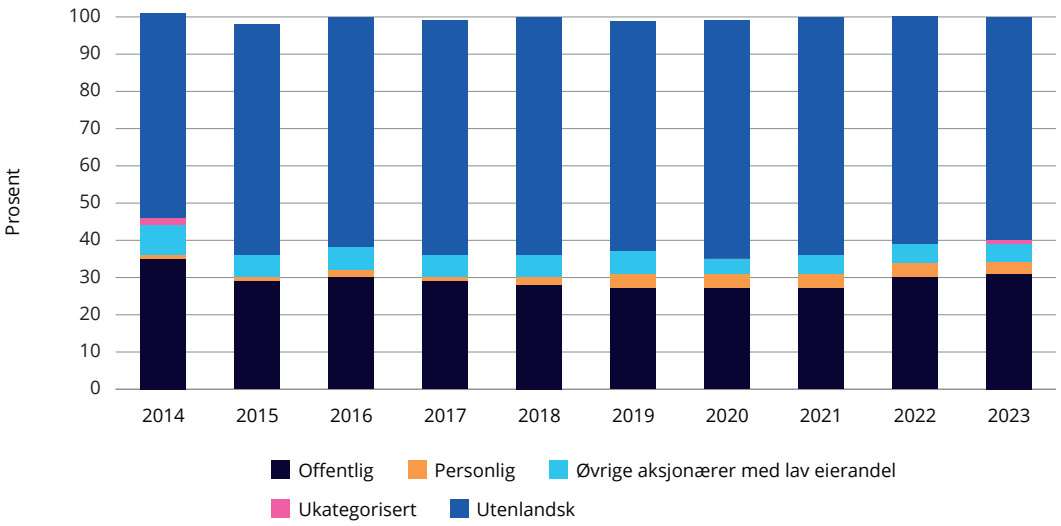
Menon viser til at eierskaps- og selskapsinformasjon i all hovedsak er basert på selskapers egenrapportering til myndigheter og offentligheten. Slik egenrapportering medfører en viss risiko for feilkilder, særlig av to årsaker:

1. *Utdatert informasjon*: Informasjonen var korrekt ved registrering, men det har senere blitt gjort endringer som ikke er fanget opp. Dette kan eksempelvis skyldes manglende innmeldingsrutiner hos selskapet, eller at enkelte nasjonale registre ikke krever løpende oppdateringer.
2. *Feilinformasjon*: Informasjonen er nylig oppdatert, men ukorrekt. Dette kan både være ubevisste misforståelser av regelverk, og bevisste handlinger for f.eks. å skjule reelle rettighetshavere. Her kan det også finnes mer komplekse tilfeller hvor informasjonen på papiret er korrekt, men hvor det kan virke som andre personer eller enheter utøver makt over de registrerte rettighetshaverne.

I tillegg er dette kun et øyeblikksbilde av hvordan eierskapet ser ut akkurat nå. Det kan ha blitt gjort vesentlige endringer i eierskapet til enkeltselskaper på kort tid.

På tross av dette viser likevel Menons analyse på et overordnet nivå at den historiske fordeling av eierskapet i alle selskapene som har vært omfattet av kartleggingen (vektet etter omsetning) har vært ganske stabil i perioden 2014-2023:

Figur 6.3 Historisk fordeling av ultimat eierskap i alle selskapene som kartlegges, vektet etter omsetning



Kilde: Menon Economics (2024), figur 4-3.

6.2.5 Eierskap i selskaper som eier/råder over kritisk digital kommunikasjonsinfrastruktur

Menons kartlegging viser at utenlandsk eierskap dominerer, og er mer utbredt i kritisk digital kommunikasjonsinfrastruktur enn i norsk næringsliv generelt. I følge Menon var 35 prosent av næringslivet utenlandsk eid i 2021, mens tilsvarende eierandel for kritisk digital kommunikasjonsinfrastruktur var på om lag 64 prosent, målt i omsetning.[61]

Undersøkelsene viser også at offentlig eierskap er langt mer utbredt i kritisk digital infrastruktur, sammenlignet med eierskapet i øvrig norsk næringsliv. I følge Menon viser analysen at det offentlige (norske og utenlandske myndigheter) eier nesten halvparten av selskapene kartlagt her, men det offentlige eide 22 prosent av norsk næringsliv i 2021 (omfatter kun eierskapet til den norske stat).[62]

Menon viser til at en naturlig forklaring på at offentlig eierskap er utbredt, er at det er svært kapitalkrevende å bygge ut infrastrukturen, samtidig som det er samfunnskritisk. Av samme årsaker er privat eierskap mindre utbredt for disse selskapene, sammenlignet med næringslivet som helhet.

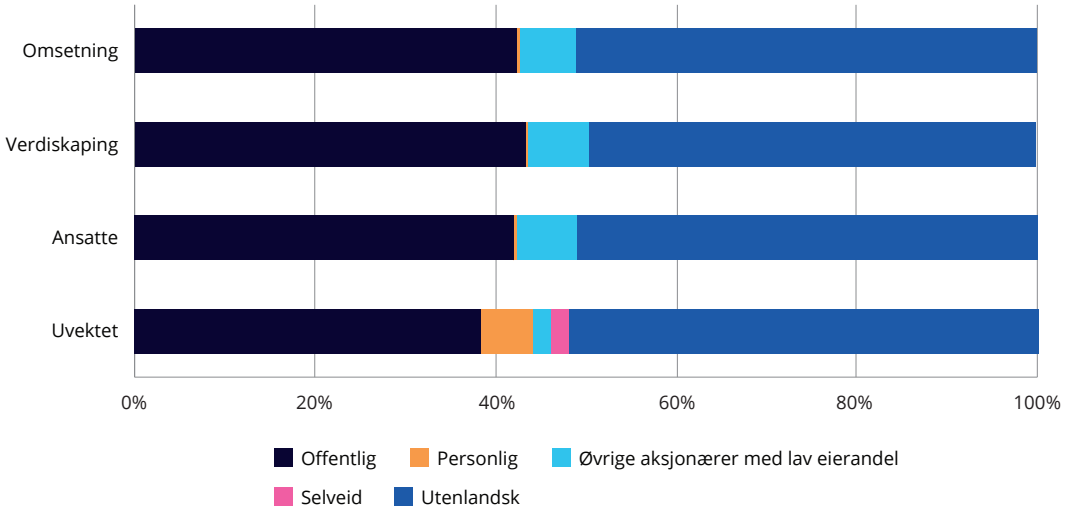
[61] Beregningen av utenlandsk eierskap basert på omsetning er utført av Menon med utgangspunkt i datasettet som ligger til grunn for rapporten Privat eierskap i Norge i 2021. Beregningen var opprinnelig ikke inntatt i Menon Economics (2024).

[62] Menon Economics (2024). Privat eierskap i Norge 2021.

Utvalget vil her peke på at utbredt statlig eierskap også må sees i sammenheng med at det tidligere var staten selv som leverte teletjenester, og at de store selskapene har sitt opphav i at denne statlige virksomheten ble omdannet til kommersielle selskaper da markedene ble liberalisert. I tillegg har flere av selskapene sitt utspring i lokale kraftselskaper, der man så synergier mellom utbygging av kraftnett og kommunikasjonsinfrastruktur.

Figuren nedenfor angir en overordnet fordeling av eierskapet basert på ulike vektinger.

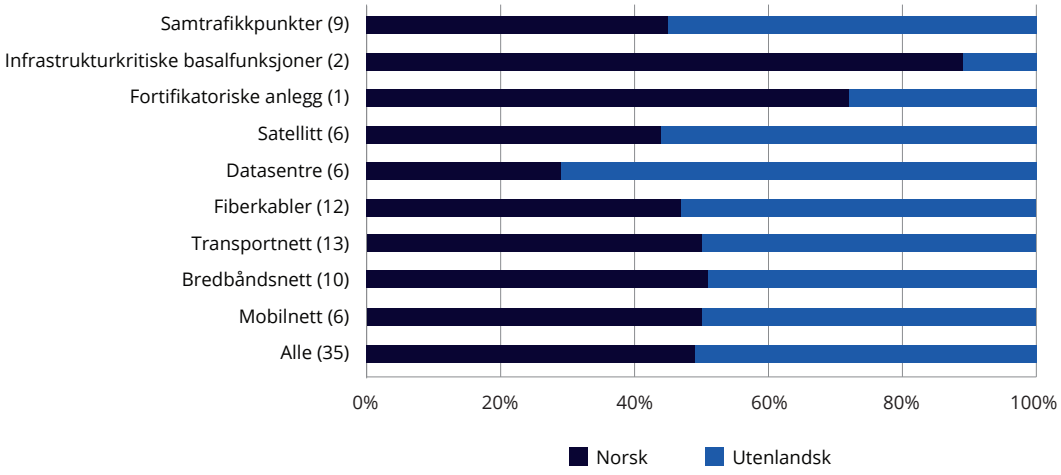
Figur 6.4 Fordeling av eierskap blant eiere og forvaltere, etter vekting



Kilde: Menon Economics (2024), figur 4-4.

Menon har videre analysert fordelingen mellom norsk og utenlandsk eierskap innenfor de ulike infrastrukturkategoriene utvalget har basert arbeidet sitt på. Som vist i figur 6.5 under er fordelingen av eierskap ganske lik på tvers av ulike eierskapskategorier. Unntakene er datasentre som i større grad har utenlandsk eierskap, og i motsatt ende fortifikatoriske anlegg (eid av Telenor Towers) og infrastrukturkritiske basalfunksjoner (Norid og NRDB). Oversikt over de hvilke selskaper som inngår i de ulike infrastrukturkategoriene er inntatt på side 21-22 i Menon (2024).

Figur 6.5 Fordeling mellom norsk og utenlandsk ultimat eierskap innenfor ulike infrastrukturkategorier, vektet etter omsetning. Antall selskaper i parentes. Kun eiere og forvaltere.

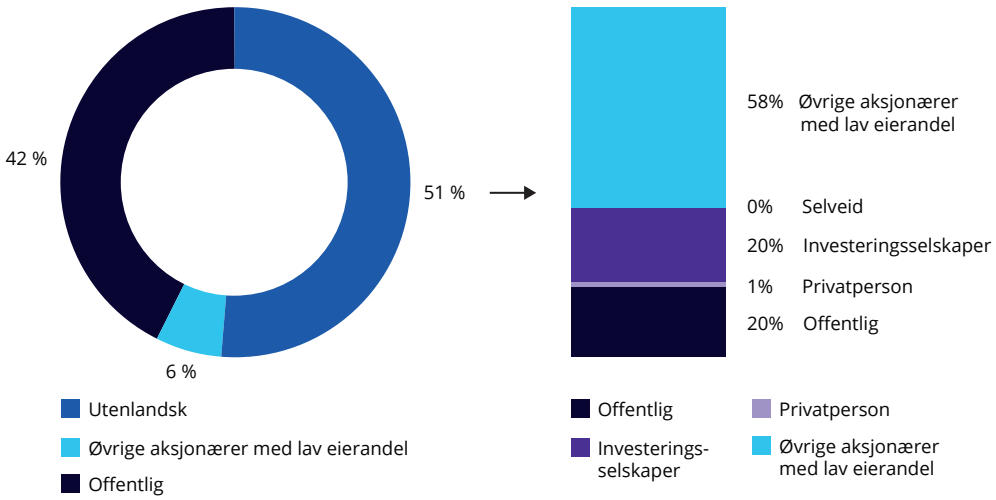


Kilde: Menon Economics (2024), figur 4-6.

Kartleggingen viser også at en betydelig del av eierskapet består av småaksjonærer uten vesentlig innflytelse. Dette gjelder særlig Telenor ASA og Telia AS. Telenor ASA er børsnotert og Telia AS er heleid av svenske børsnoterte Telia AB. En betydelig andel av begge selskapene eies av aksjonærer med mindre enn to prosent eierandel.

På overordnet nivå for selskapene som inngår i analysen, viser funnene at majoriteten av det utenlandske eierskapet består av aksjonærer med små eierandeler, her vist ved figuren under.

Figur 6.6 Fordeling av ultimat utenlandsk eierskap blant eiere og forvaltere, vektet etter omsetning

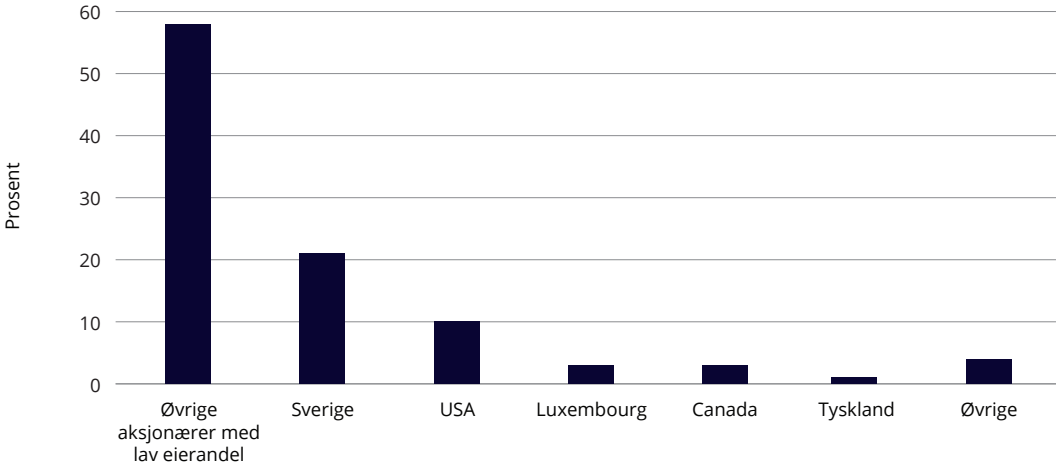


Kilde: Menon Economics (2024), figur 4-5.

Fordeling utenlandsk eierskap, Norden, EØS, NATO og andre

Menon har sporet utenlandsk eierskap så langt det har latt seg gjøre. Som nevnt, består majoriteten av det utenlandske eierskapet av aksjonærer med små eierandeler som ikke har blitt videre kartlagt. Dette medfører at det utenlandske eierskapet i denne gruppen ikke kan knyttes til ett enkelt land.

Figur 6.7 Geografisk fordeling av utenlandsk ultimat eierskap blant eiere og forvaltere, vektet etter omsetning.

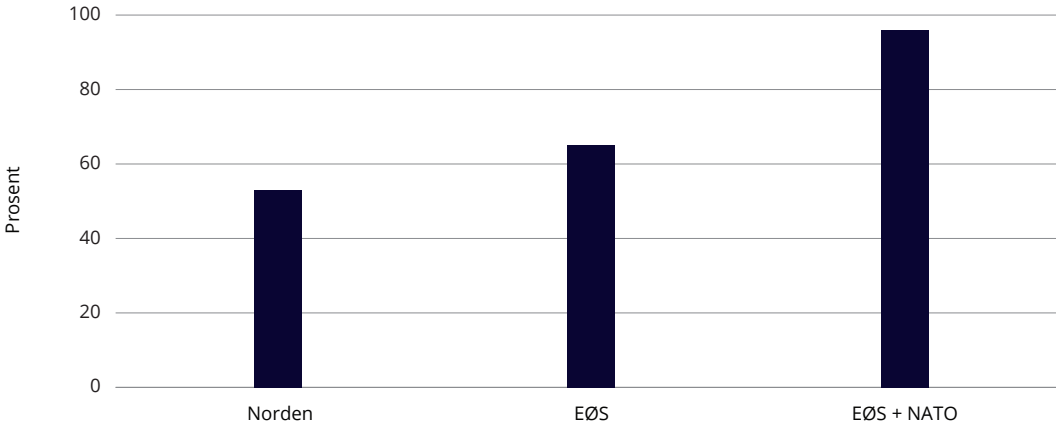


Kilde Menon Economics (2024), figur 4-7.

Som det fremgår av figuren så peker Sverige seg ut som det fremste eierlandet blant ultimate utenlandske eiere, etterfulgt av USA og Luxembourg. Det er likevel viktig å understreke at det kan finnes andre aktører i andre land selv om dette er der eierskapskjeden Menon har kartlagt stopper. Eksempelvis er alt eierskapet registrert i Luxembourg i stor grad knyttet til fond forvaltet av EQT (en av Europas største fondsforvaltere) – som igjen er eid av et bredt sett av investorer med små effektive eierandeler. I slike tilfeller har det ifølge Menon ikke vært hensiktsmessig å gå videre bakover i eierkjeden fordi de fleste investorene har små eierandeler i disse fondene, og eierkjeden stopper derfor i Luxembourg i Menons data.

For å få et bedre overblikk over hvordan eierskapet fordeler seg på ulike regioner, har Menon også gruppert utenlandsk eierskap etter hvorvidt er en del av Norden, EØS eller NATO.

Figur 6.8 Regionvis fordeling av kjent ultimat utenlandsk eierskap blant eiere og forvaltere, vektet etter omsetning



Kilde: Menon Economics (2024), figur 4-8.

Oversikten viser at majoriteten av det utenlandske eierskapet ligger i Norden. Til sammen ligger noe mer av eierskapet i EØS, og tilnærmet alt ultimat eierskap kan spores tilbake til et NATO-land. Det er kun en andel på fire prosent av den samlede omsetningen i selskapene som eies utenfor disse landene. Blant disse er eierskap fra Israel størst, med én prosent effektivt eierskap i selskapene som eiere eller kontrollerer kritisk digital kommunikasjonsinfrastruktur.

Når det gjelder eierskapsinformasjon ned på selskapsnivå så vises det til tabell 4-1 i Menons rapport der det gis en kort omtale av eierskapet. Et utvalg av informasjonen er likevel gjengitt under for *enkelte selskaper* innenfor et utvalg infrastrukturkategorier.

Tabell 6.3 Beskrivelse av eierskap i et utvalg av de kartlagte selskaper

Selskap	Beskrivelse
Bulk Infrastructure Holding AS	Eierskapet er hovedsakelig fordelt mellom styreleder Peter Nærbø og investeringsselskapet BGO. Utover dette finner vi flere mindre aksjonærer, inkludert John Fredriksen og ansatte.
Lefdal Mine Datacenter AS	Majoritetseid (2/3) av Ameriprise Financial Inc., som igjen spores til mindre eierandeler hos investeringsfond fra Vanguard og BlackRock, samt en rekke småaksjonærer med < 3 prosent eierskap. Den resterende tredjedelen eies av tyske stiftelser.
Green Mountain AS	Heleid av Azrieli Group, som igjen er majoritetseid av den israelske Azrieli-familien.
Inmarsat Solutions AS	Eies av Viasat. Største ultimate eiere er BlackRock og The Baupost Group (investeringsselskap), men ingen har mer enn 11 prosent i ultimat eierskap.
Space Norway AS	Heleid av Nærings- og fiskeridepartementet
Starlink Norway AS	Majoritetseid av The Elon Musk Trust. Utover dette ligger det ultimate eierskapet hos en rekke investeringsfond, men fordelingen mellom disse er svært usikker.
GlobalConnect AS	Heleid av ulike EQT-fond, som kan spores tilbake til svært mange mindre aksjonærer
Telenor ASA	Majoritetseid av Nærings- og fiskeridepartementet. Utover dette er de største ultimate eierskapene i ulike norske og internasjonale investeringsselskap, men ingen har mer enn fem prosent eierskap.
Telia Norge AS	Største ultimate eier er svenske myndigheter. Utover dette er de største ultimate eierskapene i en rekke investeringsselskap, men ingen har mer enn fire prosent eierskap.
Telia Towers Norway AS	Eies 51 prosent av Telia Company AB, som gir svenske myndigheter en ultimat eierandel på 21 prosent. De resterende 49 prosentene fordeles mellom investeringsselskapene Brookfield (Canada) og Alecta (Sverige)
Lyse Tele AS	Heleid av norske kommuner
Eidsiva Bredbånd AS	Heleid av norske kommuner og fylkeskommuner, med Oslo kommune og Innlandet fylkeskommune som største aksjonærer.

Kilde: Menon Economics (2024).

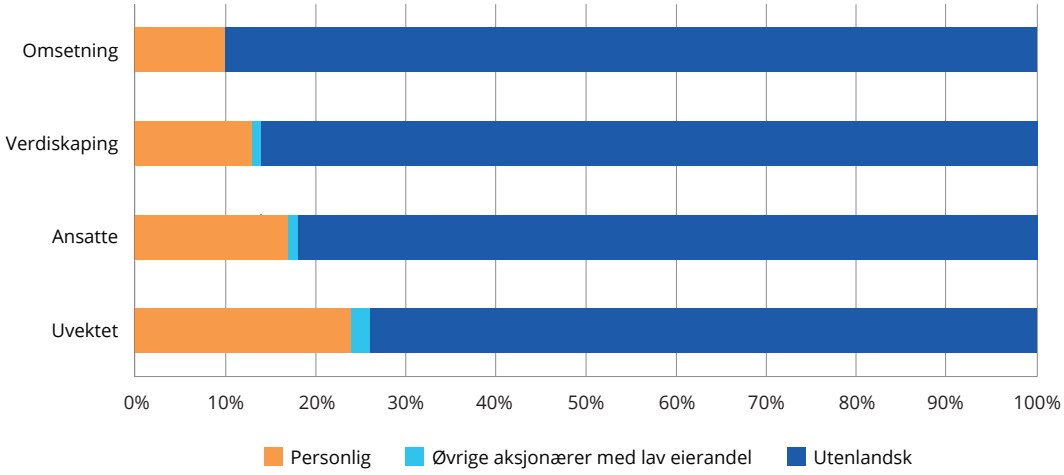
6.2.6 Eierskap for underleverandører som er avgjørende for utbygging, drift og vedlikehold av infrastrukturen

Som det fremgår av tabell 6.2 over, foretok Menon en kartlegging av i alt 15 viktige underleverandører til eiere av kritisk digital kommunikasjonsinfrastruktur. Underleverandørene ble delt inn i to kategorier der Menon for den ene kategorien (i rapporten omtalt som kategori 2A) skulle gjennomføre en full kartlegging på lik linje som for identifiserte infrastruktureiere. For den øvrige delen av underleverandørene (i rapporten omtalt som kategori 2B) foretok Menon en kartlegging begrenset til eierskap i norske aksjonærregistre.

Blant funnene Menon trekker frem fra den generelle kartleggingen av underleverandører (kategori 2A+2B) er at underleverandørene har betydelig mindre offentlig eierskap enn selskapene som eier eller kontrollerer kritisk digital kommunikasjonsinfrastruktur, og heller en større andel personlig og utenlandsk eierskap.

Fordelingen av eierskap varierer noe mer etter hvordan selskapene vektes mot hverandre, men dette anser Menon som naturlig ettersom denne kategorien omfatter et mindre antall selskaper. Fordeling av eierskap er gjengitt i figuren under.

Figur 6.9 Fordeling av eierskap blant leverandører, etter vekting

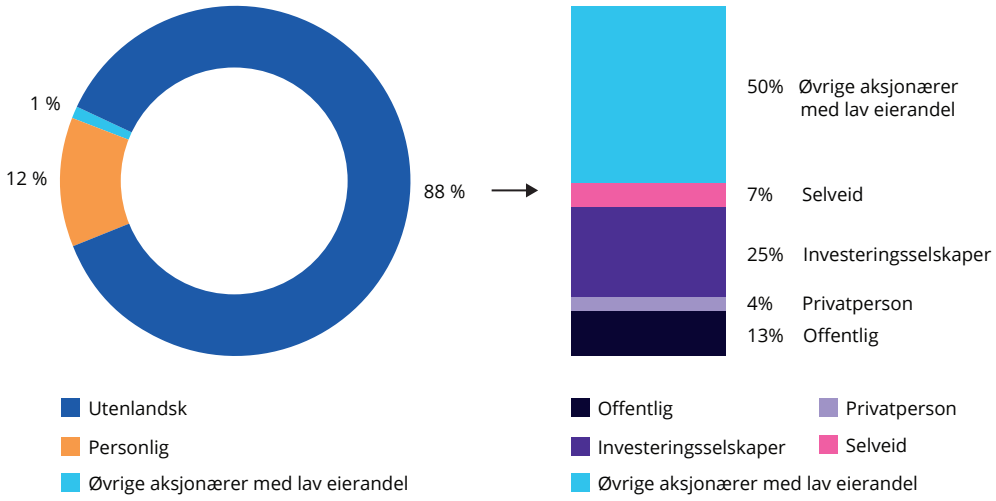


Kilde: Menon Economics (2024), figur 6-2.

En overordnet fordeling av det utenlandske eierskapet er inntatt i figur 6.10 under. Tilsvarende som for infrastruktureierne, fordeler det utenlandske eierskapet blant underleverandørene med fullstendig kartlegging seg primært mellom aksjonærer med små eierandeler, investeringsselskap og offentlige eiere. Samtidig ser man en større andel eierskap hos privatpersoner og selveide aktører (primært stiftelser), og mindre eierskap hos offentlige aktører (13 prosent mot 20 prosent i figur 6.6) og aksjonærer med lav eierandel (50 prosent mot 58 prosent i figur 6.6). Menon tar forbehold om at eierskapsfordelingen baserer seg på et svært begrenset utvalg selskaper – kun fem av leverandørene med full kartlegging (kategori 2A) spores tilbake til utenlandsk eierskap.

Dermed vil denne fordelingen kunne endres betydelig ved endringer i eierskapet til enkeltselskaper.

Figur 6.10 Fordeling av utenlandsk ultimat eierskap hos leverandører med fullstendig kartlegging (kategori 2A), vektet etter omsetning

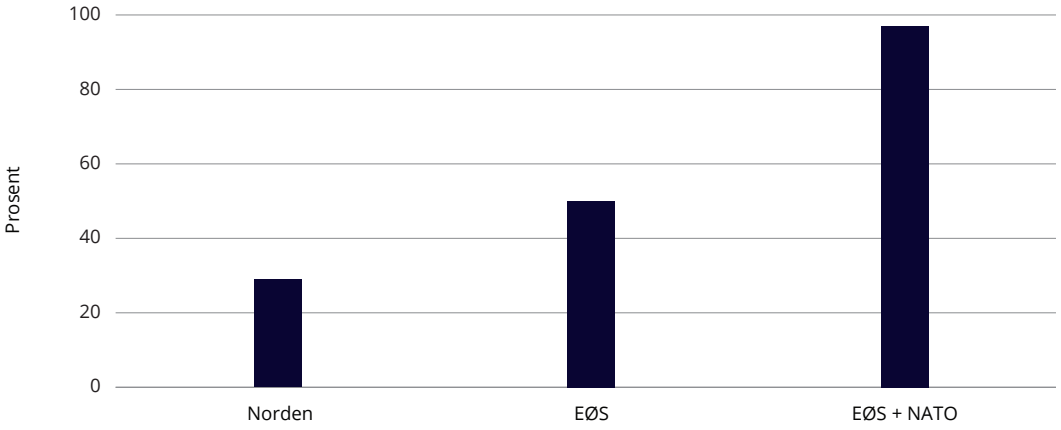


Kilde: Menon Economics (2024), figur 4-10.

Menons funn viser at de største andelene eierskap innen denne kategorien knyttes enten til Sverige eller Storbritannia.[63] Når Menon grupperer eierskapet etter ulike regioner (Norden, EØS og EØS+NATO) finner de at det er en mindre andel av det utenlandske eierskapet for leverandørene (kategori 2-selskapene) som kan knyttes til Norden og EØS enn for selskapene som eier kritisk digital kommunikasjonsinfrastruktur. Dette skyldes i hovedsak den høye andelen av eierskapet som kan knyttes til Storbritannia. Samtidig kan mesteparten av eierskapet, på samme måte som for eiere av infrastrukturen (kategori 1), knyttes til et NATO-land. Som vi ser av figuren nedenfor, kan kun tre prosent av eierskapet knyttes til land utenfor NATO og EØS. Blant disse landene er eierskap fra Chile størst, hvor 1,3 prosent av det ultimate eierskapet i selskapene kan spores til Chile.

[63] Omtalen her baseres på figur 4-11 og 4-12 i Menon (2024).

Figur 6.11 Regionvis fordeling av kjent utenlandsk eierskap blant leverandører i kategori 2A, vektet etter omsetning.



Kilde: Menon Economics (2024), figur 4-12.

For nærmere informasjon om ulike ultimate eierskap kartlagt av Menon for underleverandører, se punkt 4.2.1 tabell 4-2 i Menon (2024).

6.2.7 Menons vurderinger knyttet til utenlandsk eierskap

Menon har ikke avdekket eierforhold som de mener fremstår som problematiske i de selskapene de har undersøkt. Eierskap er en viktig del av risikovurderingen for mulige sårbarheter i infrastrukturen, men gir ikke det hele bildet.

Ifølge Menon må risikovurderingen også inkludere andre faktorer som kontrollmuligheter utover eierskap, inkludert leverandører av hardware, software og sabotasjekapasitet. Dette gjør risikovurderinger komplekse, spesielt ved spesialiserte tjenesteleverandører som kan ha små men kritiske leveranser av viktige komponenter som inngår i en stor forsyningskjede.

Når Menon har vurdert eventuell risiko knyttet til hvert enkelt eierforhold, har det blitt lagt vekt på to ulike elementer; innflytelse (eierandel) og risikoprofil på eieren. Hvor vanskelig det er å innhente eierskapsinformasjon på selskapet bør også anses som en risikofaktor – både fordi det gir usikkerhet knyttet til hvem som eier selskapet, men også fordi vanskeligheten ved å innhente informasjon ofte er korrelert med risikoprofilen på eieren.

Det er generelt få tilfeller der konsulentselskapet enten ikke har lykkes med å nøste eierskapet tilbake til en ultimat eier eller hvor eieren fremstår som et åpenbart risikoelement. Man har hatt særlig søkelys på å avdekke ultimate eiere av norsk digital infrastruktur i stater som kan utgjøre en risiko for Norge og norsk infrastruktur. I praksis finner man i liten grad eierforhold som anses som direkte problematisk med tanke på bindinger til fremmede makter eller statsborgerskap i stater som vurderes som en etterretningstrussel.

En viktig nyanse er at man kategoriserer investeringsselskap som en type ultimat eier. Dette omfatter i all vesentlig hovedsak er forvaltningsselskaper hvor de som eier investeringsselskapet forvalter midler på vegne av investorer. Det er med andre ord ikke (bare) forvalterne av kapitalen som eier kapitalen. Man har derfor i enkelte tilfeller kartlagt de *største* eierne av investeringsselskapet (forvaltningsselskapet), mens man i andre tilfeller har kartlagt de største innskyterne av kapital som forvaltes av investeringsselskapet.

Menon påpeker at innskyterne av kapitalen (såkalte «limited partners») vanligvis har lite innflytelse på forvaltningen av kapitalen. I begge tilfeller har man identifisert og undersøkt eierne, enten de står bak en vesentlig andel av kapitalen eller de eier en vesentlig andel av investeringsselskapet. Det er identifisert et begrenset antall utenlandske privatpersoner med en eierandel i en størrelsesorden som gjør det interessant å undersøke privatpersonene. For samtlige utenlandske private eiere med mer enn 10 prosent eierandel har Menon har gjort omfattende undersøkelse av hvem eieren er og om de har kontroverser knyttet til seg og/eller kjente bindinger til regimer som utgjør en risiko. Det har ikke blitt avdekket slike kontroverser eller kjente bindinger.

Identifiserte risikoelementer som man bør være bevisst på:

Til tross for at det ikke er identifisert alvorlig risiko ved eierskapet til de kartlagte selskapene er det likevel noen elementer knyttet til enkelte selskap og eierforhold Menon mener at det er naturlig å adressere i en risikovurdering. Det er særlig tre forhold som er ønskelig å belyse med disse eksemplene:
- Selskaper eid fra udemokratiske land
- Eierskap og makt konsentrert på enkeltpersoner som er politisk markerte
- Eierskap gjennom lavskatteland (definert som jurisdiksjon med gunstig skatteregime).

Huawei Technologies Norway AS, eid av Huawei Technologies Co., Ltd., er en global leverandør av kommunikasjonsinfrastruktur. Selv om Huawei formelt sett er eid av ansatte, er det bekymringer rundt selskapets tilknytning til kinesiske myndigheter, spesielt på grunn selskapet sivilmilitære funksjoner, grunnleggerens militære bakgrunn og Kinas etterretningslovgivning som innebærer at selskaper til enhver tid kan bli pålagt å dele informasjon med myndigheten. Dette har ført til at Huawei anses som en sikkerhetsrisiko i flere vestlige land, inkludert Norge.

Et annet tilfelle med eierskap som Menon trekker frem er **Starlink Norway AS**, der Elon Musk Trust er majoritetseier. Dette er det fremste tilfellet av de undersøkte eierforholdene på at en utenlandsk privatperson sitter med majoritetseierskap og kontroll av en eier av digital kommunikasjonsinfrastruktur. Starlinks rolle i Ukraina har vært både kontroversiell og essensiell. Tjenesten har vært viktig for Ukrainas kommunikasjon under krisen, og har blant annet vært brukt til flere forsvarsformål. Samtidig har det også vært diskusjoner rundt Starlinks påvirkning og potensielle begrensninger i bruk. Spørsmålet om hvorvidt russiske styrker kan eller har brukt Starlink er også relevant i sikkerhetssammenheng.

Det er bekymringer rundt maktkonsentrasjon over kritisk infrastruktur hos enkeltpersoner med politiske engasjement. Selv om dette ikke utgjør en direkte trussel mot norsk infrastruktur, understreker det ifølge Menon behovet for årvåkenhet over eierskap og kontroll av sentral teknologi.

Menon trekker frem at eierskap gjennom lavskatteland kan være motivert av flere forhold: Eierskap kan være drevet av skattemessige hensyn, ønske om diskresjon og hemmelighold, samt for å forenkle internasjonale investeringer. Dette er vanlig blant aktører som ønsker å tiltrekke kapital fra medinvestorer, spesielt i Nord-Amerika. Norfund har også benyttet slike jurisdiksjoner for å tilrettelegge investeringer, til tross for økt omdømmerisiko.

6.3 Oppsummering

Menons vurdering er at det i kartleggingen ikke er avdekket eierforhold som fremstår som problematiske, bortsett fra eierskapet til Huawei som allerede er godt kjent for norske myndigheter. Rapporten viser at utenlandsk eierskap er utbredt i kritisk digital kommunikasjonsinfrastruktur, og mer utbredt blant leverandørene enn i selskapene som eier infrastrukturen. Kartleggingen viser også at utenlandsk eierskap er mer utbredt i kritisk digital infrastruktur enn i norsk næringsliv generelt.

Utvalget viser til Menons vurdering av at følgende forhold bør inngå i en risikovurdering av utenlandsk eierskap:

- Selskaper eid fra udemokratiske land
- Eierskap og makt konsentrert på enkeltpersoner som er politisk markerte
- Eierskap gjennom lavskatteland

Utvalget deler Menons bekymring knyttet til eierskap fra udemokratiske land, eierskap gjennom lavskatteland og eierskap og makt konsentrert til enkeltpersoner. Samtidig finner utvalget at det verken er «skattenivået» eller «demokratinivået» i seg selv som skal være vurderingskriteriet. At lavskatteland kan ha mangel på transparens knyttet til eierskap, er derimot en bekymring fordi det reelle eierskapet kan være skjult. Videre vil svake eller manglende demokratiske institusjoner kunne føre til uforutsigbarhet i beslutningsprosesser og i rettssystemet. Det er denne uforutsigbarheten som vil være kjernen i en risikovurdering, og ikke styreformen i seg selv. Det er i risikovurderinger knyttet til eierskap fra andre land også nødvendig å ta hensyn til scenarioer som kan oppstå på et senere tidspunkt, og når man befinner seg høyt i krisespennet.

”

I dette kapittelet ser utvalget nærmere på teknologiske og markedsmessige utviklingstrekk i kritisk digital kommunikasjons-infrastruktur.

Foto: Anders Martinsen (Nkom)

07

Teknologiske og markedsmessige utviklingstrekk frem mot 2030

Utvalget har som ledd i sitt arbeid gitt Oslo Economics (OE) og Norsk Utenrikspolitisk Institutt (NUPI) (heretter OE/NUPI) i oppdrag å analysere hvordan teknologiske- og markedsmessige endringer og geopolitisk utvikling kan påvirke nasjonal kritisk infrastruktur de neste årene frem mot 2030. Oppdraget har vært delt i inn i tre deler der man beskriver de viktigste driverne for:

1. 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. 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. Eventuelle utviklingstrekk som bidrar til å redusere sårbarheten i forsyningen av de digitale tjenestene.

I det følgende har utvalget valgt å benytte flere momenter fra utredningen til OE/NUPI inn i utvalgets egne vurderinger.

7.1 Utviklingen i de digitale tjenestene og samfunnets avhengighet av disse

Samfunnet blir stadig mer avhengig av digitale tjenester, og i flere offentlige rapporter fremheves at Norge er et av verdens mest digitaliserte land. Digitaliseringen har gjennomgått flere bølger siden de første datamaskinene ble oppfunnet rundt midten av forrige århundre.

Etter internetts utbredelse fra tidlig 90-tallet ble informasjon mer tilgjengelig, og raskere utveksling av informasjon over store avstander ble mulig. Dette reduserte behovet for fysisk nærhet mellom leverandører og kunder, og sammen med lavere fraktkostnader og liberalisering av internasjonal handelspolitikk, bidro det til økt internasjonal handel fra slutten av 1990-tallet og utover 2000-tallet.

Utviklingen i verdenshandelen har gitt økt handelsvolum, men også endret hvordan varer produseres og kjøpes. Selskaper som samarbeider med strategiske partnere og spesialiserte leverandører har ført til mer desentraliserte og nettverksbaserte verdikjeder. Mange verdikjeder er derfor avhengige av varer produsert i flere land, og de globale forsyningskjedene er igjen avhengige av digitale tjenester for å utveksle informasjon, gjennomføre transaksjoner og organisere disse logistikkverdikjedene.

7.1.1 Skyteknologi og smarttelefoner

Det neste store skiftet kom med oppfinnelsen av smarttelefoner og skyteknologi. Skytjenester, som inkluderer dataprosessering og datalagring på eksterne servere, har gjort det mulig for selskapene å kjøpe slike tjenester fra skyleverandører i stedet for å lagre data i egne lokale datasentre.

Fordelene med skytjenester inkluderer skalerbarhet og rask tilgang til nye applikasjoner og teknologi, samt enklere samarbeid og datadeling. Bruk av skytjenester kan også føre til høyere sikkerhet fordi man får tilgang til mer oppdaterte IT-systemer og gir mulighet for å kvitte seg med utdatert programvare og systemer som kan ha innebygget sårbarhet som kriminelle/fiendtlige aktører kjenner til og kan utnytte.

Mange virksomheter i både offentlig og privat sektor har tatt i bruk skytjenester. I 2023 oppga 71 prosent av alle næringer, utenom finansnæringene, at de har kjøpt en eller flere skytjenester. Blant statlige virksomheter benytter omtrent 97 prosent skytjenester.

Økt bruk av skytjenester har ført til sentralisering av datalagring og prosessering i store datasentre, noe som har økt datasentrenes betydning i den digitale infrastrukturen. Dette har gjort mange virksomheter avhengige av internett for tilgang til data og applikasjoner, og verdien som bæres over transportnettene mellom datasentre, bedrifter og sluttbrukere har økt.

Utviklingen av smarttelefoner har gjort det mulig å utvikle nye digitale økosystemer med applikasjoner for nær sagt alt fra rene underholdningstjenester/sosiale medier (TikTok, Instagram. Facebook, Snapchat, Netflix, YouTube og Spotify mv.) til nyttetjenester som interaksjon med det offentlige (Helsenorge, Digipost, DFØ, BankID osv.) eller private tjenester som reise, strøm, bank og forsikring for å nevne noe.

7.1.2 Digitale tjenester

Mobilbetalinger er en av de andre trendene som fremkommer i rapporten fra OE/NUPI. Denne betalingsmetoden har blitt fremtredende og utgjør nå en stor del av betalingene i Norge. Ifølge Norges Bank ble 82 prosent av alle betalinger mellom privatpersoner i 2023 utført med mobiltelefon, mens bruk av mobilbetaling på utsalgssteder utgjorde 16 prosent.[64] Etter utvalgets oppfatning tilsier dette at tilgang til digitale betalingsmidler/-løsninger også bidrar til å øke befolkningen og samfunnets avhengigheter til de digitale kommunikasjonsnettene.

Det digitale offentlige Norge. Norge har en befolkning med høye digitale ferdigheter og høye forventninger til digitale offentlige og private tjenester. Dette har også ført til at Norge rangeres høyt sammenlignet med andre land i digitalisering av offentlige tjenester. Allerede i april 2012 besluttet regjeringen at digital kommunikasjon skal være den foretrukne kanal for all skriftlig kommunikasjon mellom forvaltningen på den ene siden og innbyggerne og næringslivet på den andre.

Statlige virksomheter og kommuner tilbyr stadig flere digitale selvbetjeningsløsninger og informasjonsløsninger knyttet til ulike tjenester, som Helsenorge for helsetjenester og Altinn for bl.a. rapportering om skatt, avgift og regnskap, arbeidsgiverrapportering, registrering knyttet til næringsvirksomhet og søknader knyttet til støtte- og tilskuddsordninger.

I tillegg kommer satsninger på ulike velferdsteknologier som kan bidra til å avlaste og hjelpe personer med ulike helseutfordringer, nedsatt funksjonsevne osv. Bruk av velferdsteknologi kan bidra til økt trygghet, sosial deltakelse, mobilitet, og styrker den enkeltes evne til å klare seg selv i hverdagen.

Digital hjemmeoppfølging av pasienter innebærer at hele eller deler av et behandlingstilbud skjer digitalt enten det være seg dialog eller deling av data og informasjon.[65] Digitalisering av helse- og omsorgssektoren kan bidra til å øke effektiviteten i tjenestene som leveres slik at helsepersonell får bedre tid til å utføre kjerneoppgaver, noe som samtidig vil kunne øke kvaliteten på tjenestene og øke pasient- og brukertilfredsheten.[66] Samtidig stiller dette også økte krav og forventninger til de ulike digitale kommunikasjonsnettene som bærer tjenestene.

Internasjonalt anerkjennes Norge for å ligge langt fremme, men det pekes også på at vi som nasjon har noen utfordringer foran oss slik det kommer til uttrykk i OECD-rapporten «Going Digital: Shaping Norway's Digital Future»:[67]

> «Norway is at the digital frontier in many areas. The challenge for Norway is how to keep pace with rapid technological developments and competition, while improving performance in areas in which there are opportunities to catch up. Staying at the frontier requires agility, flexibility and well-co-ordinated digital policies. A national digital strategy can play an important role to ensure the policy framework in place makes the most of digital technologies and data for growth and well-being.»

64 Norges Bank Memo 1/2023 https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Norges-Bank-Memo-/2023/memo-12023-betalingsformidling/nettrapport-memo-12023-betalingsformidling/

65 Helsedirektoratet – https://www.ehelse.no/velferdsteknologi-og-digital-hjemmeoppfolging

66 NOU 2023: 4 *Tid for handling – Personellet i en bærekraftig helse- og omsorgstjeneste*, https://www.regjeringen.no/contentassets/337fef958f2148bebd326f0749a1213d/no/pdfs/nou202320230004000dddpdfs.pdf

67 https://www.oecd.org/en/publications/shaping-norway-s-digital-future_d3af799c-en/full-report.html

7.1.3 Digitaliseringsstrategi 2024-2030

Regjeringens digitaliseringsstrategi for offentlig sektor 2024-2030 har klare ambisjoner om ytterligere digitalisering, med mål om at enda flere oppgaver skal løses digitalt og at brukerne skal oppleve én digital offentlig sektor. Strategien er ambisiøs og vektlegger fem kategorier med tiltak som blant annet omfatter:

1. *Et enklere og tryggere hverdagsliv* – Høyhastighets bredbånd for alle med minst 1 Gbit/s nedlastingshastighet og bedre mobildekning. Tilbud om digital lommebok og elektronisk ID, samt utvikling av grunnleggende digitale ferdigheter. Personvernet skal styrkes, og folks motstandskraft mot desinformasjon skal økes.
2. *Mer moderne, offentlige tjenester* – Hele den offentlig sektor skal digitaliseres for å tilby raskere saksbehandling, bedre digitale tjenester, og frigjøre tid og ressurser til de viktigste oppgavene. Digitaliseringstiltak skal prioriteres langsiktig for å sikre at de skjer på områdene med størst behov og gir størst gevinst for samfunnet.
3. *Skape verdier med data og KI* – En nasjonal infrastruktur for kunstig intelligens (KI) skal bygges for bruk i forskning, næringsutvikling og en mer moderne offentlig sektor. En ny lov om datadeling skal fremmes, og offentlige og private virksomheter skal få tilgang til data fra offentlig sektor for innovasjon og verdiskaping.
4. *Verktøy for vår tids omstillinger* – Kompetanse skal fortsatt være Norges fremste konkurransefortrinn, og derfor skal det bygges sterkere digital kompetanse fra grunnskolen til høyere utdanning og etter- og videreutdanning. Næringslivets konkurranseevne skal styrkes gjennom innovativ bruk og deling av data, KI mv. Digitalisering skal være en drivkraft for omstillinger og for å skape nytt næringsliv og nye selskaper.
5. *Trygg digital oppvekst* – Alle skal få mulighet til å delta i det digitale samfunnet, og innbyggere skal beskyttes mot digitale trusler og angrep. Barn og unge skal lære å bruke teknologi på en ansvarlig måte, i tillegg til at det for eksempel skal settes krav til store tech-selskaper der de har for mye makt.

Dersom Norge lykkes i omstillingen til en enda mer digital hverdag så innebærer det samtidig en betydelig forsterket avhengighet til de digitale kommunikasjonsnettene våre. Dette støttes også av rapporten fra OE/NUPI.

Selv om totalen dermed innebærer at verdiene som bæres over den digitale infrastrukturen vil øke, så kan det likevel trekkes frem at OE/NUPI også tar for seg enkelte forhold som kan bidra til å begrense eventuelle negative konsekvenser ved sikkerhetsbrudd hos enkeltstående aktører eller systemer:

- den digitale infrastrukturen er ikke en enkeltstående enhet, men består 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.
- sluttbrukere er i økende grad opptatt av sikker kommunikasjon, og implementerer tiltak for å spre trafikk og data geografisk og hos flere tilbydere.

7.2 Viktige teknologiske trender fremover

Når man skal se på hvordan samfunnets avhengigheter til kritisk digital infrastruktur kan utvikle seg fremover er det samtidig viktig å se på hvilke teknologiske fremskritt eller utviklingstrekk som kan bli avgjørende. I det følgende omtales flere av de momentene OE/NUPI tar opp i sin rapport til utvalget.

7.2.1 Bruk av kunstig intelligens (KI)

Få ting har så til de grader vært med på å prege den teknologiske utviklingen i de senere år som kunstig intelligens og forventningene til hva teknologien skal kunne brukes til er mange.

Bruk av KI vil føre til at flere oppgaver som i dag gjennomføres manuelt vil kunne automatiseres, samtidig gir det større avhengighet til de digitale tjenestenes verdikjeder. Dette vil igjen føre til en økning i verdiene som bæres over den digitale kommunikasjonsinfrastrukturen.

I Teknologirådets årsrapport beskrives 2023 som året da kunstig intelligens (KI) for alvor ble en del av norsk samfunnsliv og politikk En undersøkelse utført av Samfunnsøkonomisk Analyse (SØA) på vegne av NHO, Abelia, Finans Norge og Nelfo høsten 2023, viste at én av fire virksomheter har tatt i bruk KI, og det forventes at bruken vil øke.

I sin rapport peker OE/NUPI på andre mulige bruksområder knyttet til kunstig intelligens, for eksempel hvordan kunstig intelligens og maskinlæring kan brukes for å drifte nettverk. Det vises til rapport fra sammenslutningen av europeiske ekommyndigheter (BEREC – Body of European Regulators for Electronic Communications) som bl.a. peker på at ved overgang til mer bruk av softwarebaserte nett og visualiserte nettverksfunksjoner, så 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.[68]

OE/NUPI viser videre til forsøk med å utvikle teknologiske løsninger som vil gjøre det mulig å kjøre KI-applikasjoner nær sluttbruker på kanten av nettverket (edge). Treningen av store språkmodeller krever betydelig prosesseringskapasitet, noe som gjør at denne treningen sannsynligvis må utføres sentralt i større datasentre. Etter treningen kan modellene *tolke og analysere nye data* basert på kunnskapen de har opparbeidet seg fra treningsdatasettet på kanten av nettverkene (edge). Dette vil redusere behovet for dataoverføring mellom sluttbruker og datasenter, redusere tidsforsinkelser, og gjøre det mulig for enheter å fungere uten konstant internettforbindelse. Flere selskaper utvikler derfor teknologi for å kjøre KI-applikasjoner på edge-enheter.

Også telekom-operatører vurderer muligheten for å tilby tilstrekkelig prosessor- og lagringskapasitet i sine nettverk for å støtte KI-applikasjoner hos sluttbrukere. Det finnes flere slik samarbeidsprosjekter mellom aktører i verdikjeden, for eksempel samarbeider NVIDIA, Ericsson, Nokia og T-Mobile om å etablere et AI-RAN Innovation Center. Målet er å utvikle en plattform for å optimalisere mobilnettverkene med KI og levere edge computing-tjenester til sluttbrukere.

[68] https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-impact-of-artificial-intelligence-ai-solutions-in-the-telecommunications-sector-on-regulation

7.2.2 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 ifølge OE/NUPI skapt usikkerhet om hvilke skytjenester 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 av ulike typer data. Flere statlige virksomheter har derfor vært avventende med å migrere beskyttelsesverdig ugradert data over i skytjenester, og har fortsatt å benytte on-premise løsninger for disse dataene. Etter hvert som det utvikles ulike skytjenester for ulike deler av statsforvaltningen vil mer data i statsforvaltningen som i dag lagres on-premise migreres over i ulike skytjenester.

Innen telekomsektoren har BEREC gjort undersøkelser av hvordan sektoren selv benytter skytjenester.[69] Undersøkelser viser at telekomselskaper har en risikobasert tilnærming til hvilke tjenester de plasserer i skytjenester som de ikke drifter selv. Tjenester med lav risiko, som fakturering og kundeanalyser, plasseres ofte i allmenne skytjenester. Mer kritiske funksjoner, som drift av kjernenett, holdes i egne løsninger.

Rapporten viser også en trend mot økt bruk av teknologier som virtualisering av kjernettfunksjoner for å drifte nettverkene. Virtualisering og softwarebaserte nettverk gjør det mulig å kontrollere nettverkene med software i stedet for dedikert hardware. Dette bidrar til å sentralisere styringen og gjør driften av nettverkene mer effektiv, samtidig som det reduserer behovet for ytterligere investeringer i nettverksinfrastruktur. På den annen side øker dette kompleksitetene i nettene og øker verdien av operasjonene som gjøres sentralt.

Men som det også fremkommer i BEREC-rapporten så er det også enkelte telekomselskaper som har inngått samarbeid med skytjenesteleverandører der de tester å plassere 5G-kjernen i virtuelt lukkede skytjenester fra allmenne skytjenesteleverandører.

7.2.3 Utvikling av datasenterindustrien

OE/NUPI peker i rapporten på en forventning om 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, noe som medfører 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.

[69] https://www.berec.europa.eu/en/all-documents/berec/reports/berec-report-on-cloud-and-edge-computing-services

Her kan Norge være et attraktivt sted å etablere neste generasjons datasentre. Dette skyldes blant annet at Norge har tilgang på regulerbar 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.

7.2.4 Større verdier bæres over de kommersielle kommunikasjonsnettene

Større verdier bæres over de kommersielle kommunikasjonsnettene – den teknologiske utviklingen gjør det mulig å opprette virtuelle private nettverk innad i kommersielle 5G-nett. Dette vil gjøre at kunder som i dag har egne fysisk private nettverk i større grad kan kjøpe dette som en tjeneste fra kommersielle telekomoperatører. Dette muliggjør blant annet at dagens Nødnett kan migrere over i de kommersielle mobilnettene, i tillegg til at Forsvaret over tid også tester ut ulike løsninger i de kommersielle mobilnettene.

7.2.5 Internet of Things og virtuell virkelighet

Internet of Things (IoT) og Machine-to-Machine (M2M) dekker et vidt spekter av teknologier. IoT refererer til alle tingene rundt oss som kan kobles til internett. Når tingene er koblet til nett, kan de kommunisere med hverandre og omgivelsene. Typiske bruksområder spenner fra smarthøyttalere og sporingstjenester til digitale kjørebøker og sensorer som måler temperatur, strøm, luftkvalitet, fuktighet og vann. Antallet IoT-enheter som er koblet til internett har økt betydelig, og det er forventet at antallet vil fortsette å øke i fremtiden. Disse enhetene vil produsere store mengder data og drive utviklingen mot stadig mer digitaliserte verdikjeder. Utbygging av 5G-nett med lav forsinkelse og bruk av kunstig intelligens vil gi nye muligheter innen ulike industrisektorer og bidra til vekst innen IoT.

Virtuell virkelighet (VR) er kunstig gjengivelse av miljø med bruk av bilder og lyd. VR-simuleringer blir stadig bedre innen felt som medisin, byggeteknikk og 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 typen teknologi sannsynligvis ha høye krav til båndbredde og lav tidsforsinkelse.

7.3 Viktige markedsmessige trender fremover

I Europa er det, i likhet med Norge, stort søkelys på utbygging av fremtidsrettet ekominfrastruktur, både 5G-nett og fibernett. I enkelte europeiske land har utrullingen av fullverdige 5G-nett kommet svært kort, noe som skaper en generasjonsforskjell i mobilnett mellom enkelte EU-land. Dette gjelder også utbyggingen av fibernettdekning. For Norges del arbeider også de tre norske mobilnetteierne med utvikling av egne fullverdige 5G-nett, dvs. at både radio- og kjernenett er basert på 5G-arkitektur.

Europakommisjonen er bekymret for at utbyggingen ikke er i rute til å nå målene i strategien for EUs digitale tiår (Digital Decade Policy Programme 2030). Kommisjonen anslår at det er behov for investeringer på mellom 150 og 220 milliarder euro for å oppnå målet om at alle europeiske husstander har tilgang til et gigabit nettverk, og alle befolkede områder har 5G-dekning.

Flere rapporter om europeisk konkurransedyktighet og fremtiden til det indre markedet understreker behovet for en velutbygget kommunikasjonsinfrastruktur for at EU skal lykkes med omstillingen til en konkurransedyktig, grønn og digital økonomi.[70] I denne sammenheng løftes også frem mulighet for ytterligere konsolidering innen ekomsektoren i de samme nasjonale markedene. Hittil har Kommisjonen og nasjonale konkurransemyndigheter opprettholdt streng kontroll over fusjoner mellom konkurrerende mobiloperatører for å sikre flere uavhengige mobilnett og opprettholde konkurransen. Fokuset har i svært stor grad vært rettet mot forbrukerpriser og ikke mot andre og viktige forhold som investeringer i økt sikkerhet i kritisk kommunikasjonsinfrastruktur som også har stor betydning for forbrukerne og som gagner samfunnet som helhet. Dette bildet kan være i ferd med å endre seg. Det europeiske ekommarkedet er under økt press, og det pekes på behovet for å stimulere investeringer i utbygging av infrastrukturen og styrke europeiske virksomheters innovasjonskraft og konkuranseevne. Det er den klare konklusjon på bakgrunn av Mario Draghis omfattende analyse til Kommisjonen fra september 2024. Samtidig må den digitale infrastrukturen styrkes for å fortsatt være motstandsdyktig, og det krever økte investeringer og sterke aktører for å sikre den nødvendige robustheten og sikkerheten i nettene. Konsolidering av nettverksinfrastruktur i sektoren kan bidra til å skape stordriftsfordeler og sikre forutsetningene for de nødvendige investeringer.

7.4 Viktige geopolitiske trender

I rapporten sin viser OE/NUPI gjennom utstrakt kildebruk at det i løpet av de siste 20 årene har skjedd betydelige endringer i samspillet mellom digital teknologi og globale maktrelasjonene. I de tidlige fasene av digitaliseringen var det en utbredt oppfatning, spesielt i vestlige land, at digital teknologi krevde unike styringsformer med minimal statlig inngripen. Denne tilnærmingen ble drevet av troen på at dette ville fremme økonomisk vekst og utnyttelse av ny teknologi. I tillegg reduserte vestlige selskapers dominans i teknologisektoren behovet for sterk statlig kontroll. Autoritære stater som Kina og Russland argumenterte på sin side for «digital suverenitet» og sterkere statlig kontroll i møte med det de oppfattet som amerikansk dominans.

På 2010-tallet ble behovet for nasjonal kontroll mer fremtredende i Europa og USA, særlig drevet fremover av flere faktorer:

1. **Sikkerhetsutfordringer**: Store sikkerhetsbrudd som WannaCry og NotPetya i 2017 synliggjorde de alvorlige konsekvensene cyberangrep kunne få for viktige sektorer som helse og global handel. Angrepene førte til økt politisk oppmerksomhet og krav om sterkere statlig regulering for å beskytte kritiske samfunnsinteresser.
2. **Økonomisk vekst i Kina**: Kinas økonomiske vekst og fremveksten av nettverkskritiske leverandører som Huawei og ZTE skapte bekymringer i en rekke vestlige land om deres egen teknologiavhengighet til land man ikke var sikkerhetspolitisk alliert med.
3. **Monopoltendenser**: Store teknologiselskapers økende makt og innflytelse ble problematisert, noe som førte til politisk mobilisering for sterkere statlig inngripen.

[70] Se for eksempel Europakommisjonens Hvitbok *How to master Europe's digital infrastructure needs?,* Enrico Lettas rapport *Much more than a market (2024)*, og Mario Draghis rapport *The future of European competitiveness* (2024)

Den geopolitiske utviklingen har ført til at digital teknologi nå er et mer sensitivt område mellom stater. Økte spenninger mellom USA og Kina, samt en gradvis endring i Europa mot å se handel og geopolitikk i sammenheng, har forsterket behovet for nasjonal kontroll. Uforutsette globale hendelser som Covid-19-pandemien og den russiske invasjonen av Ukraina har ytterligere understreket risikoene ved teknologiske og økonomiske avhengigheter, og behovet for robust nasjonal digital infrastruktur.

I de kommende årene forventes økt statlig inngripen og nasjonal kontroll over digital infrastruktur. Nasjoner vil fokusere på å redusere problematiske avhengigheter og forsterke samarbeidet med allierte for å styrke nasjonal kontroll og legge sterkere føringer for økonomisk samhandling basert på hensynet til nasjonal sikkerhet.

Teknologiske og økonomiske avhengigheter blir i økende grad sett på som potensielle sårbarheter. Avhengighet av utenlandske teknologileverandører kan føre til tap av sensitiv informasjon og usikkerhet rundt kritiske tjenesters tilgjengelighet i hele spennet mellom fred-krise-krig. Manglende nasjonal kontroll kan også svekke evnen til å sikre verdikjeder, spesielt under sikkerhetspolitiske kriser.

Den geopolitiske situasjonen vil ikke bare påvirke behovet for kontroll i Norge, men også hos våre allierte. For et lite land som Norge er det nasjonale handlingsrommet for handels- og industripolitiske tiltak begrenset. Det er derfor særlig relevant å se på transatlantisk sikkerhetspolitisk samarbeid som, gitt industripolitisk koordinering blant vestlige land, antakelig vil kunne gjøre behovet for nasjonal kontroll langt mindre.

I rapporten tar OE/NUPI derfor også for seg viktige regulatoriske utviklingstrekk i USA og EU.

7.4.1 USA

Utviklingen i USA er sterkt påvirket av forholdet til Kina. Kinas økonomiske vekst har skapt gjensidig avhengighet, men også økt skepsis i USA mot avhengighet innen handel, investeringer og ikke minst teknologi. Denne skepsisen har også sitt opphav i oppfatningen om at kinesiske selskaper i stor grad opererer i forlengelse av den kinesiske staten. Amerikanske myndigheter har jevnlig anklaget kinesiske selskaper for industrispionasje og urettferdige praksiser, noe som har ført til økt interesse om å begrense kinesiske selskapers tilgang til den amerikanske økonomien.

Da Donald Trump ble president i USA i 2016 endret USA sin tilnærming til global handel, og økonomisk velstand ble definert som et mål for nasjonal sikkerhet. Denne retorikken har fortsatt under Biden/Harris administrasjonen med subsidier, lån, tariffer og skatteinsentiver for å sikre at USA leder an 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 her vil bli opp mot 4 billioner dollar.

USA har også strammet grepet om nasjonal kontroll gjennom Committee on Foreign Investment in the United States (CFIUS), som har fått utvidede fullmakter til å blokkere investeringer som truer nasjonal sikkerhet. I 2022 ble det spesifisert at CFIUS særlig skulle vurdere effekten av utenlandske investeringer på verdikjeder, amerikansk lederskap i nye teknologier, cybersikkerhetsrisiko og risikoen for amerikanske borgeres

personopplysninger. For utvalgte teknologiområder har amerikanske myndigheter indikert en politikk der det for særlig kritiske teknologier og innsatsfaktorer bak disse pålegges strenge begrensninger, også på *utgående* investeringer.

For telekombransjen har «Team Telecom» vurdert sikkerhetsrisikoen ved utenlandsk deltakelse.[71] I 2021 ble prosessen formalisert med et tydelig mandat om å vurdere sikkerhet ved utstedelse av lisenser. USA har også fokusert på verdikjeder og mulige avhengigheter, med tiltak for å utestenge leverandører som antas å kunne samarbeide med fiendtlige makter.

7.4.2 EU

Mens USA og Kina har vært i sentrum av stormaktsrivaliseringen, har EU lenge vært en mindre aktiv aktør i sammenvevingen av økonomi og sikkerhet. De siste årene har EU imidlertid gjennomgått et betydelig skifte med mer omfattende reguleringer og et sterkere ønske om teknologisk uavhengighet.

Siden 2017 har EU gradvis endret sin tilnærming til kontroll og utvidet sitt regelverk for økonomisk sikkerhet. Dette inkluderer strategi rundt forholdet til Kina (2019), gjennomgang av handelspolitikken (2021), oppdaterte regler for eksportkontroll (2021), tiltak mot utenlandske subsidier (2023), et felles instrument mot økonomisk maktbruk (2023) og utviklingen av en økonomisk sikkerhetsstrategi (2023). Mest relevant er reguleringen rundt investeringskontroll vedtatt i 2019 og i bruk siden oktober 2020. Denne reguleringen gir EU-kommisjonen myndighet til å vurdere potensielle investeringer fra tredjeland som kan påvirke kritisk infrastruktur, teknologi, råvarer, sensitiv informasjon og mediestyring. Se for øvrig ytterligere omtale av investeringskontroll-regelverket og forslag fra januar 2024 til endret EU-regulering i kapittel 10.

Samtidig med dette har EU også iverksatt tiltak for å styrke Europas posisjon innenfor viktige områder som eksempelvis det grønne skiftet og digital teknologi. Blant disse kan European Chips Act som trådte i kraft i 2023 nevnes spesielt fordi den setter søkelys på konkrete mottiltak til Europas avhengighet av importerte halvledere gjennom forskning på halvlederteknologi, innovasjon og produksjon av halvledere mv. Regjeringen har i statsbudsjettet for 2025 foreslått en årlig bevilgning på 40 millioner kroner for å sikre norsk deltakelse i programmet.

For særlig kritiske teknologier har EU også introdusert Strategic Technologies for Europe Platform (STEP) som skal legge til rette for investeringer og styrke Europas uavhengighet. Den totale budsjettrammen er på 160 milliarder euro, og digitale sektorer som skytjenester, 5G, kunstig intelligens og cybersikkerhet er eksplisitt nevnte satsningsområder.

EU har i de senere årene også tatt viktige regulatoriske grep innen cybersikkerhetsområdet, for eksempel gjennom Cybersecurity Act (vedtatt 2019) som etablerer en sertifiseringsordning for cybersikkerhetsprodukter og tjenester og

[71] Team Telecom er en samling av byråer (Department of Justice, Defence med ansvar for ulike deler av nasjonal sikkerhet og som gir råd til den føderale kommunikasjonskommisjonen (FCC) om mulige sikkerhetsrisikoer ved utgivelse av lisenser for å delta i det amerikanske ekommarkedet.

Cyber Resilience Act (vedtatt oktober 2024) som sikter på å heve sikkerhetsnivået for hardware og software på det europeiske markedet. Regelverket vil også potensielt gi Europakommisjonen myndighet til å utestenge produkter som ikke har tilfredsstillende standard fra EU.

Av andre viktige initiativ fra EU-siden kan med fordel også NIS 2 (direktivet om tiltak for å sikre et høyet felles nivå for sikkerhet i nettverks- og informasjonssystemer, vedtatt 2022), CER (direktivet om kritiske enheters motstandsdyktighet, vedtatt 2022) og Cyber Solidarity Act (forslag 2023) nevnes. Det samme gjelder for hvitboken som Kommisjonen publiserte i februar 2024 som har en egen del viet til sikker og motstandsdyktig digital infrastruktur i Europa, herunder også en egen anbefaling knyttet til internasjonale sjøfiberkabler.

Alle disse initiativene er med på å underbygge at Europa tar på alvor ulike sikkerhetstruende aktiviteter og samtidig forsøker å sikre europeisk uavhengighet i viktige leverandørkjeder.

7.4.3 Konklusjon

EU har de 10 siste årene utviklet seg til å ta en større rolle 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. EU har endret karakter fra en forkjemper for frihandel til en mer strategisk orientert geoøkonomisk aktør. Dette har resultert i reguleringer som strammer kontrollen over økonomisk samhandling, koordinering blant medlemslandene, og investeringer i nøkkelindustrier for å styrke europeisk teknologiuavhengighet. Draghi-rapporten fra 2024 peker på en retning for Europa som bruker økonomisk politikk for å styrke strategisk posisjon og geopolitiske innflytelse. Hvilken retning EU tar videre vil ha stor betydning for Norges handlingsrom og behov for nasjonal kontroll.

Det er mer uro i verden, og spenninger internasjonalt øker behovet for kontroll over kritisk teknologi og kritisk digital 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 Norge fatter lignende tiltak. Tiltak for nasjonal kontroll må derfor være tilpasset den geopolitiske konteksten, og ikke avvike for mye fra våre nærmeste samarbeidspartnere.

I rapporten tar OE/NUPI til orde for en utvikling over de neste 5-10 årene der man vil se at verdikjeder i EU og USA blir mindre avhengige av leverandører fra land man ikke har sikkerhetspolitisk samarbeid med. Økt robusthet hos Norges samarbeidspartnere vil da være med på å øke vår egen robusthet, slik at eventuelle tiltak for nasjonal kontroll kan målrettes mot risikoer knyttet til investeringer og eierskap.

Foto: Nkom

III

Om eierskap og andre virkemidler for nasjonal kontroll

”

Kapittelet redegjør for hvilke eierskap og eierskapstransaksjoner som gir innflytelse, samt eiers rettigheter og terskler for innflytelse i selskaper. Det ses også på kilder for kontroll med eierskap og risiko knyttet til utenlandsk eierskap.

Foto: Adobestock

08

Eierskap og eierskapstransaksjoner som påvirker nasjonal kontroll

8.1 Innledning

I dette kapittelet redegjør utvalget for hvilke eierskap og eierskapstransaksjoner som gi innflytelse i et foretak, samt eiers rettigheter i et foretak og terskler for innflytelse. Det ses også på kilder for norske myndigheters kontroll med eierskap. Til slutt ser utvalget nærmere på hvordan utenlandsk eierskap kan svekke nasjonal kontroll.

8.2 Innflytelse i foretak

8.2.1 Innledning

Aksjeselskap er den vanligste foretaksformen i Norge, og som det framgår av punkt 6.2.1, er alle de identifiserte aktørene som eier eller råder over kritisk digital infrastruktur, organisert som aksjeselskaper (med unntak av De-Cix Management GmbH som er organisert som et NUF[72] samt Telenor ASA (allmennaksjeselskap[73]). Det betyr at investeringer og eierskifter i disse selskapene normalt skjer ved erverv av aksjer enten gjennom direkte kjøp i annenhåndsmarkedet eller ved nytegning. Utgangspunktet er at alle aksjer gir lik rett i selskapet (jf. aksjeloven (asl.) § 4-1) og at en aksjonærs eierandel i selskapet er avgjørende for hvilken innflytelse aksjonæren har over beslutningene som fattes i selskapet. Den som eier alle aksjer i et aksjeselskap, vil dermed også ha

[72] Norskregistrert utenlandsk foretak

[73] Allmennaksjeselskap en selskapsform for store norske selskaper med mange aksjonærer og med aksjekapital på minimum 1 million kroner som er regulert i allmennaksjeloven. Hovedforskjellene mellom et ASA og et AS er at det er færre begrensninger i kjøp og salg av aksjene i et ASA, og at det derfor kan børsnoteres og aksjene kan omsettes fritt.

full kontroll over selskapet og kan utøve sitt eierskap innenfor de rammer som følger av regelverket. Innflytelse i selskaper utøves imidlertid ikke bare gjennom eierskap – for eksempel kan aksjonæravtaler og andre avtaler som inngås, endre kontroll og innflytelse på beslutningene. At aksjeeiers innflytelse i selskapet påvirkes for eksempel av aksjonæravtaler om hvordan stemmerettigheter skal utøves og som ikke trenger være kjent for andre enn avtalepartene, eller ved at aksjene kan ha ulik stemmerett, kan gjøre det vanskelig å få oversikt over hvem som har den reelle innflytelse knyttet til selskapsbeslutninger.

8.2.2 Ulike typer innvesteringer som gir innflytelse i et aksjeselskap

I NOU 2023: 28 *Investeringskontroll* punkt 10.2 gis det en nærmere oversikt over hvordan et selskap eller en person gjennom investeringer i et aksjeselskap, kan skaffe seg innflytelse i det aktuelle selskapet. Nedenfor følger en kort oversikt over ulike transaksjoner og avtaler som direkte eller indirekte kan gi innflytelse i et selskap.

Det betegnes gjerne som *oppkjøp* dersom investor kjøper opp alle eller flertallet av aksjene i et selskap. Et oppkjøp vil gi kjøper bestemmende innflytelse når det gjelder forvaltningen av selskapet og selskapets verdier. Mens oppkjøp gjelder transaksjoner knyttet til eierandelene i selve foretaket, brukes *virksomhetsoverdragelse* som betegnelse på en transaksjon som innebærer overdragelse av innholdet i et foretak – gjerne kalt en innmatstransaksjon.

Kjøp av enkeltaksjer eller mindre aksjeposter vil normalt ikke gi bestemmende innflytelse i selskapet med mindre investor allerede eier aksjer i selskapet og kjøpet medfører at eierandelen samlet sett representerer flertallet av aksjene i selskapet.

For børsnoterte allmennaksjeselskaper gjelder det særlige regler om tilbudsplikt ved erverv av aksjer. Det følger av verdipapirhandelloven § 6-1 at «*Den som gjennom erverv blir eier av aksjer som representerer mer enn 1/3 av stemmene i et norsk selskap hvis aksjer er notert på norsk regulert marked (notert selskap), plikter å gi tilbud om kjøp av de øvrige aksjene i selskapet*». Dette betyr at den som erverver tilstrekkelig antall aksjer til å oppnå såkalt negativt flertall[74], og dermed kan forhindre vedtak på generalforsamling som krever kvalifisert flertall, har plikt til å tilby å kjøpe også de øvrige aksjene i selskapet når selskapet er notert på norsk regulert marked. Videre må aksjeeier som eier aksjer som representerer mer enn en tredel av stemmene i et notert selskap, gi tilbud om kjøp av de øvrige aksjene i selskapet (gjentatt tilbudsplikt) ved erverv av aksjer som øker antall stemmer i selskapet til 40 prosent eller mer og 50 prosent eller mer. Det er beskyttelse av minoritetsaksjonærer som er hovedhensynet bak reglene om tilbudsplikt og gjentatt tilbudsplikt.

Aksjer kan også erverves ved *nytegning*. En emisjon gjennom nytegning gjennomføres for å skaffe selskapet egenkapital. I slike tilfeller er det selskapet selv som utsteder nye aksjer og som mottar oppgjøret.

[74] Har man mer enn 1/3 flertall av aksjene har man såkalt negativt flertall. Det innebærer at man kan blokkere vedtektsendringer, fusjoner, fisjoner, kapitalforhøyelser og kapitalnedsettelser. Se nærmere i avsnitt 8.2.3.

En *opsjon på kjøp av aksjer* er et finansielt instrument som gir en rett, men ingen plikt, til å kjøpe eller tegne aksjer innen en bestemt tidsperiode, og til en bestemt pris eller en pris knyttet til en prismekanisme.

Konvertible lån er lån som gir långiver rett til å kreve aksjer i selskapet som er låntaker. Långiver kan betale aksjeinnskudd i penger, eller ved å motregne lånet mot aksjeinnskuddsforpliktelsen. Lånet vil i sistnevnte tilfelle anses nedbetalt. Også andre typer låneavtaler kan gi långiver innflytelse i selskapet, for eksempel ved at det stilles som vilkår for lånet at långiver må godkjenne visse selskapstransaksjoner.

To eller flere selskaper kan slås sammen til ett selskap gjennom en *fusjon.* Det overtakende selskap videreføres, mens overdragende selskap slettes. Aksjonærene i det overdragende selskapet får vederlag for verdiene sine gjennom aksjer i det overtakende selskapet. Et selskap kan gjennom en *fisjon* deles i to eller flere selskaper. Aksjonærene i selskapet som fisjonerer – det overdragende selskapet – vil som vederlag for eiendelene som overdras, få aksjer i overtakende selskap. Fisjon kan innebære at det overdragende selskapet overfører alle eiendeler til to eller flere selskaper og selv opphører å eksistere, eller ved at det overdragende selskapet beholder deler av verdiene selv, og overfører de resterende verdiene til overtakende selskap. Det overtakende selskap kan enten være nystiftet eller være et eksisterende selskap som vil foreta en kapitalforhøyelse ved overføringen av eiendelene.

8.2.3 Eiers rettigheter og innflytelse i et aksjeselskap – terskelverdier for ulik innflytelse

Eier av en aksje i et aksjeselskap har ulike aksjonærrettigheter som kan deles inn i
- økonomiske rettigheter som rett til utbytte og tilbakebetaling av aksjekapitalen, fusjonsvederlag og fortrinnsrett til aksjer som utstedes ved kapitalforhøyelse,
- disposisjonsrettigheter som rett til å erverve, realisere og pantsette aksjer, samt
- forvaltningsrettigheter som retten til å møte, tale og stemme på generalforsamlingen.

Knyttet til innflytelse i selskapet er særlig retten til å møte, tale og stemme på generalforsamlingen viktig. Generalforsamlingen er øverste myndighet i et aksjeselskap og det er gjennom deltakelse på generalforsamlingen at eierne utøver den øverste myndigheten i selskapet. Det følger av aksjeloven at det er generalforsamlingen som treffer beslutningen i en rekke viktige spørsmål, for eksempel om utdeling av utbytte, kapitalforhøyelse, kapitalnedsettelse, fusjon eller fisjon.

Gjennom vedtekter, instrukser og andre beslutninger, fastsetter generalforsamlingen overordnede rammer og nærmere regler for styret og daglig leder om driften av selskapet. Det følger av aksjeloven § 6-3 at det er generalforsamlingen som velger alle eller flertallet av styremedlemmene. Har selskapet bedriftsforsamling[75], er det den som velger medlemmene i styret.

Et aksjeselskap ledes av styret og eventuelt en daglig leder. Det er styret som har det overordnede ansvaret for at selskapet drives i tråd med selskapets formål, det vil si at

[75] Alle AS og ASA skal ha bedriftsforsamling dersom selskapet har mer enn 200 ansatte (asl. og asal. § 6-35). Den skal bestå av minst 12 medlemmer, der 2/3 velges av generalforsamlingen, mens 1/3 velges av og blant de ansatte.

selskapet drives innenfor det som er vedtektenes angivelse av virksomhetsområde, vedtektene for øvrig og eventuelle instrukser fra eierne. Styret har også ansvaret for at selskapet etterlever lover og regler samt avtaler selskapet har inngått. Daglig leder skal forholde seg til de pålegg og retningslinjer som styret gir. For å kunne utøve eierinnflytelse i et aksjeselskap, er det derfor sentralt å ha kontroll over styret. Som oftest kan den som har flertallet av stemmene på generalforsamlingen, sikre seg at styret eller i hvert fall flertallet av styret består av medlemmer som flertallsaksjonæren foretrekker. Den som erverver mer enn halvparten av aksjene i selskapet, vil dermed kunne fjerne alle eller flertallet av de sittende styremedlemmene og velge nye styremedlemmer.

Terskler for innflytelse

Utgangspunktet i aksjeloven (§ 5-17) er at en beslutning som treffes av generalforsamlingen krever flertallet av de avgitte stemmene, med mindre det er fastsatt noe annet i lov eller vedtektene. At flertallskravet knytter seg til avgitte stemmer, betyr at aksjonæren må delta på generalforsamlingen selv eller ved fullmektig.

For å kunne treffe beslutning i enkelte saker av mer grunnleggende betydning, kreves det kvalifisert flertall. Begrunnelsen for dette er at utgangspunktet om at flertallet bestemmer, kan gi flertallet for sterk stilling overfor mindretallet, og at flertallsmakten kan misbrukes til skade for minoriteten. Dette gjelder blant annet forslag om å endre vedtektene, og må ses i sammenheng med at innenfor lovens rammer kan aksjonærrettigheter reguleres gjennom vedtektene i det enkelte selskap. En slik regulering gjennom vedtekter kan for eksempel gjelde regler om aksjeklasser. Det vil si at selskapet har ulike typer aksjer der aksjer i en av selskapets aksjeklasser har én stemme, mens aksjer i en annen aksjeklasse ikke har stemmerett – gjerne kalt A-aksjer og B-aksjer.

Normalt krever vedtektsendring to tredels flertall både av avgitte stemmer og av aksjekapitalen som er representert på generalforsamlingen. Når det kreves at også to tredeler av kapitalen står bak beslutningen, har det sammenheng med at rettighetene også skal tilkomme aksjonærer med aksjer som ifølge selskapets vedtekter er uten stemmerett.

Tilsvarende flertallskrav som for vedtektsendringer må være oppfylt for blant annet:
- Beslutning om å oppløse selskapet
- Beslutning om fusjon (§ 13-10) og fisjon (§ 14-6)
- Styrefullmakt til å forhøye eller sette ned aksjekapitalen
- Styrefullmakt til erverv av egne aksjer
- Beslutning om å sette til side bestemmelser om aksjeeieres fortrinnsrett til å tegne nye aksjer ved kapitalforhøyelse (§ 10-5, jf. § 10-4)
- Beslutning om å ta opp konvertibelt lån (§ 11-2)

I enkelte tilfeller er det satt strengere krav for at en beslutning kan treffes. Dette gjelder for vedtektsendringer som endrer en eller flere aksjeklassers rettsstilling, uten at andre aksjeklassers rettsstilling endres tilsvarende (§ 5-18). Beslutning som forringer en hel aksjeklasses rett, må tiltres av eiere av to tredeler av den representerte kapital i den berørte aksjeklassen. Dessuten må minst halvdelen av stemmene fra de aksjeeiere som ikke eier aksjer i noen annen klasse, være avgitt for forslaget.

I selskaper der aksjer kan skifte eier uten samtykke fra selskapet, kreves det tilslutning fra eiere av aksjer som utgjør mer enn ni tideler av den aksjekapitalen som er representert på generalforsamlingen, samt tilslutning fra minst to tredeler av de avgitte stemmene, dersom

- det for allerede utgitte aksjer skal vedtektsfestes en forkjøpsrett,
- aksjer bare kan erverves med samtykke fra selskapet, eller
- aksjeerverver eller aksjeeiere skal ha visse egenskaper (§ 5-19).

Hvis allerede utgitte aksjer skal være underlagt andre vilkår for omsetning, kreves ikke bare flertall som for vedtektsendring, men også tilslutning fra samtlige berørte aksjeeiere. Aksjeloven krever også at vedtak må fattes med enstemmig tilslutning fra samtlige aksjonærer hvis generalforsamlingen skal treffe beslutning om

- at aksjeeiernes forpliktelser i forhold til selskapet økes,
- at aksjer kan være gjenstand for tvungen innløsning, og
- at forholdet mellom tidligere likestilte aksjer skal endres. Dette betyr at det kreves enstemmighet for et vedtak om at selskapets aksjer skal inndeles i forskjellige aksjeklasser.

Kravet om enstemmighet henger sammen med utgangspunktet i aksjeloven om at hver aksje gir lik rett i selskapet og dermed at en aksjonær ikke må godta at aksjene hans får færre rettigheter enn andre aksjer i selskapet. Kravet gir den enkelte aksjonær mulighet til å forhindre et vedtak som flertallet eller alle andre aksjonærer går inn for.

En aksjonærrettighet knyttet til erverv av aksjer og som har betydning for aksjeeierens innflytelse i selskapet, følger av aksjeloven § 4-26. En aksjeeier som eier 90 prosent av aksjene, kan tvangsinnløse aksjonærminoriteten i selskapet og på denne måten sikre seg full kontroll på alle beslutninger som treffes på selskapets generalforsamling. Motsetningsvis har minoritetsaksjonær rett til å kreve at majoritetsaksjonæren innløser minoritetsaksjonærens aksjer.

I NOU 2023: 28 side 75 gis denne skjematiske oversikten over eierskap, rettigheter og kontroll i et aksjeselskap:

Tabell 8.1 Eierskap, rettigheter og kontroll i et aksjeselskap

Kjøpets størrelse	Rettighet	Innhold	Krav til oppmøte på generalforsamling?
0 prosent	Innsynsrett	I aksjeeierbok I regnskap	Nei
Én aksje	Møterett på generalforsamling Rett til å få tatt opp sak på generalforsamlingen Rett til forholdsmessig andel av utbyttet	Møterett er lovfestet i aksjeloven Innflytelse – får tilgang til den informasjon som gis på generalforsamling Styret foreslår om det skal betales utbytte Rett til utbytte kan begrenses i vedtekter	Ja
Over 10 prosent	Rett til å kreve ekstraordinær generalforsamling (AS) Kan fremme forslag om gransking Kan blokkere innløsning av minoritetsaksjeeiere	Kan kreve at en bestemt sak behandles på ekstraordinær generalforsamling	Nei Krav fremmes overfor styret
Over 1/3	Negativt flertall	Kan forhindre vedtak på generalforsamlingen som krever kvalifisert flertall: endre aksjekapitalen, vedtektsendringer, fusjon og fisjon	Ja
Over 1/2	Simpelt flertall	Alminnelige beslutninger som krever simpelt flertall av de fremmøtte, for eksempel valg av styret	Ja
Minst 2/3	Kvalifisert flertall	Kan gjennomføre vedtak på generalforsamlingen som krever kvalifisert flertall: endre aksjekapitalen, vedtektsendringer, fusjon, fisjon, endre selskapets navn	Ja
Over 90 prosent	Rett til å tvangsinnløse minoritetsaksjeeiere Kan endre rettigheter knyttet til aksjene	Kan tvinge minoritetsaksjeeiere til å selge og bli eneeier Styret i morselskapet beslutter innløsningen	Nei
100 prosent	Fulle eierbeføyelser	Alt ovenfor	Ja

Kilde: NOU 2023: 26 *Investeringskontroll*

8.3 Kilder for norske myndigheters kontroll med eierskap

I NOU 2023: 28 kapittel 4 (side 36) pekes det på at for å få oversikt over hvem som kontrollerer eller har innflytelse over et foretak, er det en forutsetning at man kan identifisere de personene som er reelle rettighetshavere og at det i praksis kan være komplisert å få oversikt over hvem disse er. Med reelle rettighetshavere bruker Investeringskontrollutvalget i denne sammenheng begrepet om den fysiske personen eller de fysiske personene, eller den staten, som i siste instans eier eller kontrollerer en juridisk person[76], enhet eller annen sammenslutning.

Investeringskontrollutvalget fremhever at lange eierkjeder kan være en utfordring i saker hvor eierskap i et foretak kan ha betydning for nasjonale sikkerhetsinteresser, og viser til Nasjonal sikkerhetsmyndighets rapport Risiko 2023 side 16 der det står:

> «Norske virksomheter som forvalter viktige verdier eller har strategisk plassert eiendom bør være oppmerksomme på fordekte investeringer og oppkjøp fra andre land Norge ikke har et sikkerhetssamarbeid med. Slike økonomiske transaksjoner kan skje gjennom stråselskaper og komplekse selskapsstrukturer og kan dermed være vanskelig å avdekke».

Skatteetaten, Kartverket og Brønnøysundregistrene fikk i september 2023 oppdrag av Finansdepartementet (FIN), NFD og Kommunal- og distriktsdepartementet (KDD) om å kartlegge offentlige myndigheters behov for opplysninger om direkte og indirekte eierforhold til aksjer og fast eiendom. Rapporten[77] som ble lagt fram i januar 2024, viser at opplysninger om eierskap er viktig for å utøve en rekke samfunnsoppdrag – herunder samfunnsoppdrag knyttet til stats- og samfunnssikkerhet. Kartleggingen viser at det kan være krevende å skaffe oversikt over viktige opplysninger på en effektiv måte og at det ofte er nødvendig å innhente opplysninger fra flere ulike kilder. Kartleggingen peker på at eierstrukturer kan være komplekse og at det ofte er vanskelig å finne fram til hvem som egentlig eier et aksjeselskap fordi selskapet eies gjennom flere ledd. Kartleggingen viser også at det er utfordrende å identifisere utenlandske eiere.

I punkt 7.1 i NOU 2023: 28 redegjør utvalget for kilder til informasjon om eierskap. Nedenfor følger en beskrivelse hentet fra denne redegjørelsen av ulike kilder som også vil være relevante når det gjelder eierskap i foretak som eier eller råder over kritisk digital kommunikasjonsinfrastruktur, eller har en viktig eller kritisk rolle for utbygging, drift og vedlikehold av slik infrastruktur. I tillegg gis en særlig beskrivelse av registeret over reelle rettighetshavere som ble etablert fra 1. oktober 2024.

Fra NOU 2023: 28 punkt 7.1 siteres følgende:

> «Skatteetatens oversikt over aksjeeiere
>
> Det såkalte aksjonærregisteret i Skatteetaten er utviklet for skatteformål og inneholder opplysninger om aksjeeiere i alle norske aksjeselskaper og utenlandske aksjeselskaper registrert på Oslo Børs.

[76] Rettssubjekt som ikke er en fysisk person, men for eksempel et selskap

[77] Kartlegging av offentlige myndigheters mulige bruk av opplysninger om eierskap til aksjer og fast eiendom https://www.regjeringen.no/globalassets/departementene/fin/2024/kartlegging-eierskapsopplysninger-v-1.0.pdf

Alle aksjeselskaper og allmennaksjeselskaper er forpliktet til å sende inn aksjonærregisteroppgave med informasjon om alle aksjeeiere per 31. desember, senest 31. januar påfølgende år. Registeret oppdateres ikke løpende gjennom året. Registeret skal gi oversikt over innskudd, gevinster, overdragelser osv. Registeret gjelder formelle aksjeeiere (fysisk eller juridisk person som direkte eier). Aksjonærregisteret gir dermed ikke nødvendigvis informasjon om hvem som er reell rettighetshaver.

Aksjeeierregisteret (VPS)

Alle allmennaksjeselskaper skal registreres i en verdipapirsentral. I Norge er det kun Verdipapirsentralen ASA (Euronext VPS). Aksjeselskaper med mange eiere kan også velge å registrere aksjene i Euronext VPS.

Registrering i VPS skal dokumentere eierskap, og gir selskapet oversikt over aksjeeiernes kontaktinformasjon. Hvis selskapet er registrert i norsk verdipapirsentral, skal registrering også gi rettsvern (sikre rettigheten mot tredjeparter). VPS gjelder formelle aksjeeiere (fysisk eller juridisk person som direkte eier).

Utenlandske aksjeeiere kan velge å registrere eierskapet gjennom en forvalter. Det vil da være forvalterens navn som står oppført som eier av verdipapiret. Forvalter kan motta meldinger, bistå med kommunikasjon og bistå med informasjon om rapporteringsforpliktelser e.l. Forvalter er ofte en bank eller en annen finansinstitusjon som er godkjent av Finanstilsynet. Forvalter har ikke eierskap til aksjen. Forvalter er forpliktet til å oppgi informasjon om reell eier på forespørsel, og om nødvendig innhente opplysninger fra andre forvaltere i kjeden.

Aksjeeierbok

Ifølge aksjeloven er alle norske aksjeselskaper forpliktet til å holde en til enhver tid oppdatert aksjeeierbok, hvis de ikke vedtektsfester å ha aksjeeierregister. Denne oppbevares hos selskapet selv, regnskapsfører eller annen leverandør. Aksjeeierboken dokumenterer aksjeeiere (fysisk eller juridisk person som direkte eier). Registrering i aksjeeierboken gir rettigheter «som tilkommer en aksjeeier», men gir ikke rettsvern. Disse kan også oppnås ved at eierskapet er meldt og godtgjort, ikke avhengig av innføring i aksjeeierboken.

Foretaksregisteret

Brønnøysundregistrene utvikler og driver flere registre, herunder Foretaksregisteret. Foretak som driver næringsvirksomhet i Norge, plikter å oppdatere informasjonen i Foretaksregisteret ved endringer. Registeret skal gi oversikt over hendelser i aksjeselskaper og allmennaksjeselskaper m.fl., som kapitalendringer, vedtekter, styreendringer og lignende.

Foretaksregisteret inneholder informasjon om hvem som stiftet aksjeselskapet, dvs. aksjeeiere på opprettelsestidspunktet, foretaksregisterloven § 4-4 jf. aksjeloven § 2-3. Foretaksregisteret inneholder også informasjon om deltakerne

i ansvarlige selskaper. Foretaksregisteret inneholder ikke opplysninger om eiere utover dette.

Foretaksregisteret inneholder blant annet følgende informasjon: Selskapets vedtekter, styremedlemmer og eventuelt varamedlemmer, og hvem som er styrets leder, daglig leder, hvem som representerer selskapet utad og tegner dets firma. Foretaksregisteret viser om selskapet er unntatt fra revisjonsplikt.

Grunnboken (Statens kartverk)

Grunnboken er et offentlig register som viser tinglyste rettigheter og forpliktelser i eiendom. Grunnboken viser hvem som er tinglyst eier av eiendommen. Den viser også eventuelle pengeheftelser, erklæringer og avtaler, eller om andre eiendommer eller personer har tinglyste rettigheter på eiendommen.

Statens kartverk fører også det offisielle eiendomsregisteret (matrikkelen). Matrikkelen omfatter ca. 3,3 millioner eiendommer, 4,3 millioner bygninger, 2,6 millioner boliger og 2,5 millioner veiadresser. Matrikkelen inneholder registrert eiers eller festers navn eller organisasjonsnummer. Matrikkelen inneholder også opplysninger om eiendomsgrenser, adresser, bygninger, boliger og gårds- og bruksnummer. Informasjonen omfatter også historiske opplysninger fra grunnboken.»

Lov om register over reelle rettighetshavere ble vedtatt i 2019 og formålet med loven er å sikre økt åpenhet om norske virksomheters eierstrukturer og gi bedre oversikt over utenlandske eiere av norske selskaper.

Reelle rettighetshavere er de fysiske personene som i siste instans eier eller kontrollerer en juridisk person, arrangement, enhet eller annen sammenslutning. En reell rettighetshaver er ifølge dette regelverket en fysisk person som gjennom sin eierandel eller stemmeandel i virksomheten, kontrollerer virksomheten. Andelen må overstige 25 prosent. Også en fysisk person som har rett til å utnevne eller avsette minimum 50 prosent av medlemmene i virksomhetens styrende organer, anses å være en reell rettighetshaver. Det skal også innhentes og registreres opplysninger om personer som på annen måte utøver kontroll over virksomheten. Regelverket vil bidra til å motvirke misbruk av de aktuelle virksomhetene til hvitvasking, terrorfinansiering og økonomisk kriminalitet.

Registeret skal inneholde opplysninger om reelle rettighetshavere samt hvilken måte de kontrollerer den registreringspliktige på, det vil si om det er gjennom eierskap, stemmerett eller annen måte. Det betyr at hvis det er relevant, må registreringspliktige innhente opplysninger om eventuelle formelle eller uformelle avtaler som regulerer utøvelsen av eierrettigheter og stemmerettigheter i den registreringspliktige virksomheten. Registreringen skal angi om det er direkte eller indirekte eierskap, altså om det foreligger mellomliggende norske eller utenlandske foretak. Eies eierandelen gjennom et annet foretak, skal navn og organisasjonsnummer på mellomliggende foretak registreres. På denne måten gir registeret bedre oversikt over selskapsstrukturen.

Registreringspliktige virksomheter skal registrere reelle rettighetshavere. Med registreringspliktige menes juridiske personer, enheter og andre sammenslutninger

og forvaltere av utenlandske truster og lignende juridiske arrangementer som driver virksomhet i Norge[78]. Det er altså foretaket selv som skal identifisere og registrere reelle rettighetshavere, og både navn, fødselsnummer/D-nummer, bostedsland og statsborgerskap skal registreres. Har ikke rettighetshaveren fødselsnummer eller D-nummer, skal fødselsdato registreres.

Registreringspliktig skal dokumentere grunnlaget for identifisering av den reelle rettighetshaveren. Mener den registreringspliktige at det ikke finnes noen reell rettighetshaver, skal det også begrunnes og dokumenteres.

Registeret – som driftes av Brønnøysundregistrene[79] – åpnet mulighet til å starte registrering 1. oktober 2024. For at virksomhetene skal få tid til å innrette seg, er det en innfasingsperiode fram til 31. juli 2025 for virksomhetene til å gjennomføre registreringen.

Regelverket legger til rette for et register som gir visse offentlige myndigheter tilgang til opplysninger om hvem som i realiteten har kontroll over foretak. Informasjon fra registeret er tilgjengelig for følgende myndigheter, jf. forskriften § 3-11:

a. Politi- og påtalemyndighet
b. Enheten for finansiell etterretning ansvarlig for å motta opplysninger om mistenkelige forhold etter hvitvaskingsloven § 26
c. Skattemyndigheter
d. Tilsynsmyndigheter for rapporteringspliktige etter hvitvaskingsregelverket
e. Andre myndigheter med ansvar for å etterforske og påtale hvitvasking, primærforbrytelser og terrorfinansiering
f. Andre myndigheter med ansvar for sporing, båndlegging og inndragning av utbytte
g. Sikkerhetsmyndigheten
h. Tilsynsmyndighet for stiftelser

Forskriften gir altså «sikkerhetsmyndigheten» tilgang til opplysninger. Et departement er ansvarlige for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder. Begrepet «sikkerhetsmyndigheten» er i forskriften tatt inn i entallsform – i motsetning til «skattemyndigheter» – noe som kan tilsi at «sikkerhetsmyndigheten» kun omfatter NSM. Ordlyden i forskriften skaper usikkerhet om for eksempel et departement som er sektormyndighet etter sikkerhetsloven, anses som «sikkerhetsmyndigheten» i denne sammenhengen og kan innhente opplysninger fra registeret. På denne bakgrunn har utvalget følgende anbefaling:

> **«Utvalget mener at Finansdepartementet må klargjøre hvem som etter dagens regelverk vil kunne få adgang til registeret over reelle rettighetshavere, knyttet til oppgaver etter sikkerhetsloven. Hvis dagens regelverk ikke åpner for at et departement som har sektoransvar etter sikkerhetsloven får tilgang til opplysninger, bør forskriften til lov om register over reelle rettighetshavere endres, slik at alle myndigheter som har sektoransvar etter sikkerhetsloven, gis tilgang til opplysninger fra registeret.»**

[78] Lov om register over reelle rettighetshavere § 3, jf. § 2. Unntak fra registreringsplikten følger av forskrift til lov om register over reelle rettighetshavere § 1-2.

[79] https://www.brreg.no/reelle-rettighetshavere/

8.4 Hva er spesielt med utenlandsk eierskap?

8.4.1 Innledning

Utvalget har tidligere, særlig i kapittel 4, drøftet hvordan utenlandsk eierskap kan svekke nasjonal kontroll. Formålet med det utenlandske eierskapet kan i ekstreme tilfeller være sikkerhetstruende (jf. punkt 4.2.3). Imidlertid har utvalget også påpekt at de aller fleste utenlandske eiere ikke vil ha slike hensikter, men ha normale forretningsmotiver. Utvalget tar nå sistnevnte utgangspunkt og prøver å se nærmere på hva som likevel kan gi opphav til bekymring ved utenlandsk eierskap. Følgelig drøftes altså hva som synes å være kildene til at utenlandsk eierskap kan svekke nasjonal styringsevne selv om den utenlandske aktørens motiv er legitimt. Det bidrar også til at man får fram hvilke kilder som kan gjøre norske eiere utsatt for utilbørlig press fra en utenlandsk statsledelse.

Diskusjonen her komplementerer den som er skrevet i 4.3 om økonomisk aktivitet som kan ha kontrollsvekkende effekt. Der er fokuset primært på organisatoriske forhold og eierskapsformer, mens her ser utvalget kun på eierskapets nasjonale tilknytning. Nærmere bestemt går man inn på de markedsmessige, økonomiske, juridiske og sikkerhetsmessige sidene ved utenlandsk eierskap i aksjeselskaper som kontrollerer kritisk digital kommunikasjonsinfrastruktur.

I de fleste tilfeller skulle det ikke være noen forskjell på nasjonalt eller utenlandsk eierskap så lenge alt annet enn nasjonaliteten til eierne er likt. Dersom eierne er frie og har samme formål – for eksempel profittmaksimering – og samme perspektiv, skulle de typisk treffe tilsvarende avgjørelser, for eksempel hva angår å opprettholde selskapets leveranseforpliktelser overfor sine kunder og gjøre investeringer i utvikling av selskapets tjenester for framtiden.

Åpenbart kan offentlige, utenlandske eiere (altså ikke private) ha andre formål enn profittmaksimering. I tillegg kan de være del av eller kontrollert av den utenlandske statsledelsen. Selv om formålet opprinnelig skulle vært profittmaksimering, kan statsledelsen formodentlig selv endre sitt formål. Således kan den utenlandske statsledelsen potensielt bruke sitt eierskap til å fremme sin egen nasjon sine interesser i strid med høyest mulig avkastning for det aktuelle selskapet og i strid med norske sikkerhetsinteresser.

Det kan også forekomme politiske systemer som gjør at avstanden mellom myndigheter og private selskaper fra samme land blir kort og at skillet mellom offentlige og private selskaper blir uklart. Det vil si at myndighetenes innflytelse over private selskaper er betydelig og målsettingen sammenfaller mer med myndighetenes mål. Et eksempel på dette er følgende beskrivelse av det politiske systemet i Russland fra Bergen Engines-vedtaket (Kongelig resolusjon, 21/1898, s. 3):

> «Russland har et politisk system med en tett sammenblanding mellom politikk og økonomi, mellom statlig og privat virksomhet, og mellom sivile og militære sfærer. De russiske etterretnings- og sikkerhetstjenestene griper dypt inn i alle samfunnssektorer. Det er i liten grad formålstjenlig å skille mellom statlige og private interesser og aktiviteter i Russland når det gjelder vurderinger som har betydning for Norges nasjonale sikkerhet. Russiske myndigheter bruker en stor

bredde av virkemidler for å understøtte statlige målsettinger, inkludert sivile selskap og andre næringslivsaktører.»

Det er ganske åpenbart at selskaper som den utenlandske statsledelsen kontrollerer enten direkte gjennom sitt eierskap eller grunnet uvanlig tette forbindelse som nevnt foran. Her velger utvalget derfor å fokusere på private utenlandske selskaper med en armlengde avstand til sin statsledelse, altså med hva man i Norge ville tenke på som en normal uavhengighet fra statsledelsen.

I drøftingen forutsettes så langt mulig at alt annet er likt utenom at nasjonaliteten til eierskapet er utenlandsk istedenfor norsk. Med alt annet likt menes, for eksempel, at eierne har identisk kompetanse, identiske eierandeler i det aktuelle og andre, relaterte selskaper, og at ikke slike forskjeller gir insentiver til å opptre forskjellig.[80] Dette er selvsagt stilisert, men vil bidra til å holde fokuset på nasjonalitetsdimensjonen (andelen utenlandsk eierskap). Det legges til grunn at både utenlandske og norske private eiere er profittmaksimerende, altså at de søker å maksimere avkastningen på sin investering.[81] Det forutsettes videre at eierne er uavhengige av staten i den forstand at staten ikke er medeier i selskapet eller har særlige bindinger til selskapet eller dets eiere. Utvalget søker altså å isolere betydningen av at det kun er eierens nasjonalitet som er forskjellig i drøftingen. Dette gjøres for å tydeligere belyse årsakene til at utenlandsk privat eierskap påvirker nasjonal kontroll.

Det kan være flere årsaker til at utenlandsk privat eierskap, selv med slik armlengde avstand, gir den utenlandske statsledelsen mer innflytelse enn om samme eierandel var eiet av norske private, noe som medfører økt risiko og redusert norsk nasjonal kontroll. Eksempler på slike årsaker kan være at utenlandske eiere er:

- lovpålagt å samarbeide
- mer avhengige av sin nasjon
- lojale mot sin nasjon

[80] Eierne kan alle være profittmaksimerende, men de kan ha forskjellige perspektiver. For eksempel, noen kan ha et kortsiktig perspektiv, mens andre er langsiktige eiere. Noen kan også eie relatert virksomhet og oppnå indirekte gevinster fra selskapet derigjennom og derfor ha andre interesser enn dem som kun er aksjonærer i selskapet.

[81] Dette behøver ikke alltid være tilfelle. Stiftelser vil eksempelvis ofte ha andre formål. Eiere av aksjeselskaper kan også ha andre formål som det kan være vanskelig å avdekke, noe som kan være utfordrende når de får kontroll gjennom høy eierandel (derav aksjelovens beskyttelse av minoritetsaksjonærer nevnt tidligere). Uansett må selskapet over tid oppnå tilstrekkelig lønnsomhet til å kunne dekke sine kostnader eller få tilført ny kapital for ikke å gå konkurs.

8.4.2 Lovpålagt innflytelse

Den utenlandske statsledelsen kan ha større innflytelse og kontroll dersom eieren er et privat selskap eller personlige eiere fra den utenlandske statsledelsens land og derfor underlagt den utenlandske statsledelsens jurisdiksjon. I noen tilfeller har den utenlandske statsledelsen eksplisitt innflytelse over egne statsborgere ved lov, jf. Waage et al. 2021 (FFI-rapport 20/03149), s. 63:

> «Enkelte land, herunder Kina, har sikkerhetslovgivning som pålegger kinesiske borgere i utlandet å samarbeide med kinesiske sikkerhetstjenester. På den måten kan en kinesisk samarbeidspartner bli satt under betydelig press for å samarbeide, og kan i praksis ha få muligheter til å nekte. Mange amerikanske selskaper har også rapportert om tilsvarende press fra amerikanske myndigheter, hjemlet i amerikansk sikkerhetslovgivning (Normann 2020).»

Dette er juridiske sider ved utenlandsk eierskap som vil kunne øke trusselen fra et utenlandsk eierskap relativt til et norsk eierskap, ved at en utenlandsk stat får økt beslutningsdyktighet over kritisk digital kommunikasjonsinfrastruktur i fred, krise og krig, på bekostning av Norges nasjonale sikkerhetsinteresser.

8.4.3 Avhengighet

Utenlandske eiere (juridiske og fysiske personer) vil typisk ha en større avhengighet til sin nasjon og derigjennom kunne være mer utsatt for press eller tvang fra sin statsledelse, også i fravær av et lovpålegg om å samarbeide.

Statsborgere har normalt en rettighetsavhengighet til sitt land hvor de har rettigheter som følger av statsborgerskapet, som for eksempel rett til permanent opphold, til å ta arbeid, til å eie eiendom, til sosiale ytelser, med mer. Motsvarende har de typisk færre og mer begrensede slike rettigheter i land hvor de ikke er statsborgere, eksempelvis begrenset oppholdstillatelse. Derfor kan de være mer utsatt for press fra sitt hjemlands statsledelse enn fra et annet lands statsledelse. De må typisk oppholde seg mest i sitt hjemland og er under sitt hjemlands jurisdiksjon. En statsledelse kan kreve dem utlevert til sitt hjemland under visse omstendigheter. Denne avhengigheten til hjemlandet, hvor de har sitt statsborgerskap, vil således kunne gjøre dem mer utsatt for press fra sitt hjemlands statsledelse.

Normalt vil det også foreligge ressursmessige avhengigheter, dersom man har betydelige eiendeler i sitt hjemland som er immobile, som fast eiendom. I tillegg er det gjerne også sosiale avhengigheter knyttet til familie og venner som følge av å være født og oppvokst i et land. Disse avhengighetene kan gjøre en person mer sårbar for sin statsledelses bruk av press. Selv om disse to avhengighetene normalt er knyttet til landet hvor man har statsborgerskap, kan også slike avhengigheter gjelde norske statsborgere som har bodd lenge i et annet land enn Norge. De kan også gjelde i mindre grad for utenlandske statsborgere som i liten grad har bodd i sitt hjemland.

For selskaper vil det også kunne foreligge en viss juridisk avhengighet knyttet til sitt hjemland (hvor de har registrert sitt hovedkontor), eksempelvis skatteplikter eller nødvendige tillatelser, konsesjoner og lignende knyttet til virksomheten. I tillegg kommer

ressursmessige avhengigheter eller bindinger som ofte følger av at et utenlandsk selskap normalt har virksomhet i sitt hjemland. For eksempel, dersom selskapet har betydelige verdier i hjemlandet som både er lite mobile og vanskelig omsettelige. Merk at slike avhengigheter også vil kunne gjelde norske selskaper som har investert betydelig i utlandet. Det vil kunne gjøre et norsk selskap utsatt for press fra den utenlandske statsledelsen.

Avhengigheten til selskaper kan også være knyttet til markeder eller kundesiden (analogt til på leverandørsiden, jf. fokuset på avhengighet til utenlandske leverandører omtalt tidligere). En norsk bedrift som eksporterer det meste av sin produksjon til et bestemt utland, eller har virksomhet i utlandet, vil kunne tape mye dersom de står i fare for å miste tilgang til det markedet. Derigjennom vil selskapet kunne være utsatt for press fra landets statsledelse, eksempelvis for tilgang til å selge i landet eller drive virksomhet der. Mange selskaper er multinasjonale med avhengigheter til flere land, både på leverandørsiden, i forhold til i hvilke land de har sine egne ressurser lokalisert, samt på markedssiden i forhold til land hvor de selger det meste av sin produksjon.

8.4.4 Lojalitet

Statsborgere – både utenlandske og norske – vil generelt føle en lojalitet og tilhørighet til egen nasjon, noe som gjør at de gjerne ønsker å samarbeide med sin statsledelse til fordel for sin egen nasjons interesser, selv i fravær av et lovpålegg eller press om dette.[82] Lojaliteten kan være knyttet til et språklig og kulturelt fellesskap, til sosiale relasjoner med andre statsborgere (som familie, venner og bekjente), med videre. Det kan også henge sammen med ressursmessige og sosiale avhengigheter nevnt foran og en interesse av å beskytte sine verdier i eget hjemland. Dette kan gjøre utenlandske eiere mer tilbøyelige til å samarbeide med sitt hjemlands statsledelse i strid med norske interesser og derigjennom utgjøre en økt risiko mot nasjonal sikkerhet. En slik lojalitet kan imidlertid også forekomme hos norske statsborgere som, for eksempel, har tilbragt mye tid i et annet land og fått en tilhørighet der. En slik lojalitet kan gjøre at eiere kan treffe avgjørelser til fordel for et annet land og som kan redusere avkastningen til selskapet. En slik lojalitet kan muligens også øke faren at eiere blir mottagelige for kompensasjon eller bestikkelser.

8.4.5 Bestikkelser og økonomisk press

Den utenlandske statsledelsen kan i hvert av tilfellene over hvor den utnytter en årsak eller kilde til innflytelse over private utenlandske eiere (lovpålegg, avhengighet, lojalitet), også kompensere dem for eventuell tapt avkastning eller andre kostnader slik at de private eierne ikke blir økonomisk skadelidende. En kompensasjon til eieren for å treffe ugunstige avgjørelser for seg selv og selskapet, ville kunne kategoriseres som belønning av lojalitet eller kompensasjon/bestikkelse. Statsledelsen kan utnytte en kombinasjon av årsakene samtidig til å utøve innflytelse, som trusler om press og lovnad om belønning.

[82] Det betyr også at de kan handle på eget initiativ, ikke på vegne av instrukser fra sin statsledelse.

En statsledelse kan ty til mange former for bestikkelser eller belønning for samarbeid til private eiere. Eksempler inkluderer tilskudd og andre direkte betalinger, skattelettelser, ettergivelse av gjeld, fordelaktig behandling i regulatoriske saker (eksempelvis tildeling av konsesjoner/driftstillatelser), subsidier i naturalier, fordelaktig finansiering fra statlige (eller statsstøttede) finansinstitusjoner, privilegert tilgang til informasjon, eksplisitt eller implisitte garantier, fordelaktig behandling ved offentlige anskaffelser, støtte i form av kommersielt diplomati og unntak fra antitrusthåndhevelse eller konkursregler.[83] Slike fordeler kan også tildeles andre selskaper som de private eier, i bytte for samarbeid i selskapet som eier kritisk digital kommunikasjonsinfrastruktur.

De fleste av fordelene nevnt foran kan statsledelsen også bruke med motsatt fortegn for å presse private eiere til å samarbeide. For eksempel en trussel om ufordelaktig behandling ved offentlige anskaffelser.

Her kan det igjen være på sin plass å minne om at også norske selskaper eller eiere som har en avhengighet til utlandet, kan være utsatt for en del av de samme pressmidlene fra den utenlandske statsledelsen. Det er selvsagt også slik at det finnes eiere som ut fra selviske hensyn er tilbøyelige til å bli bestukket, helt uavhengig av nasjonalitet.

8.4.6 Forsterkende faktorer

Noen faktorer kan potensielt forsterke risikoen knyttet til utenlandsk eierskap som skyldes en av de tre grunnleggende årsakene; lovpålegg, avhengighet og lojalitet. En slik faktor er at utenlandske eiere kan lettere unndra seg norsk jurisdiksjon. Dette kan redusere nedsiden for utenlandske eiere ved ulovlige handlinger i Norge (f.eks. tyveri av informasjon eller sabotasje) på vegne av en utenlandsk statsledelse.[84] Merk at også norske eiere kan prøve å unndra seg håndhevelse av norsk jurisdiksjon ved å flytte utenlands, og eventuelt få nytt statsborgerskap. Dette vil imidlertid være mer krevende slik at det er større risiko ved utenlandsk eierskap, alt annet likt.

En annen faktor er at eiere kan ha en (ubevisst) preferanse for å samarbeide og samhandle med lignende personer («similarity attraction»), eksempelvis med samme nasjonalitet, kultur og språk. Dette kan gjøre at utenlandsk eierskap øker sannsynligheten for at det også blir flere utenlandske statsborgere ansatt i eller tilknyttet selskapet.[85] Det kan igjen øke muligheten for en utenlandsk statsledelse til å utøve innflytelse grunnet årsakene nevnt foran (lovpålegg, avhengighet og lojalitet).

Utvalget vil nå se på hvilke trusler mot nasjonal sikkerhet denne innflytelsen kan brukes til. Trusler er nevnt tidligere, eksempelvis i punkt 4.2, men vil her knyttes mer direkte opp mot utenlandsk kontra norsk eierskap.

---

[83] De fleste formene for fordelaktig behandling er nevnt i Cai og Li (2019), men da i forhold til offentlige eide selskaper.

[84] Når salget av Bergen Engines AS ble stanset, var noen av begrunnelsene i forslaget til vedtak faren for ulovlige handlinger som omgåelse av eksportregelverk samt etterretning og sabotasje. (Kongelig resolusjon, ref. nr. 47, saksnr.: 21/1898, av 26. mars 2021 https://www.regjeringen.no/contentassets/e775dc91a33e4713a090da7398e6f3f5/endelig-godkjent-kgl.res.-stans-av-salget-av-bergen-engines-as.pdf)

[85] Selv om vi legger til grunn at private eiere søker å opptre rasjonelt og profittmaksimerende, åpner vi for at de kan være ubevisst påvirket av oppfatninger som gir skjevheter i deres beslutninger («bias»).

8.4.7 Fra eierskap til trusler mot nasjonal sikkerhet

Med eierskap følger kontroll og muligheten til å påvirke kritisk digital infrastruktur som nevnt innledningsvis i kapittelet. Videre vil utenlandsk eierskap kunne gi en utenlandsk statsledelse økt innflytelse i forhold til om samme eierandelen var norsk eier som diskutert foran. Denne innflytelsen eller kontrollen kan en utenlandsk statsledelse bruke til å arbeide langsiktig i fredstid for å svekke nasjonal sikkerhet i tilfelle en eventuell fremtidig krise eller konflikt. Innflytelsen vil også kunne brukes mer akutt i en krise eller konflikt til å skade funksjoner som er kritiske for norsk samfunn, som kritisk digital kommunikasjonsinfrastruktur.

Det er flere typer risiko for eller trusler mot nasjonale sikkerhetsinteresser. Disse inkluderer (Moran 2009, NOU 2023: 28, Waage et al. 2021):

1. tilgang til og kontroll med kunnskap, informasjon, infrastruktur og/eller eiendom
    a. infiltrasjon (forberede sabotasje)
    b. overvåking og informasjonslekkasje
    c. overføring av kapasitet og kompetanse til utenlandsk eiers hjemstat
    d. utkontraktering og nedbygging av kapasitet og kompetanse i Norge
2. påvirkning av norske politikere eller andre sentrale aktører til å endre beslutninger, eller motivere oppførsel og beslutninger som er fordelaktige for hjemstaten til eier
3. bortfall av varer, tjenester eller kompetanse (typisk høyt i krisespennet)
    a. leveransenekt (kritiske ressurser er ikke i Norge)
    b. sabotasje (kritiske ressurser er i Norge)

Utvalget minner om at vårt fokus er på hvilken ytterligere innflytelse en utenlandsk statsledelse kan oppnå gjennom utenlandsk privat eierskap kontra at samme eierandel hadde vært norskeid. Det er ikke nødvendigvis slik at risikoen vil være lav dersom eierne er norske. Som nevnt tidligere kan også norske eiere ha avhengigheter til utlandet som gjør dem utsatt for press, eller de kan føle lojalitet med eller sympatisere med utenlandske nasjoner, eller simpelthen være tilbøyelige til å motta bestikkelser eller oppnå fordeler fra utlandets statsledelse. Dette kan kanskje særlig gjelde lavt i krisespennet når en mulig konflikt, krise eller krig synes fjernt. Under drøftes kort noen av truslene knyttet til økonomisk aktivitet.

Dersom ressurser som er kritiske for digital kommunikasjonsinfrastruktur flyttes utenlands, for eksempel gradvis over tid gjennom utkontraktering, reduseres nasjonal kontroll. Utenlandsk eierskap med bestemmende innflytelse vil kunne øke sannsynligheten for at ressurser flyttes ut av Norge og dermed faller utenfor norsk kontroll.[86] Det er imidlertid viktig å være oppmerksom på at profittmaksimerende eiere kan treffe avgjørelser som svekker nasjonal kontroll, uavhengig av deres nasjonalitet. Dersom et selskap kunne øke lønnsomheten ved å flytte deler av produksjonen til et lavkostland eller endatil flytte hovedkontor til et land med lavere selskapsskatt, så ville både utenlandske og norske profittmaksimerende eiere ha insentiv til å flytte ut virksomhet. Slik utflytting vil derfor også kunne skje under norsk eierskap, men sannsynligheten kan kanskje være noe lavere dersom norske eiere har en preferanse for å ha virksomhet i Norge, for eksempel grunnet lojalitet.

[86] Dette vil kanskje være spesielt aktuelt dersom utenlandske eiere kommer fra et lavkostland og dermed også har høyere språklig og kulturell kompetanse til å flytte virksomhet dit (jf. Gerbl, M., McIvor, R., & Humphreys, P. (2016). Making the business process outsourcing decision: why distance matters. International Journal of Operations & Production Management, 36(9), 1037-1064.).

Uavhengig av nasjonaliteten til profittmaksimerende eiere, ville en slik utflytting av aktiviteter og ressurser fra Norge svekke nasjonal kontroll over de utflyttede ressursene.

Bortfall av kritiske tjenester grunnet leveransenekt kan være en alvorlig trussel. Et eksempel på bekymringen for et slikt bortfall av samfunnskritiske tjenester grunnet utenlandsk eierskap er uttrykt slik i Waage et al. (2021, s. 48):

> «Muligheten til å stenge ned telekomtjenester for hele landet og slik utøve press, var blant annet en bekymring i Nederland i kjølvannet av det meksikanske selskapet America Móvil sitt forsøk på å kjøpe opp hele det nederlandske telekomselskapet KPN (Retter et al. 2020).»

Som nevnt tidligere, er det imidlertid i utgangspunktet ingen grunn til at en profittmaksimerende utenlandsk eier skulle ha større insentiv til å stenge ned tjenester og utøve press, enn en norsk eier. Den ville jo tape lønnsomhet på å stenge ned. Om den er under innflytelse (kontroll) fra egen statsledelse som er i konflikt med Norge, kan dette endre seg og den vil kunne bli presset til eller kompensert for å treffe ulønnsomme avgjørelser, som å stenge ned. Som nevnt tidligere, er det derfor tvang, press fra den utenlandske eierens statsledelse og politikere eller økt tilbøyelighet til å samarbeide ut fra lojalitet, som er kilden til bekymring fordi dette kan medføre sikkerhetstruende avvik fra normal profittmaksimering.[87] Bortfall av tjenester, for eksempel gjennom leveringsnekt, ville gjerne være spesielt aktuelt høyere opp i krisespennet. Om alle nødvendige ressurser for drift befinner seg i Norge, eksempelvis ved beredskapslagre, personell med nødvendig kompetanse, med videre, så vil norske myndigheter likevel kunne gripe inn og gjenoppstarte driften.

En annen utfordring er at norske selskaper kan være utsatt for utenlandsk innflytelse indirekte ved at de er avhengige av innsatsfaktorer fra en internasjonal verdikjede hvor det er utenlandske eiere. Da kan det være krevende både å ha oversikt over eierskapet og avgrense tydelig hvor i verdikjeden man tillater utenlandsk eierskap. Videre kan det være at norsk eierskap av viktige deler av en slik internasjonal verdikjede ikke helt løser utfordringen. Som nevnt tidligere kan norske selskap være eksponert for økonomisk press fra andre land de har betydelig eksport til eller virksomhet i (f.eks. utenlandsk datterselskap). Waage et al. (2021) påpeker at dette er et viktig område, men som de ikke har hatt mulighet til å drøfte innenfor sin rapport. Utvalget går i noen grad inn på verdikjedeproblematikken i kapittel 6 ved at man spør om hvem eierne av underleverandører er og hvor disse er hjemmehørende.

Utvalget har nå sett på negative sider ved utenlandsk eierskap, men det vil også være negative sider ved å begrense utenlandsk eierskap.

[87] Med normal i denne sammenheng menes hva som ville skjedd i fravær av en slik innflytelse, altså når eieren er uavhengig og fri.

8.4.8 Negative sider ved begrensninger på utenlandsk eierskap

Begrensninger på utenlandsk eierskap vil redusere tilgangen til finansiell kapital, fysisk kapital (teknologi) og human kapital (ekspertise). I utvalgets spørreundersøkelse av og dialog med aktørene (vedlegg 5) har flere aktører påpekt bekymringer for redusert tilgang til alle tre typene kapital. Særlig kan særnorske regler for ekomsektoren ha negativ innvirkning på kapitaltilgang, innovasjon, teknologitilgang, utvikling og effektiv drift. Aktører bemerket også at slike regler kan svekke konkurranseevnen og markedsadgangen for selskaper i sektoren. Ettersom begrensninger på utenlandsk eierskap vil kunne ha negative effekter på utviklingen av og kvaliteten på digital kommunikasjonsinfrastruktur, må disse balanseres opp mot sikkerhetshensynet.

Norge har tradisjonelt vært i en gunstig situasjon i forhold til finansiell kapitaltilgang (NOU 2018: 5 *Kapital i omstillingens tid – Næringslivets tilgang til kapital*). Det er en betydelig andel utenlandsk eierskap i norsk næringsliv, og enda større innen digital kommunikasjonsinfrastruktur, hvor Menons undersøkelse indikerer en utenlandsk eierandel på om lag 50 prosent for selskaper som eier kommunikasjonsinfrastruktur og enda høyere for deres underleverandører. Imidlertid gjelder eierbegrensningen typisk ikke land som Norge har et sikkerhetssamarbeid med.[88] Videre har begrensninger i utenlandsk eierskap *de facto* vært på plass i mange år allerede. Menons kartlegging av utenlandsk eierskap i kritisk digital infrastruktur indikerer at begrensningen har fungert i den forstand at det ikke er noe utenlandsk eierskap som gir grunn til bekymring per i dag.[89]

Av de tre typene kapital er finansiell kapital meget mobil og relativt lett å substituere, mens de to andre typene kapital er mindre mobile og kan være vanskelige å substituere. Sagt annerledes, et lån fra ett land kan antagelig enklere refinansieres med et lån med tilsvarende vilkår fra et annet land, enn man kan bytte leverandør av utstyr eller tilgang til kompetanse.

Generelt vil handel med utlandet gjøre at Norge kan dra nytte av komparative fortrinn og stordriftsfordeler, slik at selv om man i teorien kunne produsere noe nasjonalt, vil det være betydelig gunstigere å kjøpe dette fra utlandet. Deler av kritisk digital infrastruktur er meget teknologitung og det kreves store, ofte irreversible, investeringer i forskning og utvikling, samt gjerne også i produksjonsutstyr, for å følge med i utviklingen. Dette gir opphav til stordriftsfordeler som gjør det naturlig at slike produktmarkeder blir internasjonale og domineres av noen få, store aktører. Et eksempel på dette er mobilnett, nå i sin femte generasjon (5G). Utvikling av programvare for digital kommunikasjon kan være et annet eksempel. For programvare kan utviklingskostnaden være meget høy, samtidig som det koster lite å distribuere programvaren til brukere. Denne kostnadsstrukturen – høye faste og irreversible kostnader kombinert med lave variable kostnader – gir opphav til stordriftsfordeler, som igjen kan føre til at markedet blir konsentrert med et fåtall store aktører. I møte med slike stordriftsfordeler vil det gjerne være økonomisk uoppnåelig for de fleste små land å oppnå digital suverenitet og uavhengighet kun basert på sin egen etterspørsel. Selv om store land har bedre mulighet til dette simpelthen fordi de utgjør større markeder, vil det også for disse kunne medføre

[88] I Bergen Engines vedtaket ble det eksempelvis fremhevet at (s. 6): «Selskaper kontrollert av en stat vi har sikkerhetssamarbeid med, er ikke berørt av vedtaket. Det er altså fortsatt et stort kapitalmarked som vil kvalifisere som eier.»

[89] Menons vurdering er at det i kartleggingen ikke er avdekket eierforhold som fremstår som problematiske, bortsett fra eierskapet til Huawei (som allerede er godt kjent for norske myndigheter).

tap av stordriftsfordeler å skulle insistere på nasjonal produksjon for å sikre full nasjonal kontroll på alle områder, med mindre de også kan selge til andre land og derigjennom oppnå økte stordriftsfordeler.[90]

Steen (2022, FAFO Rapport 2022:22) påpeker at tyske myndigheter allerede i 2011 startet en prosess for å etablere en nasjonal, offentlig kompetanse og kapasitet for skyløsninger. Selv om dette er kostbart å utvikle og etablere, kan antagelig en stor nasjon som Tyskland like fullt oppnå en rimelig grad av stordriftsdeler ved at kostnaden kan spres over et stort antall offentlige virksomheter og innbyggere. En slik strategi om digital suverenitet og autonomi kan derfor svare seg i et sikkerhetsperspektiv. Det vil si at tapet av stordriftsfordeler oppveies av gevinsten ved økt nasjonal kontroll.

Norge er derimot et lite land og vil antagelig ikke kunne oppnå i nærheten av samme skala-fordeler. Derfor vil en slik strategi typisk bli for kostbar og Norge vil i større grad måtte akseptere utenlandsk eierskap og avhengighet. Det vil igjen bety redusert nasjonal kontroll. Imidlertid vil det å inngå sikkerhetssamarbeid og allianser med andre land øke det markedet Norge er en del av. Innenfor en allianse kan dermed små land samle sin etterspørsel for derigjennom å oppnå stordriftsfordeler i fellesskap. Produsenter kan gjerne komme fra små land, som eksempelvis 5G-produsentene Nokia (Finland) og Ericsson (Sverige), men det som gjør at de blir store og er blant et fåtall internasjonalt ledende leverandører, er nettopp at de har vunnet fram i en internasjonal konkurranse om store volum. Tilgangen til et stort marked, øker sjansene for å oppnå stordriftsfordeler.

Allianser som NATO eller unioner som EU, utgjør relativt store markeder og kan derfor mest sannsynlig romme et fåtall konkurrerende leverandører på de aller fleste deler av en digital kommunikasjonsinfrastruktur. Desto tettere og mer pålitelige slike internasjonale samarbeidsrelasjoner er, desto mindre blir tapet av nasjonal kontroll for det enkelte land ved å velge leverandører innenfor en slik allianse. Det synes klart at dette må være veien å gå for et lite land som Norge på de fleste områder hvor det er betydelige stordriftsfordeler.

Et viktig moment er betydningen av at begrensningene på utenlandsk eierskap harmoniseres med begrensningene som sammenlignbare land har. I valget mellom ellers like land, vil investorer foretrekke det landet som har færrest begrensninger eller usikkerhet knyttet til sitt regelverk. Det bør av den grunn ikke være relativt vanskeligere for utenlandske investorer å investere i Norge enn eksempelvis i øvrige nordiske land.

[90] En stordriftsfordel er høyere spisskompetanse som også kan bety høyere kvalitet.

”

Norge står overfor sammensatte trusler som blant annet sikkerhetstruende økonomisk aktivitet og skadelig eierskap, digitale angrep og forstyrrelser, samt påvirkning, og det er nødvendig med ulike tiltak og virkemidler for å ivareta nasjonal kontroll.

Foto: Gunnstein Myhre (Nkom)

09

Virkemidler for nasjonal kontroll

9.1 Innledning om ulike typer virkemidler for nasjonal kontroll

I Meld. St. 9 (2022–2023) pekes det på at nasjonal kontroll på områder som er strategisk viktige for nasjonal sikkerhet, er en meget viktig del av arbeidet med å styrke samfunnets kollektive motstandskraft. Regjeringens formål med meldingen var å tydeliggjøre den strategiske retningen, prioriteringene og tiltakene som kan treffes for å sikre nasjonal kontroll og nasjonal sikkerhet på ulike områder, og det vises til en rekke virkemidler som kan brukes for å styrke nasjonal kontroll.

I meldingen redegjøres det for virkemidler som nasjonalt eierskap, regulering, samarbeid nasjonalt og internasjonalt, råd og veiledning samt nasjonal deteksjonsevne og hendelseshåndtering, og det framgår på side 14 at «*Virkemidlene må vurderes både enkeltvis og i sammenheng, og de vil variere, avhengig av hvor man befinner seg i krisespennet, hvor stor grad av kontroll som er ønskelig i ulike sammenhenger og eventuelle kostnader knyttet til dette*». Inngripen for å sikre nasjonal kontroll må altså vurderes ut fra trussel- og risikobildet, og veies mot kostnadene eventuelle inngrep kan medføre.

I en vurdering av om virkemidler må tas i bruk for å sikre tilstrekkelig nasjonal kontroll, må forholdsmessigheten og kostnaden med det, vurderes opp mot effekten virkemiddelbruken vil ha. Bruk av virkemidler må også vurderes i lys av de folkerettslige forpliktelsene Norge har. I denne sammenheng er særlig EØS-avtalen viktig. Avtalen åpner i noen tilfeller for at statene kan gjennomføre tiltak som ellers ville stride med forpliktelser etter EØS-avtalen. Rekkevidden av unntakene må vurderes ved bruk av virkemidler som skal sikre nasjonal kontroll, slik at tiltak ikke kommer i strid med EØS-avtalens konkurranseregler, statsstøtteregler samt reglene om fritt varebytte og fri bevegelighet av personer, tjenester og kapital.

Utvalget redegjør nedenfor for ulike typer virkemidler som kan være aktuelle å ta i bruk – alene eller i kombinasjon med andre virkemidler – for å bidra til å sikre nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur.

9.2 Nasjonalt eierskap

9.2.1 Overordnet om nasjonalt eierskap

«Nasjonalt eierskap omfatter statlig, fylkeskommunalt og kommunalt eierskap, samt privat norsk eierskap» (Meld. St. 9, 2022–2023, s. 18). Nasjonalt eierskap kan sikre nasjonal kontroll av kritisk digital kommunikasjonsinfrastruktur gjennom at det er norske eiere som har innflytelse på eller kontroll over virksomheten som eier viktig infrastruktur. Nasjonalt eierskap kan sikre at uønskede aktører ikke får kontroll over infrastruktur som er viktig for samfunnssikkerheten og kritiske samfunnsfunksjoner.

9.2.2 Statlig eierskap

Med statlig eierskap menes i denne sammenheng at staten direkte eier andeler i selskaper. I Meld. St. 6 (2022–2023) *Et grønnere og mer aktivt statlig eierskap – Statens direkte eierskap i selskaper* (eierskapsmeldingen) fra oktober 2022, redegjør regjeringen for retningen i statlig eierskap. I eierskapsmeldingen punkt 4.1.2 står det blant annet om begrunnelser for statlig eierskap:

> «Samfunnsutviklingen og den geopolitiske situasjonen har de siste årene bidratt til økt oppmerksomhet om beredskapshensyn, for eksempel matproduksjon og beredskapslager for smittevernutstyr, vaksiner, legemidler og korn. Det er også økt oppmerksomhet om ivaretagelse av kritiske innsatsfaktorer, produksjon, tjenesteyting og infrastruktur.
>
> Regulering er det primære virkemiddelet for å ivareta hensyn knyttet til nasjonal sikkerhet, samfunnssikkerhet og beredskap. Eksempler på slik regulering er næringsberedskapsloven, kraftberedskapsforskriften, sikkerhetsloven og ekomloven. Statlige overføringer til produsenter, kontraktsinngåelser med private aktører eller andre former for samarbeid med næringslivsaktører administrert og forvaltet gjennom respektive sektordepartement er eksempler på andre virkemidler.
>
> Staten kan i særskilte tilfeller vurdere det som nødvendig å unngå at uønskede interesser kan få tilgang til informasjon, innflytelse på eller kontroll over selskaper som har betydning for nasjonal sikkerhet, samfunnssikkerhet eller beredskap, noe som blant annet kan gjøres ved å underlegge selskapene sikkerhetsloven eller eie en gitt andel i enkelte selskaper».

I eierskapsmeldingen punkt 1.2 fremgår seks begrunnelser for statlig eierskap for å oppnå ulike samfunnsmål:

- Hovedkontorfunksjoner i Norge
- Samfunnssikkerhet og beredskap
- Energi og naturressurser
- Tilrettelegging for bærekraftig omstilling og økt verdiskaping
- Infrastruktur, monopoler og tildelte rettigheter
- Fellesgoder og/eller sosial og geografisk fordeling

Både hovedkontorfunksjon i Norge og samfunnssikkerhet og beredskap fremheves som begrunnelser for statlig eierskap. Når det gjelder hovedkontorfunksjonen, trekkes ofte frem verdien av at lokalisering av hovedkontorer i Norge vil skape positive økonomiske effekter for samfunnet (samfunnsøkonomisk overskudd) utover et eventuelt bedriftsøkonomisk overskudd. At hovedkontorfunksjonen er i Norge, vil også medføre at styrefunksjonen i selskapet og andre sentrale administrative oppgaver, normalt utføres i Norge.

For å sikre at hovedkontoret forblir i Norge, er det normalt nødvendig med en eierandel på over en tredel av aksjene. Dersom formålet med statlig eierskap er begrunnet ut fra samfunnssikkerhet og beredskap gjennom at staten som eier har innflytelse i styringen av selskapet, bør eierandelen være på mer enn 50 prosent av aksjene. Ved å sitte med aksjemajoriteten, vil staten kunne sikre seg innflytelse gjennom valg av styremedlemmer, og på den måten også sikre at uønskede interesser ikke får innflytelse gjennom styreposisjoner. Styremedlemmene vil imidlertid måtte ivareta alle aksjonærenes interesser med utgangspunkt i de formål som er vedtektsfestet for selskapet.

I denne sammenheng er det sentralt at når aksjeselskapsformen benyttes for statlige investeringer, bygger det på en generell forutsetning om at slike selskaper i utgangspunktet har bedriftsøkonomisk avkastning som formål og på en forutsetning om en klar rollefordeling mellom selskapets eiere på den ene side – der statens eiermyndighet i selskapet utøves på generalforsamlingen – og selskapets ledelse bestående av styret og daglig leder på den annen side. At bedriftsøkonomisk avkastning står sentralt, betyr ikke at det må være det eneste formålet, og heller ikke at gevinst for aksjonærene skal gå foran alle andre formål eller interesser. Er samfunnssikkerhet og beredskap sentralt for eierskapet, kan en eierandel på minst to tredeler av selskapet sikre at vedtektene ivaretar slike interesser. Et slik formål med eierskapet vil imidlertid kunne svekke andres interesse i å investere i selskapet.

Statlig eierskap deles nå inn i to kategorier ut fra målet med eierskapet[91]. Kategori 1 der statens mål er høyest mulig avkastning over tid innenfor bærekraftige rammer, og kategori 2 der statens mål som eier er bærekraftig og mest mulig effektiv oppnåelse av sektorpolitiske mål. Tidligere[92] har man operert med tre kategorier med mål for eierskap. I tillegg til «Kategori 1 – Mål om høyest mulig avkastning over tid» og «Kategori 3 – Mål om mest mulig effektiv oppnåelse av sektorpolitiske mål», brukte man «Kategori 2 – Mål om høyest mulig avkasting over tid og særskilt begrunnelse for å eie». I Kategori 2 inngikk

[91] Meld. St. 6 (2022–2023) *Et grønnere og mer aktivt statlig eierskap,* kapittel 5, https://www.regjeringen.no/contentassets/b45b4a63e301435293bd1b10d1ede45b/no/pdfs/stm202220230006000dddpdfs.pdf

[92] Meld. St. 8 (2019–2020) *Statens direkte eierskap i selskaper – Bærekraftig verdiskaping,* avsnitt 5.2, https://www.regjeringen.no/contentassets/44ee372146f44a3eb70fc0872a5e395c/no/pdfs/stm201920200008000dddpdfs.pdf

selskapene der staten har mål om høyest mulig avkastning over tid, og hvor staten har særskilte begrunnelser for eierskapet. I eierskapsmeldingen fra 2022[93] begrunnes denne endringen med at:

> «Regjeringen anser det ikke hensiktsmessig å foreta denne oppsplittingen, da det vesentligste med å kategorisere selskapene er tydelighet om statens mål som eier i selskapene. Denne forenklingen av kategoriseringen innebærer ikke endringer i statens eierutøvelse».

Innenfor sektoren digital infrastruktur, eier staten direkte i dag aksjer i Space Norway AS (heleid av staten) og Telenor ASA (53,97 prosent av aksjene). I tillegg er Norid AS heleid av staten. Ifølge eierskapsmeldingen har staten eierandeler i Telenor ASA for «å opprettholde et ledende telekommunikasjons-selskap med hovedkontorfunksjoner i Norge samt å ha kontroll med samfunnskritisk kommunikasjonsinfrastruktur», mens eierskapet i Space Norway AS er begrunnet i «å utvikle, forvalte og eie sikkerhetskritisk romrelatert infrastruktur som dekker viktige, norske samfunnsbehov». Begge selskapene er nå plassert i kategori 1. Etter at Space Norway AS kjøpte Telenor Satellite AS i januar 2024, endret staten sitt mål som eier i Space Norway AS fra kategori 2 til kategori 1 fordi oppkjøpet medfører større kommersiell virksomhet. Begrunnelsen for eierskap i Norid AS er «å ha kontroll med sentral nasjonal internettinfrastruktur» og målet med eierskapet er «sikre og tilgjengelige registrerings- og navnetjenester til internettbrukerne».

Det framgår av Meld. St. 6 (2022–2023) kapittel 8 at det er et mål at staten skal være en aktiv eier. Eierutøvelsen skal bidra til å nå statens mål som eier, enten høyest mulig avkastning over tid innenfor bærekraftige rammer eller bærekraftig og mest mulig effektiv oppnåelse av sektorpolitiske mål. For å nå målene, skal staten som eier stille tydelige forventninger til selskapene, velge kompetente styrer, følge opp selskapene systematisk og stemme på generalforsamling. I denne sammenheng har regjeringen utformet ti prinsipper[94] for god eierutøvelse.

[93] Meld. St. 6 (2022–2023*) Et grønnere og mer aktivt statlig eierskap – Statens direkte eierskap i selskaper,* avsnitt 5.3

[94] https://www.regjeringen.no/no/tema/naringsliv/statlig-eierskap/eierstyring-og-ledelse/id613433/

Boks 9.1

Statens ti prinsipper for god eierutøvelse.

1. Staten skal være en aktiv og ansvarlig eier med et langsiktig perspektiv.
2. Staten skal vise åpenhet om statens eierskap, eierutøvelse og stemmegivning på generalforsamling.
3. Statens eierutøvelse skal bidra til å nå statens mål som eier. Dette skjer gjennom forventninger til selskapene, stemmegivning på generalforsamling og annen eierutøvelse.
4. Statens eierutøvelse skal legge til grunn selskapslovgivningens ansvars- og rollefordeling mellom eier, styre og daglig leder, samt allment anerkjente eierstyringsprinsipper og -standarder.
5. Statens eiermyndighet i selskapet skal utøves på generalforsamling.
6. Styret har ansvaret for å forvalte selskapet. Staten skal vurdere selskapets måloppnåelse og arbeid med statens forventninger og styrets bidrag til dette.
7. Relevant kompetanse skal være hovedhensynet ved statens arbeid med styresammensetting. Gitt kompetanse skal staten vektlegge kapasitet og mangfold.
8. Statens eierskap skal utøves i tråd med selskapsrettens prinsipp om likebehandling av aksjeeiere.
9. Statens eierrolle skal skilles fra statens øvrige roller.
10. Statlig eierskap skal ikke urettmessig medføre andre konkurransevilkår, verken fordeler eller ulemper, sammenlignet med selskaper uten statlig eierandel.

Det er åpenbart at gjennom en aktiv eierutøvelse, kan staten – avhengig av eierandel – utøve innflytelse i virksomheten den eier. I den grad begrunnelsen for eierskap er å kunne kontrollere kritisk digital kommunikasjonsinfrastruktur, bør eierandelen være over 50 prosent. Med en slik eierandel vil staten ha bestemmende innflytelse på en rekke avgjørelser knyttet til driften av selskapet og dermed sikre nasjonal kontroll over infrastrukturen, blant annet gjennom valg av styremedlemmer. Staten vil med en slik eierandel også kunne blokkere generalforsamlingsbeslutninger som krever flertall.

Hvorvidt staten skal sikre nasjonal kontroll gjennom eierskap må vurderes konkret i hvert enkelt tilfelle i lys av trussel- og risikobildet. I vurderingen må man se hen til hvilke andre tiltak som kan sikre et tilfredsstillende nivå av nasjonal kontroll, og veie forholdsmessigheten, kostnaden og effektiviteten av eierskap kontra bruk av andre virkemidler. I eierskapsmeldingen fremgår det også eksplisitt at regulering

er det primære virkemiddelet for å ivareta hensyn knyttet til nasjonal sikkerhet, samfunnssikkerhet og beredskap. Å bruke eierskap for å nå dette målet skal kun vurderes i særskilte tilfeller.

I forhold til de øvrige virkemidlene som regulering og avtaler, gir eierskap kontroll over alle gjenværende rettigheter, det vil si dem som ikke er regulert eller avtalt på forhånd – såkalte residuale rettigheter. I tilfeller hvor det er vanskelig å forutsi eller spesifisere behovet for kontroll i form av en regulering eller avtale, vil eierskap derfor kunne være bedre.

En annen styrke ved (tilstrekkelig) eierskapsandel er at det gir innsikt i selskapets strategiske beslutninger, herunder utkontraktering, nedleggelse av enkelte tjenester og salg av eiendeler og rettigheter. Slike beslutninger kan svekke nasjonal kontroll og vil typisk ikke fanges opp av reguleringer om meldeplikt knyttet til eierskap etter sikkerhetsloven. Normalt skal slike beslutninger styrebehandles, og en statlig eierandel på mer enn halvparten vil dermed kunne gi innsikt og innflytelse gjennom styreposisjon.

Statens direkte eierskap i selskaper må alltid ha grunnlag i et vedtak fra Stortinget som gir fullmakt til dette. Slik fullmakt ble for eksempel gitt i statsbudsjettet for 2024[95] der NFD ble gitt fullmakt til «*å utøve forkjøpsrett og utgiftsføre uten bevilgning under kap. 950 Forvaltning av statlig eierskap, post 96 Aksjer, og dermed erverve 30 pst. av aksjene i Telenor Fiber AS dersom Telenor ASA ikke ønsker å benytte denne retten og retten overføres til Nærings- og fiskeridepartementet, ved et eventuelt fremtidig salg av minoritetsandelen i Telenor Fiber AS*». Vedtaket hadde sammenheng med Telenor ASAs salg av en 30 prosent eierandel i Telenor Fiber AS til et konsortium bestående av KKR[96] og Oslo Pensjonsforsikring, og der Telenor ASA i avtalen hadde sikret seg en forkjøpsrett ved et eventuelt salg av de aktuelle aksjene i fremtiden.

Fullmakt ble også gitt av Stortinget da Space Norway AS (100 prosent statlig eiet) kjøpte Telenor Satellite AS 4. januar 2024. Kjøpet ble finansiert gjennom en forhøyelse av egenkapitalen i Space Norway AS på 2,36 mrd. kroner[97], som ble tilført fra staten på en ekstraordinær generalforsamling 21. desember 2023.

Space Norway AS sitt oppkjøp av Telenor Satellite AS er et eksempel på at staten ønsket å sikre statlig eierskap i infrastruktur som kritiske samfunnsfunksjoner er avhengig av. I pressemeldingen[98] fra NFD om oppkjøpet står det at «Oppkjøpet vil bidra til at vi får en stor norsk satellittoperatør som, sammen med en norsk romnæring i vekst, kan styrke Norge som romnasjon. Samtidig sikrer oppkjøpet at Norge – i en tid med økende geopolitisk uro – har kontroll over satellitter som kritiske samfunnsfunksjoner er avhengige av og som er strategisk viktige for Norge».

Selv om statlig eierskap kan gi stor grad av nasjonal kontroll, illustrerer eksemplene at statlig oppkjøp som virkemiddel til å sikre nasjonal kontroll, først og fremst egner seg som virkemiddel i et mer langsiktig perspektiv, og ikke i situasjoner der en står overfor en

95 Innst. 8 S fra næringskomiteen, behandlet i Stortinget 15. desember 2023 punkt 13.

96 KKR (Kohlberg Kravis Roberts & Co) er et globalt investeringsselskap hjemmehørende i USA (https://www.kkr.com/)

97 Se Prop. 25 S (2023–2024) og Innst. 123 S (2023–2024) kap. 922 post 95.

98 https://www.regjeringen.no/no/aktuelt/space-norway-med-avtale-om-kjop-av-telenor-satellite/id3014624/

aktuell trussel. Skal eierskap brukes som effektivt virkemiddel for å unngå at uønskede interesser får kontroll og innflytelse i selskaper som eier kritisk digital infrastruktur, må staten proaktivt og løpende vurdere det sikkerhetspolitiske bildet, ha oversikt over hva som må anses som kritisk digital kommunikasjonsinfrastruktur samt ha oversikt over eierskapet i den aktuelle infrastrukturen, og treffe avgjørelser ut fra potensielle utfordringer som risikobildet gir. Slike vurderinger krever ressurser og oppfølging, og avgjørelsen vil kunne være politisk sensitiv.

EØS-avtalen kan legge begrensninger på bruk av eierskap for å sikre nasjonal kontroll. Avtalens bestemmelser om statsstøtte gjelder uavhengig av om eierskapet i en virksomhet er offentlig eller privat, og gjelder også selskaper med statlig eierandel. Dette betyr at statsstøtteregelverket kan legge begrensninger på statens mulighet til å vektlegge ikke-kommersielle sikkerhetshensyn i eierutøvelsen når virksomheten driver økonomisk aktivitet etter EØS-avtalens artikkel 61 (1). I St. Meld. 6 (2022–2023) punkt 9.4 framgår det at

> «Dersom det offentlige tilfører kapital på grunnlag av andre hensyn og andre vilkår enn hva en sammenlignbar privat investor antas å ville ha stilt, kan det bety at tilførselen innebærer en økonomisk fordel for det aktuelle selskapet som kan gjøre det til offentlig støtte etter EØS-avtalens artikkel 61 (1), såfremt de andre vilkårene er oppfylt. Dette innebærer at staten må operere i samsvar med markedsaktørprinsippet når staten investerer i et foretak, gitt at alle kriteriene i EØS-avtalens artikkel 61 (1) er oppfylt, for å unngå at en investering blir offentlig støtte».

Det kan synes å være tilfeller av inkonsistens mellom begrunnelsen for staten sitt eierskap og statens mål med eierskapet i eierskapsmeldingen, eksempelvis i Telenor. Eierskapet er satt til kategori 1 hvor målet er høyest mulig avkastning gitt bærekraftighet. I tillegg begrunnes eierskapet i å sikre at hovedkontorfunksjoner forblir i Norge samt av hensyn til samfunnssikkerhet og beredskap.[99] Dette er uproblematisk så lenge beslutninger som gir høyest mulig avkastning for selskapet sammenfaller med samfunnssikkerhet. Imidlertid gir begrunnelsen bare mening dersom den tenkes utøvet, noe som bare vil være aktuelt i de tilfeller hvor det *ikke* er sammenfall, med andre ord, når samfunnssikkerhet går på bekostning av avkastning. Utvalget mener at når staten begrunner eierskap med å ivareta samfunnssikkerhet gjennom eierskapet, bør forvaltningen av eierskapet være tydeligere når det gjelder hvordan hensynet til samfunnssikkerhet og beredskap veies mot hensynet til avkastning, andre aksjonærer og for eksempel statsstøtteregler.

9.2.3 Kommunalt og fylkeskommunalt eierskap

Grunnloven § 49 annet ledd sier at «Innbyggerne har rett til å styre lokale anliggender gjennom lokale folkevalgte organer. Nærmere bestemmelser om det lokale folkevalgte nivå fastsettes ved lov». Bestemmelsen grunnlovfester prinsippet om det lokale selvstyret, men setter ikke «skranke for den funksjons- og oppgavefordeling innen offentlig forvaltning som Stortinget gjennom ordinær lovgivning finner hensiktsmessig,»

[99] Samfunnssikkerhet beskrives som å inkludere cybersikkerhet, utenlandske investeringer samt andre økonomiske virkemidler for å true nasjonale sikkerhetsinteresser, inkludert kritiske samfunnsfunksjoner som elektronisk kommunikasjon (Meld. St. 6 (2022–2023) side 22). Dette synes å overlappe i stor grad med behovet for nasjonal kontroll som er fokuset i denne rapporten.

se Innst. 182 S (2015–2016) side 7. Kommunalt og fylkeskommunalt selvstyre nærmere regulert i kommuneloven § 2-1:

> «§ 2-1.Kommunalt og fylkeskommunalt selvstyre
>
> Norge er inndelt i kommuner og fylkeskommuner med en egen folkevalgt ledelse.
>
> Hver kommune og fylkeskommune er et eget rettssubjekt og kan ta avgjørelser på eget initiativ og ansvar.
>
> Kommunene og fylkeskommunene utøver sitt selvstyre innenfor nasjonale rammer. Begrensninger i det kommunale og fylkeskommunale selvstyret må ha hjemmel i lov.»

Kommunenes kompetanse er negativt avgrenset, noe som betyr at de kan ta på seg oppgaver og treffe beslutninger ut fra de behovene kommunene har, så lenge oppgavene ikke i lov er gitt andre eller der er særskilt forbud mot det. Kommuner kan involvere seg i en rekke frivillige aktiviteter, herunder å drive næringsvirksomhet.

En rekke kommuner eier i dag – direkte eller indirekte – andeler av selskaper som eier digital kommunikasjonsinfrastruktur og leverer tjenester i denne infrastrukturen. Det er særlig fiberinfrastruktur og bredbåndstjenester som eies og leveres av selskaper eid av kommuner. For eksempel eies Lyse Tele AS 100 prosent av Lyse AS som eies av 14 kommuner i Sør-Rogaland.[100] Viken fiber eies indirekte av Lyse AS samt Statskraft og en rekke kommuner i Agder, Buskerud og Oppland (gjennom eierskap i Å Energi AS, Lier Everk Holding AS og Hadeland Energi AS). Eidsiva AS som eier Eidsiva bredbånd, eies direkte og indirekte av til sammen 29 kommuner.[101] Eidsiva AS eier også et datasenter.

På samme måte som for statlig eierskap, vil kommunalt eller fylkeskommunalt eierskap kunne sikre at uønskede aktører ikke får kontroll over kritisk digital kommunikasjons-infrastruktur. Mens statlig eierskap i slik infrastruktur normalt er begrunnet nettopp i behovet for nasjonal kontroll, vil det neppe være utgangspunktet for kommunalt eller fylkeskommunalt eierskap.

En begrunnelse for eierskap kan være å sikre innbyggerne tjenester. Kommuner og fylkeskommuner har stor frihet til å velge hvordan tjenestene og virksomheten skal organiseres. I stor grad skjer tjenesteproduksjonen innenfor kommunen eller fylkeskommunen som organisasjon. Kommunestyret eller fylkestinget kan imidlertid velge å organisere en del av virksomheten i egne foretak, for eksempel aksjeselskaper eller interkommunale selskaper.

Kommuner og fylkeskommuner eier store deler av kraftsektoren. Tradisjonelt har motivet for slikt eierskap særlig vært å sikre energi til befolkning og næringsliv, mens i dag er økonomisk utbytte og mulighet for å sikre kommuneøkonomien, mer sentralt for eierskap. Flere kraftselskaper med kommunalt eierskap har investert i

[100] https://www.lysekonsern.no/om-oss/eierskap-og-historie/

[101] https://www.eidsiva.no/om-eidsiva/eiere/

bredbåndinfrastruktur, og bredbåndvirksomhet utgjør en vesentlig del av inntektene[102] i mange kommunalt eide konsernselskaper. Muligheten for økonomisk utbytte og styrket kommuneøkonomi, vil nok ofte være hovedmotivet for slike investeringer.

Likevel kan hensynet til nasjonalt eierskap for å sikre trygge samfunnskritiske tjenester også være av betydning for kommunalt og fylkeskommunalt eierskap. Da Eidsiva kjøpte fjellanlegget til Tietoevry på Gjøvik, uttalte selskapet i sin pressemelding at Eidsiva ville bidra til å bygge en viktig del av den samfunnskritiske infrastrukturen for digitaliseringen av landet.[103]

Uavhengig av hva motivasjonen for eierskap er, kan staten ikke instruere kommuner og fylkeskommuner om hvordan eierskapet skal forvaltes. Hvis staten ønsker å gripe inn i forvaltningen av eierskapet, må dette gjøre innenfor de samme rammer som gjelder for andre markedsaktører, for eksempel gjennom bruk av sikkerhetsloven.

9.2.4 Privat eierskap

Privat eierskap er hovedregelen i den forstand at det er den største eierkategorien i norsk næringsliv. Privat norsk eierskap kan hindre at uønskede utenlandske aktører får innflytelse og kontroll, og på den måten treffe beslutninger og tiltak til skade for nasjonal sikkerhet, i virksomheter som eier kritisk digital kommunikasjonsinfrastruktur. Eierandeler i disse selskapene vil i utgangspunktet kunne omsettes uten norske myndigheters inngripen. Skal staten kunne gripe inn overfor private aktører for å sikre tilstrekkelig nasjonal kontroll ved et salg av eierandeler, krever det hjemmel i lov. Her står sikkerhetsloven særlig sentral og åpner for at det kan treffes vedtak om at kjøp av foretak ikke kan gjennomføres eller sette vilkår for gjennomføringen. Regulering som virkemiddel er beskrevet nærmere nedenfor.

Privat norsk eierskap som virkemiddel for nasjonal kontroll av kritisk digital kommunikasjonsinfrastruktur, bygger på en forutsetning om at man har tillit til at norske eiere i større grad enn utenlandske eiere, vil ha fokus på å ivareta nasjonale sikkerhetshensyn i forvaltningen av eierskapet. Som nevnt i punkt 8.4 kan imidlertid også norske eiere være utsatt for innflytelse av utenlandske statsledelser.

[102] Kommunale inntekter fra kraftsektoren Inntekter fra kommunalt og fylkeskommunalt eierskap i kraftsektoren og som vertskommune for slik virksomhet, samt anvendelse av inntektene. På oppdrag fra TBU – side 7: «*Vannkraft alene består av 82 prosent av verdien av eierskapet med en verdi på 360 milliarder kroner. Annen virksomhet, som består primært av fiber/bredbånd og fjernvarmevirksomhet, er nest størst med 39 milliarder kroner, etterfulgt av eierskap i nettvirksomhet som består av 27 milliarder kroner. I tillegg kommer vindkraft og kraftsalg på henholdsvis 12 og 2 milliarder kroner.*» https://www.regjeringen.no/contentassets/d28f4297bf6c4fd89c5b099d7a89f79c/kommunale-inntekter-fra-kraftsektoren-thema.pdf

[103] https://kommunikasjon.ntb.no/pressemelding/18037732/eidsiva-kjoper-etablert-datasenter-vi-skal-tilby-trygg-lagring-med-100-percent-nasjonalt-offentlig-eierskap?publisherId=17848064&lang=no

9.3 Regulering

9.3.1 Innledning

Som det framgår av eierskapsmeldingen punkt 4.1.2[104] er regulering det primære virkemiddelet for å ivareta hensyn knyttet til nasjonal sikkerhet, samfunnssikkerhet og beredskap. I innstilling fra Stortingets justiskomité om Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet[105], sier komitéen knyttet til redegjørelsen av virkemiddelapparatet for å sikre nasjonal kontroll og digital motstandskraft:

«Komiteen viser til at flere saker de siste årene har synliggjort hvor viktig det er å ha både regulatoriske virkemidler og evne til å tenke langsiktig for å sikre nasjonal kontroll og nasjonal sikkerhet. Flere virksomheter har blitt utsatt for alvorlige dataangrep de siste årene, hvilket er en påminnelse på behovet for digital motstandskraft. Komiteen er derfor enig i behovet for utvikling og tilpasning av tiltak for å kunne imøtekomme aktuelle situasjoner som kan oppstå. Det å forebygge uønskede hendelser blir stadig viktigere, spesielt i lys av de endrede økonomiske rammene. Selv om enkelte tiltak vil kunne påføre både offentlige og private virksomheter direkte kostnader og utløse økte krav til rapportering, må omkostningene veies opp mot hensynet til å kunne ivareta nasjonal sikkerhet».

Nedenfor beskrives ulike regelverk med bestemmelser knyttet til nasjonal sikkerhet og sikkerhet i digital infrastruktur samt beredskap, og som er eksempel på at regulering brukes som virkemiddel for å styrke nasjonal kontroll og nasjonal sikkerhet i kritisk digital kommunikasjonsinfrastruktur. Regelverkene som beskrives inneholder regulering som fungerer som proaktivt virkemiddel – som krav i sikkerhetsloven § 4-3 og ekomloven § 3-1 om «forsvarlig sikkerhet» – og som reaktivt virkemiddel som gir myndigheter hjemmel til å agere når sikkerhetstruende hendelser inntrer – som sikkerhetsloven § 2-5 (for å hindre sikkerhetstruende aktivitet) og § 10-3 (om stans i erverv av virksomhet).

9.3.2 Adgangen til å vedta, anvende og håndheve regler

Staten kan pålegge private parter plikter gjennom utøvelse av offentlig myndighet. Når pliktene går ut på at virksomheter skal ha bestemte strukturer eller handle på bestemte måter, og dette ikke kan forankres i statens eierrådighet eller i en avtale, er det nødvendig med hjemmel i lov (legalitetsprinsippet).

Hvis lovgivningen krever tillatelse fra forvaltningen til å foreta visse handlinger, og forvaltningen i tillegg er gitt en viss frihet til å velge om tillatelse skal gis, vil det også være lovgrunnlag for å stille vilkår for tillatelsen. Dette følger av den såkalte vilkårslæren som innebærer at når forvaltningen kan gjøre det mer, nekte tillatelse, kan forvaltningen også gjøre det mindre, stille vilkår for en tillatelse. Det vil imidlertid være en grense for hvilke inngrep forvaltningen kan gjøre – vilkårene må ha saklig sammenheng med tillatelsen, ikke være uforholdsmessig tyngende og ligge innenfor lovens formål for ikke å utfordre legalitetsprinsippet. Hvorvidt lovgivningen utfordrer legalitetsprinsippet i tilfeller der betingelsene for inngrepet er upresise, vil bero på en vurdering der relevante momenter blant annet vil være hva slags

[104] Meld. St. 6 (2022–2023) *Et grønnere og mer aktivt statlig eierskap – Statens direkte eierskap i selskaper*

[105] https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2022-2023/inns-202223-247s/?all=true#m2

forvaltningsområde det gjelder, om de aktuelle lovbestemmelsene i realiteten omfatter hele eller deler av det aktuelle forvaltningsområdet, og hvorvidt lovens formål setter snevre eller vide rammer for hvilke inngrep forvaltningen kan foreta.

For at staten skal kunne anvende og håndheve regler overfor andre, må den ha jurisdiksjon til å fastsette både generelle og individuelle normer innenfor sine grenser, samt myndighet til å håndheve disse normene. Lovgivningsjurisdiksjon handler om at lovgivningen kan gjøres gjeldende overfor noen eller noe. Domsjurisdiksjon handler om at det kan treffes avgjørelser basert på lovgivningen. Tvangsjurisdiksjon handler om adgangen til å håndheve lovgivningen.

Når det gjelder statens mulighet til å vedta og anvende regler overfor utenlandske aktører, sier Eriksen (2024)[106] følgende:

> «Norske myndigheter har jurisdiksjon til å fastsette vilkår gjennom myndighetsutøvelse, også overfor utenlandske virksomheter. Det virksomhetene gjør i Norge har norske myndighetene allerede jurisdiksjon over i kraft territorialhøyheten. Jeg antar derfor at norske myndigheter i kraft av sin suverenitet over norsk territorium kan stille vilkår om at en ny utenlandsk eier i norsk selskap, ikke skal ha tilgang til informasjon om hvor digital infrastruktur er lokalisert.
>
> Norske myndigheter har også jurisdiksjon til å regulere, og pålegge vilkår overfor det virksomheter gjør i utlandet, såfremt det er tale om handlinger som først blir fullført i Norge. Vilkår kan derfor pålegges utenlandsk selskap såfremt vilkårene angår handlinger som først blir fullført i Norge. Konkret innebærer dette at norske myndigheter kan pålegge utenlandske selskap vilkår som gjelder handlinger som først blir fullført i Norge, uavhengig av om det utenlandske selskapet selv eier infrastruktur eller tilbyr ekom- eller datasentertjenester i Norge, eller om det har kontroll over infrastrukturen og tjenestene gjennom norske datterselskaper.
>
> I tillegg antar jeg at norske myndigheter har jurisdiksjon over handlinger som foretas av utenlandske virksomheter som har direkte, vesentlige og forutsigbare virkninger i Norge jf. den folkerettslige effektdoktrinen. Det innebærer at norske myndigheter har jurisdiksjon til å fastsette vilkår overfor utenlandske virksomheter i den grad det er tale om vilkår for handlinger som har direkte, vesentlige og forutsigbare virkninger i Norge. Det kan for eksempel gi grunnlag for å stille vilkår til en utenlandsks virksomhets håndtering av informasjon om digital infrastruktur i Norge, i den grad visse måter å håndtere informasjonen på har direkte, vesentlige og forutsigbare skadevirkninger i Norge. Effektdoktrinen kan også gi adgang for norske myndigheter til å stille vilkår til utenlandske virksomheter som ikke eier infrastruktur i Norge, men som tilbyr tjenester som anvendes i riket, forutsatt at vilkårene gjelder forhold som har direkte, vesentlige og forutsigbare virkninger i Norge.»

Utvalget antar på denne bakgrunn at statens mulighet til å vedta og anvende regler knyttet til eierskap i eller kontroll av virksomheter som eier kritisk digital infrastruktur eller tilbyr tjenester i slik infrastruktur, i praksis vil være lik uavhengig av om eierskapet er norsk eller utenlandsk.

[106] Utredning av rettslige rammer for kontroll med kritisk digital infrastruktur

Knyttet til utenlandske aktører, er det imidlertid muligheten til å følge opp risikoreduserende plikter og pålegg som kan være utfordrende. For å sikre at regulering kan være et effektivt virkemiddel for å utøve offentlig myndighet, må det også foreligge mulighet til å presse virksomhetene til å oppfylle forpliktelser, med tvangstiltak. Tvangstiltakene kan kun håndheves ved tvang av norske myndigheter dersom de kan gjennomføres uten å krenke andre staters suverenitet. Norske myndigheter har ikke adgang til å gjennomføre tvangstiltak utenfor Norge uten aksept fra den staten der tvangstiltakene skjer. Selv om det er inngått en rekke avtaler – både nordiske, europeiske og andre internasjonale avtaler – om grensekryssende samarbeid om tvangsjurisdiksjon, gjelder ingen av disse konvensjonene vilkår fastsatt i kraft av offentlig myndighetsutøvelse. Det kan bety at regulering som virkemiddel for å ivareta sikkerhetsinteresser gjennom å stille vilkår overfor utenlandske aktører som eier eller kontrollerer kritisk digital infrastruktur, ikke alltid er hensiktsmessig og effektivt.

9.3.3 EØS-retten og norske myndigheters handlefrihet

EØS-retten etablerer rettslige begrensninger i handlefriheten til nasjonale myndigheter. Prinsippene om de fire friheter innebærer at Norge i utgangspunktet ikke kan ha regler som behandler grenseoverskridende bevegelser og transaksjoner mellom Norge og andre EØS-stater strengere enn rent nasjonale bevegelser og transaksjoner. Slik forskjellsbehandling vil anses som en restriksjon på den frie bevegeligheten over landegrensene. I visse tilfeller kan likevel nasjonalstatene opprettholde eller innføre regler som i utgangspunktet innebærer en restriksjon.

EØS-avtalen åpner for at medlemslandene ut fra blant annet sikkerhetsmessige grunner, kan gjøre inngrep som medfører restriksjoner på fri bevegelighet. Blant annet kan det treffes tiltak om særbehandling av utenlandske statsborgere når det er begrunnet med hensynet til offentlig orden, sikkerhet og folkehelse, jf. EØS-avtalens artikkel 33. Bestemmelsen åpnes for restriksjoner i etableringsadgangen (artikkel 31) og unntakshjemmelen kan anvendes i tilfeller hvor det er behov for å hindre en etablering av hensyn til nasjonal sikkerhet. Unntakshjemmelen kan altså ikke anvendes for å hindre retten til fri bevegelighet av kapital i artikkel 40.

Videre åpner EØS-avtalen artikkel 123 opp for enkelte unntak. Bestemmelsen har tre ulike unntak – en avtalepart kan treffe tiltak

a. som den anser nødvendig for å hindre spredning av opplysninger som er i strid med dens vesentlige sikkerhetsinteresser;
b. som angår produksjon av eller handel med våpen, ammunisjon og krigsmateriell eller andre varer som er uunnværlige for forsvarsformål, eller forskning, utvikling eller produksjon som er uunnværlig for forsvarsformål, såfremt disse tiltak ikke endrer konkurransevilkårene for varer som ikke er bestemt for direkte militære formål;
c. som den anser vesentlig for sin sikkerhet i tilfelle av alvorlig indre uro som truer den offentlige orden, i krigstid eller ved alvorlig internasjonal spenning som innebærer en fare for krig, eller for å oppfylle forpliktelser den har påtatt seg med sikte på å opprettholde fred og internasjonal sikkerhet.

Muligheten for unntak er snever og terskelen for å bruke bestemmelsen er høy.

Tiltakene må også underlegges en proporsjonalitetsvurdering, der det må vurderes om sikkerhetsinteressene som eventuelt kan begrunne unntak kan ivaretas på en annen måte. Hvis mindre inngripende tiltak er tilgjengelige, må disse benyttes.

EØS-avtalens regler om de fire friheter stiller også minstekrav til hvordan lovgivningen skal utformes for at den skal gi forvaltningen hjemmel til å pålegge private parter plikter. Gir en lovbestemmelse en for vid og upresis hjemmel for forvaltningen, vil bestemmelsen kunne anses som en uforholdsmessig restriksjon på retten til fri bevegelse av varer, personer, tjenester og kapital på tvers av landegrensene, og derfor være i strid med EØS-avtalens forpliktelser.

9.3.4 Sikkerhetsloven

9.3.4.1 Formål og virkeområde

Sikkerhetsloven trådte i kraft 1. januar 2019 og erstatter den tidligere sikkerhetsloven av 1998. Sikkerhetslovens formål er å trygge nasjonale sikkerhetsinteresser. Definisjonen på nasjonale sikkerhetsinteresser etter sikkerhetsloven er beskrevet i punkt 4.1.2.

Loven gjelder for statlige, fylkeskommunale og kommunale organer. Den gjelder også for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. I tillegg skal det enkelte sektordepartement fatte vedtak om at loven helt eller delvis også skal gjelde for virksomheter som

a. behandler sikkerhetsgradert informasjon
b. råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller som har avgjørende betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon
c. driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller som har avgjørende betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon.

Departementet kan også fatte vedtak om at lovens kapittel 10 Eierskapskontroll skal gjelde for «virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner, eller virksomheter som har vesentlig betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon.

Ifølge sikkerhetsloven skal «grunnleggende nasjonale funksjoner» som understøtter nasjonale sikkerhetsinteresser, identifiseres og beskyttes etter kravene i loven, og DFD har innenfor sin sektor identifisert følgende grunnleggende nasjonale funksjonert:

- Evne til å ivareta talekommunikasjonstjenester basert på norsk nummerplan
- Evne til å ivareta tekstbaserte meldingstjenester basert på norsk nummerplan
- Evne til å ivareta grunnleggende internettilgang
- Evne til å ivareta datalagring og prosesseringskapasitet i Norge
- Satellittbasert kommunikasjon

I tillegg er «Posisjonsbestemmelse, navigasjon og tidsbestemmelse» identifisert av NFD som grunnleggende nasjonale funksjoner. Især tidsbestemmelse er en funksjon som er viktig for mobilnettene.

Som følge av de identifiserte grunnleggende nasjonale funksjonene innen kritisk digital kommunikasjonsinfrastruktur, er en rekke virksomheter som leverer tjenester til de grunnleggende nasjonale funksjonene, underlagt sikkerhetsloven. Hvilke foretak dette gjelder er i sin helhet ikke offentlig informasjon, selv om enkelte av virksomhetene som er underlagt loven, er kjent.

Departementet skal også identifisere og holde oversikt over virksomheter som har «vesentlig betydning» for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser. I vesentlig betydning ligger det at virksomheten leverer én eller flere innsatsfaktorer for at én eller flere grunnleggende nasjonale funksjoner opprettholder sin funksjonalitet, uten at virksomheten kan sies å være av avgjørende betydning. Det at en virksomhet anses å være av vesentlig betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser, medfører ikke i seg selv at virksomheten har plikter etter sikkerhetsloven. Hensikten med å identifisere denne type virksomheter er å ha oversikt. Hvilken betydning slike foretak har, kan endre seg over tid, avhengig av trusselbildet, redundans og den generelle samfunnsutviklingen.

Sikkerhetsloven §§ 2-5, 9-4 og 10-3 gir Kongen i statsråd kompetanse (myndighet) til å stoppe en aktivitet, anskaffelse eller erverv når den innebærer en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Etter §§ 9-4 og 10-3 kan det alternativt stilles vilkår for at transaksjonen skal kunne gjennomføres. Bestemmelsen i § 2-5 om vedtak ved risiko for skadevirkninger for nasjonale sikkerhetsinteresser, gir myndighetene i ytterste konsekvens muligheten til å gripe inn i økonomisk aktivitet mot virksomheter som ikke er underlagt sikkerhetsloven. Mekanismen består av et departementsnettverk ledet av Justis og beredskapsdepartementet, samt et etatsnettverk ledet av NSM.

9.3.4.2 Sikkerhetsloven kapittel 10 om eierskapskontroll

Det overordnede målet med eierskapskontroll er å avdekke og hindre erverv som kan utgjøre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Hovedelementene i dette systemet består av tre trinn; privates meldeplikt etter § 10-1, departementets vurderingsplikt etter § 10-2 og Kongen i statsråds kompetanse (myndighet) til å stanse eller pålegge vilkår for erverv etter § 10-3. Reglene ble innført med gjeldende sikkerhetslov som trådte i kraft i 2019, og er vedtatt endret ved lov 20. juni 2023 nr. 77. Endringsloven er ikke trådt i kraft.

Ifølge gjeldende § 10-1 første ledd gjelder meldeplikten den som ved ervervet vil oppnå en eierandel på minst en tredel av en virksomhet som er underlagt sikkerhetsloven etter § 1-3. Meldeplikten gjelder virksomheter utpekt av departementet etter § 1-3 første ledd fordi virksomheten

a. behandler sikkerhetsgradert informasjon
b. råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller som har avgjørende betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon
c. driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller som har avgjørende betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon

I tillegg har departementene en mulighet til å fatte vedtak om at sikkerhetslovens bestemmelser om eierskapskontroll skal gjelde for virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner, jf. § 1-3 annet ledd. Det følger av § 2-1 første ledd bokstav b at departementene skal identifisere og holde oversikt over virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner.

I ny § 10-1[107] som er vedtatt, men ikke trådt i kraft, utvides meldeplikten til også å gjelde avhenderen av eierandelene og virksomheten selv. Erverver får meldeplikt når ervervet vil føre til at erververen direkte eller indirekte samlet oppnår minst 10 prosent av aksjekapitalen, andelen eller stemmene i virksomheten, og videre når:

a. erververens kvalifiserte eierandel økes til minst 20 prosent, en tredel, 50 prosent, to tredeler eller 90 prosent av aksjekapitalen, andelene eller stemmene i virksomheten
b. erververen oppnår betydelig innflytelse over forvaltningen av virksomheten på annen måte
c. erververen sammen med sine nærstående, jf. verdipapirhandelloven § 2-5, oppnår en kvalifisert eierandel eller en posisjon som nevnt i bokstav a eller b.

Avhenderen og virksomheten ervervet gjelder, får meldeplikt når erververen samlet vil oppnå en direkte eierandel på minst 10 prosent, eller direkte eierandel eller en posisjon etter bokstav b eller c.

Endringen i sikkerhetsloven vil når den trer i kraft, også innebære at gruppen av meldepliktige erverv utvides, slik at erverv av en kvalifisert eierandel i virksomheter som har leverandørklarering etter § 9-3 blir meldepliktige etter § 10-1. Reglene om leverandørklarering er nærmere omtalt nedenfor.

Boks 9.2

Viktige endringer ved ikrafttredelse av endringer ved lov 20. juni 2023 nr. 77

Langt flere erverv enn i dag vil bli omfattet av meldeplikten.

- behov for ny melding ved suksessive erverv
- tydeliggjøring av erverv av indirekte eierskap
- eierskap mellom nærstående selskaper eller personer slås sammen ved vurdering av om terskelen for meldeplikt er oppfylt
- både den som erverver og virksomheten som blir ervervet etter omstendighetene kan ha meldeplikt

Ingen meldepliktige erverv kan gjennomføres før meldingen er behandlet etter § 10-2

En ny § 10-4 om at informasjon som kan brukes til sikkerhetstruende virksomhet, ikke skal deles uten samtykke før ervervet er gjennomført

[107] Lov om endringer i sikkerhetsloven, https://lovdata.no/dokument/LTI/lov/2023-06-20-77

Det departementet som mottar melding, skal ta stilling til meldingen så raskt som mulig. Departementet «kan be relevante organer uttale seg om ervervets risikopotensial og erververens sikkerhetsmessige pålitelighet». Departementet eller sikkerhetsmyndigheten skal innen 60 arbeidsdager orientere melderen om ervervet er godkjent eller om saken skal behandles av Kongen i statsråd. Denne avgjørelsen skal tas på bakgrunn av en helhetsvurdering, som tar utgangspunkt i meldingen fra erverver.

Etter sikkerhetsloven § 10-3 kan Kongen i statsråd – dersom et erverv kan medføre en «ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet» – fatte vedtak om at ervervet ikke kan gjennomføres, eller sette vilkår for gjennomføring av ervervet. Det er i forarbeidene ikke sagt noe konkret om hvilke vilkår som kan settes for gjennomføringen av et erverv, utover at «vedtak etter bestemmelsen må ligge innenfor formålet med sikkerhetsloven [og] må også være forholdsmessig, slik at hensynet til nasjonale sikkerhetsinteresser må veie opp for de negative økonomiske konsekvensene av vedtaket», jf. Prop. 143 L (2016–2017), s. 152. Formålet med loven er blant annet å trygge Norges «nasjonale sikkerhetsinteresser», som er definert slik at det omfatter mer avgrensete kategorier interesser som «landets suverenitet, territorielle integritet og demokratiske styreform», og en videre kategori, «overordnede sikkerhetspolitiske interesser». Vilkårene som stilles må ha en saklig sammenheng med godkjenningen av ervervet, og ikke være uforholdsmessig tyngende.

9.3.4.3 Sikkerhetsloven paragraf 2-5 om vedtak ved risiko for skadevirkninger for nasjonale sikkerhetsinteresser

Bestemmelsen gir Kongen i statsråd myndighet til å fatte «nødvendige vedtak for å hindre sikkerhetstruende virksomhet eller annen planlagt eller pågående aktivitet som kan innebære «en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet». Bestemmelsen omfatter enhver aktivitet som kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet, og er ikke en spesifikk eierskapskontrollbestemmelse.

Begrepet «ikke ubetydelig risiko» kom inn som en del av flere nye bestemmelser i den nå opphevde sikkerhetsloven av 1998, ved en lovendring i 2016. I Prop. 97 L (2015–2016) Endringer i sikkerhetsloven s. 64 sier departementet følgende om innholdet i uttrykket «ikke ubetydelig risiko»: «Begrepet «ikke ubetydelig risiko» innebærer at det er situasjoner med risiko ut over det «normale» som skal varsles. Vurderingen vil måtte omfatte både sannsynlighet, sårbarhet og mulige konsekvenser. På sannsynlighetssiden innebærer kriteriet at det normalt ikke skal varsles dersom det kun foreligger en helt fjerntliggende eller rent teoretisk mulighet for at anskaffelsen skal kunne resultere i sikkerhetstruende virksomhet. Det bør være noe konkret med den aktuelle anskaffelsen som tilsier at risikoen er noe høyere enn ved andre anskaffelser. Bestemmelsen innebærer imidlertid ikke et krav om sannsynlighetsovervekt.»

Departementet sier videre at uttrykket «ikke ubetydelig risiko» må tolkes på bakgrunn av at det «i mange tilfeller kan være tilnærmet umulig å gjøre nøyaktige sannsynlighetsberegninger av risikoen» for at handlinger skal inntreffe, og at vurderingene da må konsentreres om «sårbarhet og mulige konsekvenser».

Etter sikkerhetsloven § 2-5 kan Kongen i statsråd treffe vedtak rettet både mot virksomheter som er underlagt sikkerhetsloven og andre virksomheter, i tillegg til fysiske personer. Dersom et selskap som eier eller kontrollerer kritisk digital infrastruktur i

Norge, inngår i en konsernstruktur eller i en annen kompleks eierstruktur, kan det også treffes vedtak rettet mot andre deler av konsernet eller eierne, såfremt lovens vilkår er oppfylt.

I Prop. 97 L (2015−2016) påpekes det i punkt 4.2.2 at det «vil være tale om et lite antall saker, og at disse sakene etter sin art vil være alvorlige og spesielle». Sikkerhetsloven § 2-5 er ment som en snever sikkerhetsventil, og vil typisk kunne brukes der det ikke finnes hjemmel i andre regelverk for å stanse eller gripe inn i aktivitet som kan medføre et skadepotensiale for nasjonale sikkerhetsinteresser. Hva slags inngrep i aktiviteten vedtaket medfører, skal tilpasses og være gjenstand for en nødvendighets- og forholdsmessighetsvurdering.

Vedtakskompetansen etter § 2-5 har blitt brukt kun få ganger. I 2017 (under tidligere sikkerhetslov) ble det fattet vedtak om forbud mot å bygge en planlagt gangbro i Nydalen i Oslo, fordi gangbroen på grunn av sin beliggenhet ville kunne brukes som plattform for spionasje, sabotasje og terror rettet mot PST. I 2021 ble § 2-5 brukt for å stanse salget av Bergen Engines AS til TMH Group. I mars 2023 ble § 2-5 benyttet i vedtaket som gjaldt GlobalConnect. I juni 2024 tok regjeringen i bruk sikkerhetsloven § 2-5 for å stanse et mulig salg av eiendommen Søre Fagerfjord på Svalbard. I desember 2024 ble § 2-5 brukt for å sørge for at fartøyet LLV Azurit forlot Båtsfjord havn.

9.3.4.4 Sikkerhetsloven kapittel 9 om sikkerhetsgraderte anskaffelser mv.

Sikkerhetsgraderte anskaffelser er regulert i sikkerhetsloven kapittel 9. § 9-1 sier at en sikkerhetsgradert anskaffelse er «en anskaffelse som innebærer at leverandøren av varen eller tjenesten kan få tilgang til eller tilvirker sikkerhetsgradert informasjon» eller får «tilgang til et skjermingsverdig objekt eller infrastruktur …».

For anskaffelser som vil medføre at en leverandør kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal leverandøren ha gyldig klarering for angitt sikkerhetsgrad (leverandørklarering). En leverandørklarering gis av NSM etter en vurdering av om leverandøren er sikkerhetsmessig skikket. En personkontroll av leverandørens styre og ledelse skal være en del av vurderingsgrunnlaget. Klareringsforskriften § 33 fastsetter at NSM blant annet skal legge vekt på økonomiske forhold og organisasjonsform og eierstruktur. Vurderingen gjøres på bakgrunn av informasjon gitt av virksomheten selv, og informasjon innhentet fra andre kilder. For utenlandske leverandører forutsetter en slik gjennomgang at Norge har en bilateral eller multilateral sikkerhetsavtale med det aktuelle landet, slik at en eventuell utenlandsk leverandørklarering kan legges til grunn for anskaffelsen.

Leverandøren har etter sikkerhetsloven § 9-3 en varslingsplikt og skal «så snart som mulig orientere klareringsmyndigheten om endringer i styret eller ledelsen, endringer i eierstrukturen, flytting av lokaliteter og utstyr, åpning av gjeldsforhandling, begjæring om konkurs og annet som kan påvirke vurderingen av om leverandøren er sikkerhetsmessig skikket». Dersom det som følge av den varslede endringen oppstår en risiko som ikke kan håndteres ved forebyggende sikkerhetstiltak, kan klareringsmyndigheten inndra leverandørklareringen.

Myndighetene har mulighet til å gripe inn i en konkret anskaffelsesprosess som gjelder anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur. Varslingsplikten og myndighet til å fatte vedtak er beskrevet i sikkerhetsloven § 9-4.

Bestemmelsen stiller krav om at den virksomheten som skal anskaffe, selv vurdere om risikoen knyttet til anskaffelsen kan innebære en ikke ubetydelig risiko for at infrastruktur kan bli rammet av eller brukt til sikkerhetstruende virksomhet. Dersom anskaffelsen kan medføre en slik risiko, kan Kongen i statsråd fatte vedtak om at anskaffelsen ikke skal gjennomføres, eller at det skal settes vilkår for den. Slikt vedtak kan fattes selv om det allerede er inngått avtale om anskaffelsen. For øvrig forutsetter bestemmelsen at underliggende organer har vurdert sikkerhetsrisiko ved anskaffelsen og varslet departementet om anskaffelsen innebærer risiko. Kongen i statsråd må likevel kunne fatte vedtak etter bestemmelsen, selv om slikt varsel ikke er gitt, såfremt de øvrige vilkårene er oppfylt.

9.3.5 Ekomloven

Ekomsektoren bærer en stadig større andel av samfunnets verdier, og det er derfor svært viktig å kunne stille krav til forsvarlig sikkerhet og beredskap i elektroniske kommunikasjonsnett og -tjenester. Fra 1. januar 2025 fikk ny ekomlov av 13. desember 2024 virkning.

Lovens formål framgår av § 1-1 som sier:

> «Lovens formål er å sikre brukerne i hele landet gode, rimelige, fremtidsrettede elektroniske kommunikasjonstjenester med forsvarlig sikkerhet, legge til rette for bærekraftig konkurranse, effektiv bruk av samfunnets ressurser og stimulere til næringsutvikling og innovasjon. Loven skal også gi forsvarlig sikkerhet i datasentre».

I den nye loven er det gjort enkelte endringer i ordlyden i formålsbestemmelsen i forhold til ekomloven fra 2003, ved å ta inn referanser til «forsvarlig sikkerhet». Endringene er gjort fordi man ønsket å synliggjøre i bestemmelsen at elektroniske kommunikasjonstjenester og datasentertjenenester skal leveres med forsvarlig sikkerhet.

Det kan være verd å merke seg at begrepet tilbyder er utvidet i den nye ekomloven og omfatter en større krets av tilbydere. Det betyr at plikten til å ivareta sikkerhet i elektroniske kommunikasjonsnett og -tjenester nå også gjelder for de nummeruavhengige person-til-person-kommunikasjonstjenestene, herunder chattetjenester og tale over IP, samt alle former for e-post. I tillegg reguleres også datasentre i den nye ekomloven.

Ekomloven § 3-1 fastsetter at tilbyder skal tilby elektroniske kommunikasjonsnett og -tjenester med forsvarlig sikkerhet for brukerne i fred, krise og krig. Tilbyder skal opprettholde forsvarlig beredskap, og viktige samfunnsaktører skal prioriteres ved behov. Formålet er å sikre at tilbyder ivaretar den grunnleggende sikkerheten i nett og tjenester, og at man sørger for nødvendig beredskap også for å kunne håndtere situasjoner utover det normale. Tilbydere skal også sikre vern av kommunikasjon og data.

Bestemmelsens første ledd sier at tilbydere skal

a. tilby elektroniske kommunikasjonsnett og -tjenester med forsvarlig sikkerhet for brukerne i fred, krise og krig
b. opprettholde forsvarlig beredskap i elektroniske kommunikasjonsnett og -tjenester, og prioritere viktige samfunnsaktører ved behov, og
c. sikre forsvarlig vern av kommunikasjon og data i elektroniske kommunikasjonsnett og -tjenester

Knyttet til bokstav b står det i forarbeidene i merknadene til bestemmelsen at «Ordlyden er endret ved at forsvarlighetsnivået høynes fra «nødvendig» til «forsvarlig» beredskap i tråd med viktigheten av elektronisk kommunikasjon for samfunnet». Tilsvarende endring og med samme begrunnelse, er gjort når det gjelder vern av kommunikasjon og data i bokstav c.

Forsvarlig sikkerhet er en rettslig standard der innholdet vil kunne forandre seg over tid basert på situasjonen i markedet, utviklingen av teknologi og endringer i samfunnet ellers. Hva som utgjør forsvarlig sikkerhet, kan også være forskjellige for virksomhetene ut fra en konkret risiko- og sårbarhetsanalyse. Tilbyders plikt til å opprettholde forsvarlig sikkerhet innebærer at tilbyder av nett og tjenester må gjennomføre fortløpende risikovurderinger og i lys av hva som kan anses som akseptabel restrisiko og kostnadene med tiltak, vurdere hvilke sikkerhetstiltak som er nødvendige for å opprettholde et forsvarlig sikkerhetsnivå.

Etter bokstav b skal tilbydere også prioritere viktige samfunnsaktører ved behov. I ekomforskriften § 2-10 er Nkom gitt hjemmel til i særlige tilfeller så langt det er nødvendig for å sikre offentlige interesser, å pålegge tilbyder å gi prioritet til viktige samfunnsaktører ved gjenoppretting etter driftsstans. Mennesker som er avhengig av mobiltelefon for å utføre særlige samfunnsviktige oppgaver kan få prioritetsabonnement som gjør at brukeren kan komme gjennom på telefonen dersom det er stor belastning i tilbyderens mobilnett. I tillegg gir tjenesten nasjonal gjesting i andre tilbyderes mobilnett ved dekningsutfall i eget mobilnett. Prioritetsfunksjonen og nasjonal gjesting har primært virkning mot lokal metning og lokale utfall i radionett, for eksempler hvis basestasjoner mister strømtilførsel eller sin forbindelse med resten av nettet ved at fiberkabler går i stykker. Nasjonal gjesting er avhengig av at egen tilbyders kjernenett er oppe. Er problemet knyttet til tilbyders kjernenett, vil ikke et prioritetsabonnement sikre fortsatt mulighet til kommunikasjon.

Ekomloven § 3-7 annet ledd setter krav til sikkerhet i datasentre. Bestemmelsen er ny, og stiller krav til forsvarlig sikkerhet i datasenter og er utformet med utgangspunkt i de samme forpliktelsene som stilles til sikkerhet i elektronisk kommunikasjonsnett og -tjenester, jf. ekomloven § 3-1.

Ekomloven 3-5 sier i første ledd at «Når det er nødvendig av hensyn til nasjonal sikkerhet eller andre viktige samfunnsinteresser, kan departementet i særlige tilfeller fatte vedtak om at tilbyder nektes tilgang til markedet». Departementet kan nekte tilgang til markedet for elektroniske kommunikasjonsnett og -tjenester både ved oppstart av virksomhet og etter at virksomheten er i gang, dersom det er forhold som tilsier at tilbyder bør nektes tilgang til markedet. Bestemmelsen er ment for tilfeller der alternative tiltak ikke finnes og terskelen for å ta i bruk bestemmelsen er høy, jf. merknadene til bestemmelsen i

forarbeidene.[108] Det framgår også av forarbeidene at «Bestemmelsen må også ses i sammenheng med sikkerhetsloven § 2-5 om vedtak ved risiko for skadevirkninger for nasjonale sikkerhetsinteresser slik disse er definert i sikkerhetsloven § 1-5. Den foreslåtte bestemmelsen om begrensinger i markedsadgang vil imidlertid omfatte sikkerhet ut over nasjonale sikkerhetsinteresser slik dette er definert i sikkerhetsloven. Andre viktige samfunnsinteresser omfatter både offentlig sikkerhet, helse eller andre særlige forhold. Det vil kunne forekomme situasjoner hvor det kan være aktuelt å fatte vedtak etter sikkerhetsloven § 2-5 og vedtak om å nekte adgang til markedet etter ekomloven».

Bestemmelsen er en videreføring av ekomloven fra 2003 § 2-10 tredje ledd (opprinnelig femte ledd). Det finnes imidlertid ingen omtale av bestemmelsen fra forarbeidene til den loven. Omfanget av bestemmelsen og forholdet til sikkerhetsloven § 2-5 framstår som uklart. Utvalget antar at bestemmelsen først og fremst er aktuell å ta i bruk overfor virksomheter hjemmehørende i en stat utenfor EØS som Norge ikke har sikkerhetspolitisk samarbeid med, eller overfor en virksomhet hjemmehørende innenfor EØS som har eller får eiere som er hjemmehørende i stater Norge ikke har slikt samarbeid med.

Mens sikkerhetsloven § 10-3 gir Kongen i statsråd adgang til å nekte erverve av en kvalifisert eierandel i en virksomhet som er underlagt loven, vil ekomloven § 3-5 gi departementet hjemmel til å nekte enhver tilbyder der eierandeler er blitt kjøpt opp, adgang til markedet, og dermed stanse virksomheten hvis man anser at virksomheten vil utgjøre en nasjonal sikkerhetsrisiko etter oppkjøpet. Utvalget antar at det også kan være aktuelt å bruke ekomloven § 3-5 dersom en tilbyder overfører rådigheten over hele eller deler av sin infrastruktur til en virksomhet hjemmehørende i land Norge ikke har sikkerhetspolitisk samarbeid med. I slike tilfeller er det ikke snakk om å selge eierandeler i virksomheten, men eierskap til innhold i virksomheten – altså tilfeller som ikke er omfattet av sikkerhetsloven § 10-3. Det følger av ekomloven § 5-4 at dersom tilbyderen som avhender hele eller vesentlige deler av aksessnettet, har leveringsplikt, har tilbyderen plikt til å varsle departementet på et tidspunkt som gir departementet mulighet til å vurdere konsekvensene av avhendelsen og behovet for å begrense markedsadgangen.

Ekomloven § 3-8 første ledd åpner for at myndigheten kan pålegge en tilbyder eller en datasenteroperatør å gjennomføre begrensninger i bruken av elektroniske kommunikasjonsnett og -tjenester, eller i datasentertjeneste, av hensyn til nasjonal sikkerhet eller andre viktige samfunnsinteresser. I avgjørelsen av om bruksbegrensning skal pålegges, må det tas hensyn til at brukere av tjenestene kan bli stående uten kommunikasjonstjenester eller datasentertjenester i en periode. I vurderingen av om pålegg skal gis, må hensynet til nasjonal sikkerhet og andre viktige samfunnshensyn veies mot de sikkerhets- og samfunnsmessige konsekvensene en bruksbegrensning kan ha for de berørte. Det betyr at det er en viss terskel for å pålegge bruksbegrensninger.

Etter *annet ledd* i bestemmelsen skal tilbyder og datasenteroperatør gjennomføre nødvendige bruksbegrensninger i nødssituasjoner som innebærer alvorlige trusler mot liv eller helse, nasjonal sikkerhet eller offentlig orden, eller fare for sabotasje mot datasenter, nett eller tjeneste. Knyttet til de aktuelle nødsituasjonene, må tilbyder eller datasenteroperatør selv ta stilling til om det foreligger fare for sabotasje mot nett eller tjenester. Når det gjelder alvorlige trusler mot liv eller helse så kan tilbyder

[108] Prop. 93 LS (2023–2024) side 279.

eller datasenteroperatør selv ta stilling til dette, eller det kan skje i samarbeid med myndigheter. I praksis vil også bruksbegrensninger knyttet til trusler mot nasjonal sikkerhet eller offentlig orden, iverksettes i samråd med tilsynsmyndigheten. Dersom tilbyder eller datasenteroperatør iverksetter bruksbegrensning uten konsultasjon med tilsynsmyndigheten, skal de straks varsle myndigheten.

9.3.6 Digitalsikkerhetsloven

Digitalsikkerhetsloven gjennomfører Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (NIS-direktivet). Loven er også et utgangspunkt for videre kravstilling og regulering innen digital sikkerhet. Direktivet og tilhørende gjennomføringsforordning[109] ble besluttet tatt inn i EØS-avtalen 3. februar 2023. Samme dag ble også forordningen om ENISA[110], om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi tatt inn i EØS-avtalen. Forordningen er planlagt inkorporert i forskrift til digitalsikkerhetsloven

Loven ble vedtatt i desember 2023, men er ennå ikke trådt i kraft fordi forskriften til loven ikke er ferdig. Utkast til forskrift har vært på høring med frist 11. desember 2024, og Justisdepartementet jobber nå med å ferdigstille forskriften. Loven gjelder ikke for tilbydere av tilgang til elektronisk kommunikasjonsnett eller -tjeneste samt datasentre – for disse gjelder ekomlovens regler om sikkerhet. I utkastet til forskrift, er imidlertid visse tjenester innenfor digital infrastruktur foreslått omfattet av samfunnsviktige tjenester i digitalsikkerhetsloven § 2. Dette gjelder sentralt register over norske toppnivådomener (Norid), rekursiv navneservertjeneste (tjeneste innenfor domenenavnsystemet (DNS)) med flere enn 50 000 aktive brukere, samt samtrafikkpunkter for internett.

Loven stiller krav til forebyggende digital sikkerhet hos virksomheter som leverer samfunnsviktige eller digitale tjenester innen en rekke ulike sektorer, herunder for sektoren digital infrastruktur. Virksomhetene blir også pålagt en varslingsplikt ved alvorlige hendelser som rammer deres nettverk eller informasjonssystemer, og som er egnet til å forstyrre leveransen av en samfunnsviktig tjeneste. Digitalsikkerhetsloven stiller grunnleggende krav om forsvarlig sikkerhet i nettverk og informasjonssystemer som ligger til grunn for leveransen av en samfunnsviktig tjeneste. Sikkerhetstiltakene skal være risikobaserte, som igjen forutsetter at virksomheten utarbeider risikovurderinger av nettverk og informasjonssystemer. Virksomheter som er underlagt sikkerhetsloven og eller regulert i ekomloven, er allerede underlagt krav til forsvarlig sikkerhet gjennom disse regelverkene.

I november 2022 vedtok EU direktiv (EU) 2022/2555, et nytt direktiv (NIS2-direktivet) som opphever NIS1. Det nye NIS-direktivet fikk virkning fra 24. oktober 2024 i EU. NIS2-direktivet er foreløpig ikke tatt inn i EØS-avtalen, men det fremgår av Totalberedskapsmeldingen at regjeringen forbereder gjennomføring av direktivet i norsk rett. Innlemmelse av NIS2-direktivet i EØS-avtalen vil medføre behov for enderinger i regelverket.

[109] Forordning 2018/151 om spesifisering av NIS-direktivet artikkel 16 nr. 1 og nr. 4, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0151

[110] Europaparlaments- og rådsforordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions cybersikkerhetsbyrå), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

9.3.7 Beredskapslovgivning

Dersom det oppstår en sikkerhetspolitisk krise eller krig – altså situasjoner øverst i krisespennet – vil det kunne være behov for at staten kan trekke på samfunnets samlede ressurser for å understøtte forsvaret av landet, ivareta sivilsamfunnets grunnleggende funksjonalitet og beskytte sivilbefolkningen. For å understøtte dette behovet finnes det ulike beredskapsregelverk der regjeringen blant annet gis adgang til å regulere tilgang til sivile beredskapskapskapasiteter gjennom definert rammelovgivning som er fastsatt på forhånd. Dette bygger på at forhåndsutarbeidet rammelovgivning om sivil beredskap er å foretrekke fremfor gjennomføring av tilsvarende tiltak når krisen oppstår med hjemmel i generelle unntaksregler som beredskapslovens system eller med forankring i konstitusjonell nødrett. Utvalget antar at deler av beredskapslovgivningen kan bli aktuell å benytte i en situasjon der tilgang til tjeneste i kritisk digital kommunikasjonsinfrastruktur står i fare eller ikke er tilgjengelig.

Beredskapsloven regulerer vilkår for utøvelse av nødrett i lovs form, og begrunnelsen for loven er at myndighetsutøvelse i nødssituasjoner burde reguleres nærmere før nødsituasjonen inntrer. Loven er en utpreget fullmaktslov som blant annet gir Kongen vide fullmakter i situasjoner som krig i riket eller hvis krig truer, eller rikets selvstendighet eller sikkerhet er i fare.

Næringsberedskapsloven er en tverrsektoriell lov med formål om «å avhjelpe forsyningsmessige konsekvenser av kriser ved å styrke tilgangen på varer og tjenester og sørge for nødvendig prioritering og omfordeling av varer og tjenester gjennom samarbeid mellom offentlige myndigheter og næringsdrivende», jf. § 1. Dersom det oppstår risiko for eller er inntruffet kriser med forsyningsmessige konsekvenser, har Kongen etter § 6 en rekke forskriftshjemler til å regulere tilgang til og omsetning av varer og tjenester, samt pålegge næringsdrivende nærmere bestemte plikter, herunder fremstilling av varer, yting av tjenester eller midlertidig avståelse av løsøre og fast eiendom.

I Prop. 11 L (2024–2025) Endringer i sivilbeskyttelsesloven (sivil arbeidskraftberedskap) foreslås det et nytt kapittel VII A om sivil arbeidskraftberedskap. I proposisjonen sies det blant annet at:

> «Etter departementets vurdering vil det være helt nødvendig å prioritere arbeidskraften til de oppgavene og funksjonene som det er størst behov for i en gitt situasjon. Dette vil på den andre siden kunne medføre at noen oppgaver som i en normalsituasjon skal ivaretas, ikke får tilsvarende prioritet. De sentrale funksjonene som må prioriteres opprettholdt på sivil side er understøttelse av forsvaret av landet, ivaretakelse av sivilsamfunnets grunnleggende funksjonalitet og beskyttelse av sivilbefolkningen. De mest kritiske leveransene til befolkningen er typisk rent drikkevann, matforsyning, varme og grunnleggende helsehjelp. Disse leveransene fordrer gjerne fungerende infrastruktur som kommunikasjonsinfrastruktur, transportinfrastruktur, strøm med videre».

9.3.8 Lov om militære rekvisisjoner

Rekvisisjonsloven med forskrift gir militære myndigheter lov til å rekvirere utstyr som er nødvendig i krig eller når krig truer. Loven skal sikre Forsvarets stridsevne og gir blant annet hjemmel til å rekvirere disposisjonsrett over sambandsmidler, jf. rekvisisjonsloven § 1 første ledd nr. 3. Etter nr. 5 kan det også rekvireres «arbeids- og produksjonsytelser» av virksomheter og bedrifter som nevnt i nr. 3, og av nr. 6 følger at militære myndigheter kan rekvirere «[a]rbeid og annen tjeneste for krigsmakten og institusjoner som er knyttet til den (...)». Det omfatter for eksempel rekvirering av arbeidskraft fra en bedrift til bruk i en annen slik at denne kan drives i flere skift i samsvar med forsvarsmaktens behov.

Rekvisisjonsordningen skal bidra til å sikre Forsvaret stridsevne.

9.4 Statlige overføringer

Offentlige myndigheter kan gjennom overføringer gi støtte til enkelte virksomheter eller enkelte næringer for eksempel i form av direkte kapitaloverføringer, reduserte skattesatser eller støtte gjennom billige lån eller andre innsatsfaktorer. Knyttet til nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur, kan overføringer i første rekke være aktuelt å bruke for å styrke sikkerheten i slik infrastruktur, men også for å sikre infrastrukturutbygging slik at flest mulig får tilgang til ekomtjenester.

Reglene om statsstøtte i EØS-avtalen, som gjelder på alle områdene som EØS-avtalen regulerer, skal hindre at offentlige myndigheter tilgodeser enkelte foretak eller næringer fremfor andre på en måte som påvirker samhandelen negativt. Utgangspunktet etter EØS-avtalen er at statsstøtte er forbudt, jf. avtalen artikkel 61(1). EØS-avtalen har likevel ulike regler som på nærmere vilkår åpner for å gi statsstøtte. Utvalget går ikke inn på de ulike ordningene som åpner for statsstøtte, men viser til at det åpnes for støtte til visse tjenester av allmenn økonomisk betydning som myndighetene anser som særlig viktige for innbyggerne og som ikke vil bli levert på en tilfredsstillende måte av markedet alene.

I ekomloven § 3-1 sjette ledd gis departementet hjemmel til å fatte enkeltvedtak eller inngå avtale om gjennomføring av tiltak for å sikre oppfyllelse av nasjonale behov for sikkerhet, beredskap og funksjonalitet i elektroniske kommunikasjonsnett og -tjenester utover det som følger av første ledd. Vedtak kan rettes mot eller avtale kan inngås med virksomhet som tilbyr elektronisk kommunikasjonsnett eller – tjeneste, eller tilbyr tilhørende fasilitet og tilhørende tjeneste, herunder virksomhet som har ansvar for passiv infrastruktur. I praksis gjennomføres slike tiltak ved at det inngås avtaler mellom Nkom og tilbydere. Tilsvarende gjelder for sikkerhet i datasentre – «Departementet kan fatte enkeltvedtak eller inngå avtale om gjennomføring av tiltak for å sikre oppfyllelse av nasjonale behov for sikkerhet, beredskap og funksjonalitet i datasentre utover det som følger av andre ledd» (jf. ekomloven § 3-7 fjerde ledd).

Det er her snakk om å inngå avtale om, eller eventuelt pålegge tilbydere, å gjennomføre tiltak som går utover det som faller inn under begrepet forsvarlig sikkerhet i ekomloven § 3-1 første ledd og § 3-7 første ledd og som henholdsvis tilbyder og datasenteroperatør må dekke selv. Tilbyders og datasenteroperatørs merkostnader knyttet til slike ytterligere tiltak kompenseres av staten. Hvert år bevilger Stortinget midler i statsbudsjettet som skal styrke beredskapsevnen og gjøre ekomnettene mer robuste. For 2025 ble

det bevilget 195,1 mill. kroner til slike tiltak. I Prop. 1 S (2024–2025) Digitaliserings- og forvaltningsdepartementet side 89 flg.[111] er ordningen nærmere beskrevet. Om målet for ordningen står det:

> «Det er eit mål med auka beredskap i krisesituasjonar og ved hendingar. Beredskapsavtaler med utvalde tilbydarar sørgjer for administrative og organisatoriske beredskapstiltak, lagring og vedlikehald av transportabelt beredskapsutstyr og investeringar i ekominfrastruktur og beredskapsmateriell. Dette skal bidra til auka beredskap i krisesituasjonar.
>
> Eit anna mål er at utbygging av forsterka ekom i nye kommunar skal bidra til vesentleg forbedra sikkerheit og beredskap for den lokale kriseleiinga og befolkninga i tilfelle med langvarige straumbrot.
>
> I tillegg er det eit mål at styrking av transportnetta gjennom fleire alternative føringsvegar og forsterking av viktige punkt i infrastrukturen gir vesentleg auka beredskap i sårbare regionar.».

Midler har blant annet blitt brukt til Nkoms program for forsterket ekom for å styrke den fysiske robustheten i den digitale grunnmuren ved å sikre nødstrøm i minimum 72 timer til basestasjoner som dekker et utpekt område i en rekke kommuner. Videre har staten for å bøte på sårbarheten og øke sikkerheten for kommunikasjon mellom Norge og utlandet, gitt støtte til utbygging av sjøfiberkabelen mellom Kristiansand og Esbjerg i Danmark.

Offentlig støtte til bredbåndsutbygging er et annet virkemiddel for å stimulere til utbygging av bredbånd i områder hvor det ikke er kommersielt lønnsomt å bygge ut digital infrastruktur. I slike områder kan stat, fylkeskommune og kommune, etter gitte kriterier gi offentlig tilskudd til utbygging av bredbånd. For 2025 er det bevilget 415,6 millioner kroner til utbygging av høyhastighetsbredbånd for en sikker og fremtidsrettet digital infrastruktur.

9.5 Kontrakt og avtaler

Enhver kan ved avtale forplikte seg til å gjøre eller unnlate noe. Det gjelder også for private parter i deres relasjoner med staten. Det offentlige kan inngå privatrettslige avtaler på linje med enhver person eller privat virksomhet. Staten kan derfor gjennom avtalevilkår sikre at virksomheter som leverer infrastruktur eller tjenester, forplikter seg til ha bestemte organisasjonsstrukturer, å handle på bestemte måter, eller unnlate å foreta visse handlinger. Offentlig sektor, både på kommunalt-, fylkeskommunalt og statlig nivå, gjennomfører anskaffelser av ekomtjenester og utgjør samlet en stor kjøpergruppe. Komplekse offentlige anskaffelser av ekomtjenester skal i tillegg til konkurransemessige forhold, også ivareta viktige aspekter av juridisk, kommersiell, teknisk og sikkerhetsmessig art, som må vurderes og balanseres utfra det behov som skal dekkes, og hva slags type løsning som skal anskaffes. Å forsikre at de sikkerhetsmessige aspektene ved en anskaffelse er ivaretatt og i tilstrekkelig grad vektet, vil kunne bidra til sterkere nasjonal kontroll.

[111] https://www.regjeringen.no/no/dokumenter/prop.-1-s-20242025/id3057309/?ch=2

Anskaffelsesregelverket som kommer til anvendelse dersom den økonomiske verdien av anskaffelsen overstiger 100 000 kroner, er for øvrig et eksempel på at forvaltningen kan være underlagt omfattende saksbehandlingsregler som ikke gjelder for private, også der forvaltningen inngå avtaler på rent privatrettslig grunnlag, og dessuten at forvaltningslovens alminnelige regler om inhabilitet og taushetsplikt også får betydning.

For virksomheter som eier eller leverer kommunikasjonstjenester i kritisk digital infrastruktur, vil kontrakter være det viktigste virkemiddelet til å sikre kontroll med underleverandører.

Den sikkerhetsmessige situasjonen kan endre seg, og det er viktig at kontrakter gir rom for å håndtere en situasjon med økt trusselnivå. Sikkerhetsklausuler i avtaler må derfor ivareta dette. Det kan for eksempel tas inn i kontrakten at leverandør skal varsle om eierskifte i virksomheten og andre hendelser av betydning for sikkerhet. Samtidig bør kontrakten regulere mekanismene for slik varsling og hvilke konsekvenser slike hendelser skal ha dersom slike hendelser inntrer.

En virksomhet som er underlagt sikkerhetsloven, må etterleve sikkerhetslovens regler i kapittel 9 når det gjelder sikkerhetsgraderte anskaffelser – det vil si når anskaffelsen «innebærer at leverandøren av varen eller tjenesten kan få tilgang til eller tilvirker sikkerhetsgradert informasjon, jf. § 5-3, eller få tilgang til et skjermingsverdig objekt eller infrastruktur, jf. § 7-1». Dette innebærer blant annet krav om sikkerhetsavtale, leverandørklarering og at virksomhetene pålegges en varslingsplikt ved sikkerhetsgraderte anskaffelser. En offentlig virksomhet som foretar en anskaffelse som er underlagt både regelverket om offentlige anskaffelser og sikkerhetsloven, bør allerede ved utformingen av konkurransegrunnlaget ta stilling til om en leverandør vil kunne få tilgang til sikkerhetsgradert informasjon, skjermingsverdig objekt eller infrastruktur, og hvilke av sikkerhetslovens krav leverandøren må kunne oppfylle ved anskaffelsen.

Siden muligheten til å gjennomføre tvangstiltak når det gjelder vilkår fastsatt i kraft av myndighetsutøvelse utenfor Norge er begrenset, peker Eriksen (2024) i sin rapport på muligheten til å fastsette vilkår i en avtale framfor gjennom myndighetsutøvelse, fordi en avtale gir større mulighet for å gjennomføre tvangstiltak når aktøren er bosatt eller hjemmehørende i utlandet. Han sier på side 53 at «Selv om staten ikke kan kreve fullbyrdet forvaltningsvedtak gjennom Lugano-konvensjonen og New York-konvensjonen, kan staten likevel påberope seg konvensjonene når staten har inngått privatrettslig avtaler med virksomheter i andre land, og det er aktuelt å begjøre tvangsfullbyrdelse av avtalevilkårene». Forutsetningen for å pålegge vilkår i en avtale, er imidlertid at det ikke gjelder vilkår fastsatt i kraft av offentlig myndighetsutøvelse, det vil si plikter som norske myndigheter ensidig pålegger private parter. Han sier på side 7:

> *«Staten har avtalefrihet og kan i utgangspunktet inngå avtaler med enhver privat part, også utenlandske virksomheter om forhold staten ikke har jurisdiksjon over. Når staten inngår avtaler med virksomheter om forhold som ligger utenfor norsk jurisdiksjon, kan staten heller ikke utøve offentlig myndighet ved avtaleinngåelsen. Såfremt staten uten utøvelse av offentlig myndighet oppnår enighet med utenlandske virksomheter om vilkår for deres eierskap eller kontroll over kritisk digital infrastruktur i Norge, kan vilkårene både gjelde strukturelle og adferdsbaserte forhold».*

Når det offentlige inngår avtaler med private parter, kan det dreie seg om privatrettslige avtaler i den forstand at avtalen kunne vært inngått også mellom to private avtaleparter, eller avtaler der et forvaltningsorgan handler på vegne av det offentlige og det dreier seg om offentlig myndighetsutøving. Utvalget er av den oppfatning at for eksempel en avtale om å tillate at en utenlandsk aktør erverver eierandeler i et norsk selskap som eier kritisk digital kommunikasjonsinfrastruktur, mot at erverver godtar visse vilkår, må anses som myndighetsutøvelse. Både formålet med en slik avtale og balansen i avtalen gjør at den ikke har preg av å være en privatrettslig avtale, men en fordeling av rettigheter og plikter under utøving av offentlig myndighet.

9.6 Informasjon, rådgiving, dialog og samarbeid

Det følger av forvaltningsloven § 11 at forvaltningsorganer innenfor sitt saksområde har en alminnelig veiledningsplikt. Formålet med veiledningen skal være å gi parter og andre interesserte adgang til å vareta sine interesser *i bestemte saker* på best mulig måte. I denne sammenheng er det imidlertid snakk om å gi råd, veiledning og informasjon samt ha dialog og samarbeid uten at det er knyttet til en bestemt sak forvaltningen har til behandling.

Eiere av kritisk digital kommunikasjonsinfrastruktur har – fordi nettene er bærere av svært viktige tjenester for samfunnet – et sentralt ansvar for samfunnssikkerheten. For å sikre at dette ansvaret ivaretas pålegges virksomhetene plikt til å sørge for et forsvarlig sikkerhetsnivå først og fremst gjennom regulering. Dialog og samarbeid mellom det offentlige og det private kan imidlertid også brukes for å sikre at private styrer virksomheten på en måte som både oppfyller virksomhetens egne behov samtidig som den ivaretar samfunnssikkerhet. Dette kan for eksempel være informasjon og rådgivning om plikter og rettigheter, holdningsskapende informasjon, informasjon knyttet til særskilte hendelser eller informasjon om trussel- og risikovurderinger og andre opplysninger som er viktige både for sikkerhetsarbeidet i den enkelte virksomhet og i samfunnet for øvrig. Deling av informasjon for å få felles forståelse av risikoer i hele krisespennet, felles situasjonsforståelse og kartlegging av tilgjengelige ressurser for krisehåndtering og gjenoppretting, vil åpenbart styrke beredskapsfunksjonen og dermed bidra til nasjonal kontroll av kritisk digital kommunikasjonsinfrastruktur.

Som virkemiddel kan informasjon virke alene eller sammen med andre virkemidler – som et eksempel på det siste vil være informasjon om rettigheter og plikter som følger av regulering på et område.

I enkelte tilfeller følger det en veiledningsplikt i regelverket. Etter sikkerhetsloven § 2-2 annet ledd bokstav d følger det at NSM skal «gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid og krav til tiltak». I merknadene til bestemmelsen i Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet (sikkerhetsloven)[112] står det at «I bokstav d reguleres sikkerhetsmyndighetens råd- og veiledningsansvar etter loven. Sikkerhetsmyndigheten skal ha en aktiv rolle når det gjelder konkret rådgivning overfor virksomhetene. Av ressursmessige og praktiske grunner forutsetter departementet at slik rådgivning fortrinnsvis gis gjennom generelle veiledere og felles kursopplegg o.l.». NSM har utdypet myndighetens regelverkforståelse og sammenhengen mellom

[112] Prop. 153 L (2016–2017) side 167, https://www.regjeringen.no/contentassets/0fcee45affd24280896b88b5413a00aa/no/pdfs/prp201620170153000dddpdfs.pdf

ulike bestemmelser i sikkerhetsloven og tilhørende forskrifter gjennom en rekke veiledningsdokumenter. NSM har myndighet og ansvar som sikkerhetsmyndighet etter sikkerhetsloven, mens Nkom er sektormyndighet. NSM og Nkom har inngått en samarbeidsavtale om at Nkom har veiledningsansvar og skal gi råd og veiledning om hvordan bestemmelser og tiltak kan tilpasses sektorens egenart.

Knyttet til tilbydernes fremtidige utbygging av 5G-nett og for å gi forutsigbarhet for fremtidige anskaffelser, var det allerede i planleggingsfasen av utbyggingen dialog mellom myndighetene og mobiltilbyderne om å gjennomføre forebyggende sikkerhetstiltak for å sørge for et «forsvarlig sikkerhetsnivå» og redusere risikoen knyttet til sikkerhetstruende virksomhet. Før tilbyderne hadde konkludert i sine anskaffelsesprosesser, valgte departementet å konkretisere hva som vil bli ansett som forsvarlig sikkerhet når det kommer til utstyrsleverandører til 5G, for å gi større grad av forutsigbarhet når virksomhetene skulle treffe investeringsbeslutninger. Departementet utelukket ikke spesifikke leverandører fra det norske markedet, men formålet var åpenbart å sikre at det kinesiske selskapet Huawei ikke kunne velges som eneste leverandør når kravet til «forsvarlig sikkerhet» innebærer at minst 50 prosent av basestasjonene skal være fra land Norge har sikkerhetsavtale med.

Dialog og samarbeid kan bidra til kompetanse og bevisstgjøring om sikkerhet både hos virksomhetene og hos myndighetene, og offentlig-privat samarbeid kan på den måten styrke det nasjonale arbeidet for digital sikkerhet. Hvorvidt virksomhetene vil sette i gang tiltak på grunnlag av dialog med myndigheter, vil imidlertid i mange tilfeller være avhengig av hva konsekvensene av å ikke gjøre anbefalte tiltak, er. Myndighetenes mulighet til å treffe vedtak om et aktuelt tiltak – altså at manglende frivillig oppfyllelse kan tvinges gjennom med pålegg med hjemmel i lov – vil åpenbart ha betydning. Tilsvarende vil myndigheters mulighet til bruk av økonomiske støtteordninger kunne bidra til igangsetting av tiltak som ellers ikke hadde blitt gjennomført.

I en tid med stadige endringer i den sikkerhetspolitiske situasjonen kan det være krevende for virksomheter å opprettholde et forsvarlig sikkerhetsnivå gjennom hele krisespennet. Tilstrekkelig informasjon fra myndighetene kan bedre næringslivets mulighet til og kunnskap om å sikre egne verdier og bli mindre sårbare. Åpenhet om trussel- og risikovurderinger kan gjøre både virksomhetene og myndigheten i bedre stand til å vurdere både om det bør settes i gang tiltak og eventuelt hvilke tiltak. Det er derfor viktig at relevante myndigheter både har rammer, ressurser og vilje til å dele informasjon av betydning for å ivareta nasjonal sikkerhet.

9.7 Internasjonalt samarbeid

Som det er pekt på i kapittel 7.4 har den geopolitiske utviklingen gjort behovet for nasjonal kontroll av kritisk digital kommunikasjonsinfrastruktur tydeligere. Samtidig medfører komplekse og dynamiske verdikjeder at det ikke er mulig med fullstendig nasjonal kontroll.

St. meld. 9 (2022–2023)[113] framhever at i en internasjonal økonomi og et digitalisert samfunn, hvor avhengigheter, virkemiddelbruk og trusselaktører ikke forholder seg til landegrenser, er det viktig med internasjonalt samarbeid for å oppnå nasjonal kontroll.

[113] St. meld. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet* punkt 3.3.3.

Stortingsmeldingen trekker fram at dette blant annet innebærer å arbeide for ansvarlig statlig oppførsel i det digitale rom og søke å benytte eksisterende kanaler, som EUs screeningmekanisme, for tilgang til informasjon om sikkerhetstruende økonomisk aktivitet.

I en slik sammenheng kan samarbeid og tiltak som gjøres for å styrke sikkerhetsnivået hos samarbeidspartnere, bidra til å redusere risikonivået og gjøre behovet for nasjonal norsk kontroll mindre. Delvis gjennom at regional kontroll reduserer risikoen ved manglende nasjonal kontroll og delvis gjennom at internasjonalt regelverk og standarder medfører en forutsigbarhet som reduserer sikkerhetsrisiko.

9.7.1 NATO

Norge er avhengig av internasjonalt samarbeid for å stå imot grenseoverskridende trusler. Medlemskapet i NATO er grunnleggende for forsvaret av Norge, vår evne til å avskrekke mot angrep og forebygge konflikt. NATOs kollektive forsvar bygger på at medlemslandene også har en godt fungerende sivil beredskap og motstandsdyktige kritiske samfunnsfunksjoner og infrastruktur. Motstandskraft krever tett sivil-militært samarbeid, og sivile ressurser og infrastruktur er sentralt for NATOs motstandskraft. Det er derfor utarbeidet retningslinjer og konkrete mål om at medlemslandene skal sikre:

1. kontinuitet for styresmaktene og kritiske offentlige tjenester,
2. en robust kraftforsyning,
3. evnen til å håndtere ukontrollert forflytning av mennesker,
4. robust mat- og vannforsyning,
5. evnene til å håndtere masseskadesituasjoner,
6. robuste sivile kommunikasjonssystemer, og
7. robuste transportsystemer.[114]

Robusthet i sivil digital kommunikasjonsinfrastruktur er altså en del av denne beredskapen. NATO har i denne sammenheng hatt særlig fokus på beskyttelse av undersjøisk infrastruktur fordi slik infrastruktur er kritisk for både stabiliteten i økonomien, samfunnssikkerheten og forsvaret av alliansen. I mai 2024 åpnet NATO et nytt maritimt senter for sikkerhet i kritisk undersjøisk infrastruktur.[115] Initiativet bygger blant annet på et tysk-norsk forslag om å styrke NATOs rolle i å beskytte undersjøisk infrastruktur fra november 2022. Under NATOs forsvarsministermøte 17. oktober 2024 signerte forsvarsministrene fra Norge og Tyskland en felles uttalelse hvor partene tar ytterligere initiativ til å styrke NATOs rolle i beskyttelsen av kritisk undersjøisk infrastruktur, ved at det opprettes regionale sentre for ulike havområder som skal overvåke undersjøisk infrastruktur og avdekke mistenkelige aktiviteter og avskrekke potensielle motstandere.[116] I januar 2025 annonserte utenriksminister Espen Barth Eide at Norge sammen med USA og våre nordisk-baltiske allierte er enige om fire konkrete tiltak som skal øke sikkerheten for undersjøisk infrastruktur.[117] Tiltakene gjelder informasjonsdeling, partnerskap mellom offentlige og private virksomheter for å forbedre reparasjons- og vedlikeholdskapasiteten, informasjonsdeling mellom kommersielle operatører om utilsiktede kabelfeil og skader,

[114] NATOs «Seven baseline requirements» vedtatt på toppmøte i Warszawa i 2016.

[115] https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui

[116] https://www.regjeringen.no/no/aktuelt/nytt-norsk-tysk-initiativ-skal-styrke-kritisk-undersjoisk-infrastruktur-i-europa/id3061340/

[117] https://www.regjeringen.no/no/aktuelt/skal-sikre-tryggere-havbunn/id3083648/

utført reparasjonsarbeid, samt å effektivisere prosessene for import og eksport og legge til rette for raskere transport av nødvendig kommersielt utstyr.

9.7.2 Europeisk samarbeid

Ved siden av NATO, er EU Norges viktigste samarbeidspartner i sikkerhetspolitiske spørsmål. Det sikkerhets- og forsvarspolitiske samarbeidet omfattes ikke av EØS-avtalen. Det er likevel klart at Norge bygger sin sikkerhet ikke bare gjennom NATO-samarbeidet, men også gjennom tett samarbeid med EU.

EØS-avtalen er den mest omfattende internasjonale avtalen Norge har inngått. Tidligere var EUs sentrale fokus å utvikle et velfungerende marked mellom medlemsstatene, mens man nå ser at en dreining mot at det handler mer om hvordan EU som fellesskap skal møte de store utfordringene og forsvare felles interesser. EUs betydning for europeisk sikkerhet – og norsk sikkerhet – har økt etter Russlands invasjon av Ukraina. I den grad EU gjennom ulike initiativer tar ansvar for europeisk sikkerhet, vil et tett samarbeid med EU også styrke sikkerheten i Norge.

Kommisjonen presenterte i februar 2024 en såkalt «hvitbok» med en rekke forslag til tiltak for å fremme innovasjon, sikkerhet og motstandsdyktighet i digital infrastruktur. Bakgrunnen er at utrulling av nye viktige, digitale tjenester i samfunnet, avhenger av konnektivitet som er sikker, har høy kapasitet og er tilgengelig for alle. Det er ventet at Europakommisjonen i 2025 vil følge opp dette arbeidet der målet er å fremme felleseuropeiske ekomtjenester og infrastruktur, sikre investeringer i digital infrastruktur og sikre motstandsdyktig infrastruktur. Samtidig med hvitboken, la Kommisjonen fram en anbefaling knyttet til sikkerhet og motstandsdyktighet i sjøfiberkabler. Utvalget mener det er viktig at departementet følger disse prosessene tett og kopler Norge på eventuelle nye samarbeidsprosjekter knyttet til sikkerhet og motstandsdyktighet i digital infrastruktur. Det er også viktig at et eventuelt nytt EØS-relevant regelverk gjennomføres raskt i Norge.

Norge og EU inngikk i mai 2024 en partnerskapsavtale[118] om forsvar – og sikkerhetssamarbeid. Partnerskapsavtalen bekrefter Norges status som en av EUs nærmeste partnere. Avtalen er ikke folkerettslig bindene, men stadfester det allerede pågående samarbeidet Norge og EU har på forsvars- og sikkerhetsområdet og gir Norge og EU en struktur for dialog og konsultasjoner. Formålet med partnerskapet er blant annet å styrke samarbeidet om krisehåndtering, forsvarsindustri, romsamarbeid, kritisk infrastruktur og hybride trusler. Knyttet til «Resilience of critical infrastructure» sier avtalen:

> «31. Norway and the EU will strengthen consultations on their respective approaches to enhance the resilience of critical infrastructure in Europe, including underwater infrastructure. The EU will base its efforts on the EU Directive on the Resilience of Critical Entities and the Council recommendation on a Union wide coordinated approach.»

EU kobler nå i langt større grad ulike saksområder til målet om et mer sikkert, motstandsdyktig og selvforsynt EU. Samarbeidet mellom de 27 medlemslandene utvikles

[118] https://www.regjeringen.no/contentassets/abc084fe921e403791ddb505622ba365/eu-norway-security-and-defence-partnership.pdf

raskt på områder som ikke dekkes av EØS-avtalen og Norges øvrige avtaleverk med EU. Det skaper et nytt sett av utfordringer som krever større grad av samordning.

Man ser også at EØS-avtalens regler om de fire friheter får betydning for regelverk som ligger utenfor avtalen. Det er derfor viktig å se hen til hvordan EUs regler som ivaretar sikkerhet utformes, for å sikre at norske regler som skal ivareta nasjonal kontroll ikke kommer i konflikt med våre forpliktelser etter EØS-avtalen. Nasjonale tiltak vil også, når de harmoniseres og håndheves likt med EU-tiltak, bedre ivareta konkurransemessige og økonomiske konsekvenser av tiltakene for norske virksomheter, og dermed begrenses eventuelle negative effekter.

EØS-avtalen er en dynamisk avtale som løpende oppdateres. Når nye rettsakter vedtas i EU, skal regelverket som er omfattet av EØS-avtalens virkeområde, også tas inn i EØS-avtalen, slik at regelverket blir likt i EU- og EØS EFTA -landene. Nytt EØS-relevant regelverk skal etter avtalen artikkel 102 innføres «så nær som mulig i tid» etter vedtak av tilsvarende regelverk i EU. Forsinkelser i implementering og gjennomføring av EU-regelverk kan, i tillegg til å være et problem for næringslivet som kan oppleve uklarhet om plikter og rettigheter og være negativt både for investeringer og etableringer, også medføre svekket tillit i samarbeidet mellom EU- og EØS EFTA-landene, og kan få som konsekvens at sikkerhetssamarbeidet generelt svekkes. Det vises i denne sammenheng til Eldringutvalget NOU 2024: 7 *Norge og EØS: Utvikling og erfaringer*, som peker på at etterslepet av rettsakter har økt de senere årene og at det på EU-siden skaper misnøye og kan oppfattes som «cherry-picking» fra Norge og de andre EØS EFTA-landenes side. Eldringutvalget sier at «Risikoen ved å bruke uforholdsmessig lang tid på innlemmelsesprosessen er at Norge og de andre EØS/EFTA-statene kan bli møtt med mottiltak fra EUs side».

Et svekket samarbeid med våre nærmeste samarbeidspartnere kan bli alvorlig, fordi Norge er avhengig av samarbeid med land – og leverandører fra land – som vi har tillit til, for å kunne sikre trygge og gode digitale tjenester. Om kontroll over kritisk digital infrastruktur oppfattes som dårligere enn hos våre sikkerhetspolitiske partnere, kan dette utfordre det bredere samarbeidet, skape friksjon og misnøye og begrense videre samarbeid.

9.7.3 Nordisk samarbeid

Etter Finlands og Sveriges inntreden i NATO, er forutsetningene for bredere sikkerhetspolitisk samarbeid i Norden endret. Gitt at robuste sivile kommunikasjonssystemer er viktig for NATOs kollektive forsvar, er det naturlig at det sikkerhetspolitiske regionale samarbeidet også omfatter samarbeid for å styrke motstandskraft og beredskap knyttet til kritisk digital kommunikasjonsinfrastruktur. Et slikt nordisk samarbeid bør især fokusere på felles nordiske løsninger på områder der landene kan oppnå bedre resultater ved å samarbeide enn ved å løse oppgavene hver for seg. Utvalget viser til at også tilbyderne mener nordisk samarbeid er viktig og at mulighetene for økt nordisk samarbeid som et risikoreduserende tiltak bør utforskes, spesielt innen sikkerhetsklarering og deling av ressurser og teknologi.

Norge samarbeider med våre nordiske naboland på digitaliseringsområdet blant annet innenfor rammene av Nordisk ministerråd. Det nordiske samarbeidet er i

mange sammenhenger utvidet til et nordisk-baltisk samarbeid. I tillegg til å styrke samarbeidet i denne regionen, gir det også Norge en mulighet til å sammen med disse samarbeidspartnerne, å få en felles stemme inn mot EU.

Akkurat som i NATO og EU, har samarbeid for å beskyttes undersjøisk kommunikasjonsinfrastruktur stått sentralt den senere tid. På nordisk-baltisk møte mellom digitaliseringsministrene i november 2024, ble grunnlaget for styrket samarbeid om kritisk kommunikasjonsinfrastruktur under vann, lagt. I en felleserklæring[119] uttalte ministrene blant annet:

> «With the ongoing policy development within the EU concerning subsea communication cables and an increased NATO cooperation, we the Nordic and Baltic Ministers of Digitalisation would like to highlight the importance of a joint Nordic-Baltic approach.
>
> To enable this, we the Nordic and Baltic Ministers for Digitalisation:
>
> **RECOGNIZE** that the underwater infrastructure for electronic communications constitute a critical infrastructure, essential for securing our countries' needs for connectivity and competitiveness in the international digital economy.
>
> **RECOGNIZE** that security considerations have become a more essential part in the design and implementation of subsea and land-based infrastructure.
>
> **ENCOURAGE** increased exchange between our countries in matters of joint interest concerning subsea communication cables.
>
> **EMPHASIZE** the need to ensure redundancy in subsea communication cables systems within our region as well as in the infrastructure for global connectivity.
>
> **EMPHASIZE** the importance of secure supply chains for the development, manufacturing, deployment, management, maintenance and repair of subsea communication cables for secure global connectivity and communication between the Nordic countries.
>
> **EMPHASIZE** the importance of joint international efforts, within and between the EU and NATO, in order to secure increased cable laying and repair capabilities and ensure the security of our critical infrastructure in the Nordic region.
>
> **RECOGNIZE** that the security and protection of subsea communication cables is a whole of government affair that requires civil-military as well as public-private collaboration.
>
> **RECOGNIZE** the importance of international cooperation concerning subsea communication cables and with this ENDORSE the New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World[120].»

[119] https://www.norden.org/en/declaration/joint-statement-nordic-and-baltic-ministers-digitalisation

[120] https://www.state.gov/joint-statement-on-the-security-and-resilience-of-undersea-cables-in-a-globally-digitalized-world/

New York-erklæringen om sikkerhet og motstandsdyktighet i undersjøiske kabler i en global, digitalisert verden, fastsetter globale prinsipper for å sikre at undersjøisk kabelinfrastruktur er sikker, pålitelig, bærekraftig og motstandsdyktig. Erklæringen ble initiert av USA i september 2024 og har senere fått sin tilslutning av en rekke land.

For å møte fremtidige utfordringer innenfor kommunikasjon, sikkerhet og infrastruktur, mener utvalget at det er viktig å benytte de nordiske landenes samlede ressurser på best mulig måte. Samarbeid mellom myndighetene i de nordiske landene kan styrke situasjonen for ekomtilbydere knyttet til de utfordringene som følger med globalisering, teknologisk utvikling og økende krav til robusthet i infrastrukturen. Det er for eksempel et økende press på å tiltrekke kompetanse, og samarbeid mellom landene kan fremme løsninger som gjør det lettere å benytte knappe personalressurser på tvers av landegrensene. Samarbeid som legger til rette for robuste felles løsninger knyttet til for eksempel transportnett og mobilkjernenett vil kunne styrke den tekniske infrastrukturen i regionen, sikre mer robust og integrert infrastruktur i Norden og dermed å styrke både nasjonal og regional sikkerhet i kommunikasjonsinfrastrukturer.

9.8 Oppsummering og tiltak

I dagens situasjon står Norge overfor sammensatte trusler som blant annet sikkerhetstruende økonomisk aktivitet og skadelig eierskap, digitale angrep og forstyrrelser, samt påvirkning, og det er nødvendig med ulike tiltak og virkemidler for å ivareta nasjonal kontroll. Regulering er fremhevet som det primære virkemiddelet for å sørge for nasjonal kontroll. Det krever at de aktuelle regelverkene oppdateres og endres i tråd med situasjonen i sektoren. Til dette kreves oversikt, innsikt og kunnskap. Det er derfor behov for samarbeid og informasjonsdeling både nasjonalt mellom myndigheter og aktører og mellom militær og sivil sektor, samt internasjonalt samarbeid fordi ulike aktører har relevant informasjon som samlet kan bidra til bred innsikt og forståelse av utfordringsbildet og som kan styrke beslutningsgrunnlag og styrke regulering som virkemiddel. Samtidig må forvaltere av regelverk ha ressurser og kompetanse til å gi råd og veiledning til relevante aktører som kontrollerer kritisk digital kommunikasjonsinfrastruktur slik at de er i stand til å etterleve reguleringen. Dette viser at selv om regulering er det sentrale virkemiddelet, styrkes dette virkemidlet når det brukes sammen med øvrige virkemidler. I arbeidet med å sikre nasjonal kontroll, må også virkemiddelbruken hele tiden balansere målet om å ivareta nasjonale sikkerhetsinteresser og samtidig sørge for at Norge forblir et attraktivt land å investere i.

I det internasjonale samarbeidet er EØS-avtalen og øvrig samarbeid med EU sentralt. EØS-relevant regelverk skal gjennomføres i norsk rett, og det er viktig å sikre at annet nasjonalt regelverk som skal ivareta nasjonal kontroll ikke kommer i konflikt med våre forpliktelser etter EØS-avtalen. Utvalget har på denne bakgrunn følgende forslag til tiltak:

> **«Utvalget mener at Digitaliserings- og forvaltningsdepartementet og Justis- og beredskapsdepartementet bør se til at EØS-relevant regelverk for digital kommunikasjonsinfrastruktur gjennomføres i Norge og at det skjer i så nær tid som mulig med tilsvarende regulering i EU.»**

Det er i flere sammenhenger uttalt at statlig eierskap er et virkemiddel som kan tas bruk i særskilte tilfeller. Samtidig sier regjeringen i Hurdalsplattformen at det er «avgjørende

at fellesskapet bruker statlig eierskap for å sikre nasjonal kontroll» og at «statlige eierskapet skal utvikles og forsterkes i omstillingen av norsk økonomi». Det pekes i denne sammenheng blant annet på kontroll av viktig infrastruktur.

Selv om staten allerede i dag begrunner eierskap utfra hensynet til samfunnssikkerhet og beredskap, er det ikke tydelig hvordan dette hensynet forvaltes gjennom eierskapet. På denne bakgrunn har utvalget følgende forslag til tiltak:

> **«Utvalget mener at når staten begrunner eierskap med å ivareta samfunnssikkerhet gjennom eierskap, må staten i forvaltningen av eierskapet være tydeligere på hvordan hensynet til samfunnssikkerhet og beredskap veies mot hensynet til avkastning, andre aksjonærer og for eksempel statsstøtteregler.»**

Kapittelet gir en beskrivelse av screeningregelverket i Sverige, Danmark og Finland. Mange vestlige land, inkludert de nordiske, har regelverk for å redusere sårbarheter knyttet til utenlandske investeringer som kan true nasjonale sikkerhetsinteresser. Dette som et motsvar mot enkelte staters økte bruk av sikkerhetstruende økonomisk aktivitet.

Foto: Adobestock

10

Screeningregelverk i sammenlignbare land

10.1 Innledning

Det følger av mandatet at *«Utvalget skal beskrive hvordan reguleringsregimer eller andre hensyn til nasjonal kontroll er ivaretatt i nordiske land»,* og i dette kapittelet gis en beskrivelse av screeningregelverket i Sverige, Danmark og Finland. Mange vestlige land, inkludert de nordiske, har regelverk for å redusere sårbarheter knyttet til utenlandske investeringer som kan true nasjonale sikkerhetsinteresser. Dette som et motsvar mot staters økte bruk av sikkerhetstruende økonomisk aktivitet. Det skilles gjerne mellom første- og andregenerasjons regelverk;

Førstegenerasjonsregelverk inneholder typisk en tillatelsesordning for investeringer i utpekte foretak eller i en avgrenset sektor, slik som vi har i Norge. Andregenerasjonsregelverk er mer omfattende og legger opp til løpende behandling av et større antall meldinger i henhold til faste kriterier og gjerne utført av en dedikert offentlig myndighet. De nordiske landene utvalget skal omtale i dette kapitlet er eksempler på land som har et andregenerasjons screeningregelverk.

Videre er det relevant å se til forordning (EU) 2019/452 om kontroll av utenlandske direkteinvesteringer som er EUs gjeldende regelverk for screening (ikke del av EØS-avtalen). Formålet bak dette regelverket er å etablere en felles tilnærming til kontrollen av investeringer fra land utenfor EU som kan utgjøre en sikkerhetsrisiko, og oppstiller noen minstekrav til hvordan nasjonale screeningregelverk skal utformes. Dermed vil vi se at Sverige, Danmark og Finlands screeningregelverk har mange likhetstrekk med hverandre da de bygger på EUs screeningregelverk. Etter en evaluering av det gjeldende screeningregelverket har man kommet frem til at mangel på harmonisering blant

medlemslandene er et problem, og i januar 2024 la Europakommisjonen frem et forslag til et nytt screeningregelverk. Dermed vil både EUs gjeldende screeningregelverk og forslaget til ny forordning også bli omtalt i kapittelet.

10.2 Sverige

Lagen om granskning av utländska direktinvesteringar (2023:560) trådte i kraft 1. desember 2023 og regulerer investeringskontrollen i Sverige. Formålet med loven er å hindre investeringer som kan ha skadelig effekt på Sveriges sikkerhet eller på offentlig orden eller offentlig sikkerhet. *Inspektionen för strategiska produkter (ISP)* er utpekt som kontrollmyndighet for utenlandske direkteinvesteringer i Sverige. ISP er et statlig organ som jobber med spørsmål knyttet til Sveriges forsvars-, sikkerhets- eller utenrikspolitikk. En stor del av deres arbeid er å kontrollere eksporten av enkelte produkter, med sikte på at verken produkter eller teknologi skal spres til uvedkommende. Investeringer som innebærer at en investor får betydelig innflytelse i skjermingsverdige aktiviteter skal meldes til ISP, som avgjør om investeringen må gjennomgås. Dersom dette er tilfelle, må ISP avgjøre om investeringen skal godkjennes, forbys eller tillates på vilkår. Den svenske loven dekker investeringer i virksomheter som er underlagt i syv ulike sektorer:

- Samfunnsviktig aktivitet
- Sikkerhetssensitive aktiviteter
- Kritiske råvarer, metaller eller mineraler
- Sensitive personopplysninger eller stedsdata
- Krigsmateriell eller teknisk støtte angående krigsmateriell
- Produkter med dobbelt bruksområde eller teknisk assistanse
- Fremvoksende teknologi eller annen teknologi som kan beskyttes strategisk[121]

Den svenske screeningen blir ikke gjennomført av et departement slik det er praksis for i de fleste andre land, men utføres som nevnt av det offentlige organet ISP, assistert av andre instanser. Den svenske grunnloven forbyr nemlig generelt regjeringen fra å påvirke beslutninger tatt av regjeringsinstanser i enkeltsaker. Av denne grunn, når ISP først behandler en sak, har ikke regjeringen lov til å påvirke om en spesifikk investering bør tillates eller ikke. Men en avgjørelse tatt av ISP, inkludert et forbud eller tillatelse på vilkår, kan påklages av investor til regjeringen. Dette kan bidra til å gjøre den svenske screeningsmekanismen mer transparent sammenlignet med land der beslutninger tas direkte av regjeringen. Alle involverte myndigheter må i tillegg sende inn sin mening skriftlig til ISP.[122]

Prosess

I Sverige er meldeplikt hos investor, og meldeplikten gjelder ikke kun for utenlandske investorer, men også svenske. Den som har til hensikt direkte eller indirekte å investere i en skjermingsverdig virksomhet, skal varsle ISP om investeringen dersom investeringen medfører at investor får en viss innflytelse i virksomheten. Investors meldeplikt starter dersom investoren etter investeringen, direkte eller indirekte, ville komme til å ha stemmer som tilsvarer eller overskrider visse terskler fastsatt i loven. Tersklene er 10, 20, 30, 50, 65 eller 90 prosent av stemmene i en skjermingsverdig virksomhet. ISP kan også

[121] https://www.isp.se/utlandska-direktinvesteringar

[122] https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2022/perspectives-on-the-economic-effects-of-fdi-and-investment-screening.pdf

sette i gang en granskning på eget initiativ. Slik egeninitiert granskning innebærer at også investeringer i skjermingsverdig virksomhet som ikke er meldepliktig, kan gjennomgås.

Prosessen for screening kan deles i to faser. I fase 1 er det en slags «prøvefase» hvor myndighetene har 25 dager på seg til å bestemme om investeringen kan ha *skadelig effekt på Sveriges sikkerhet eller på offentlig orden eller offentlig sikkerhet,* og om det er grunnlag for å innlede en granskning. Dersom man mener det er tilfelle, går man over til fase 2 hvor myndighetene har tre måneder på seg til å gjennomføre granskingen og beslutte å enten forby eller godkjenne investeringen. Dersom det foreligger særlige grunner, kan vedtaket meddeles innen seks måneder. I granskningsfasen foregår det en dybdeundersøkelse hvor myndighetene kan stille mer utdypende spørsmål til investoren, men også til selskapet som er gjenstand for investeringen. Begge disse skal på forespørsel fra ISP gi de opplysninger eller dokumenter som myndigheten trenger for sin gjennomgang.

Før ISP fatter vedtak i en sak, må myndigheten samarbeide med *Kommerskollegium, Försvarsmakten, Försvarets materielverk, Säkerhetspolisen och Myndigheten för samhällsskydd och beredskap*. Kommerskollegiumet er myndighet for utenrikshandel, EUs indre marked og handelspolitikk, og oppgaven er blant annet å bidra med dokumentasjon om investeringens betydning for økonomi, investeringsklima og dens handelspolitiske aspekter. Når granskningen er fullført, bestemmer ISP seg for å enten forby eller godkjenne investeringen. Investeringen kan også godkjennes på vilkår.

Samarbeid med Europakommisjonen
Europaparlamentets og Rådets forordning (EU) 2019/452 om kontroll av utenlandske direkteinvesteringer har en del felles prosedyrer for alle medlemsland som har et screeningregelverk. Blant annet skal alle medlemsland ha et kontaktpunkt mot Europakommisjonen, og ISP er Sveriges kontaktpunkt i samsvar med forordningen. Dette innebærer blant annet at ISP skal varsle Europakommisjonen og andre medlemsland om alle utenlandske direkteinvesteringer som vurderes av myndigheten.[123] Samarbeidsmekanismen og prosedyrene mellom Kommisjonen og medlemslandene i gjeldende EU-forordning er omtalt nærmere i punkt 10.5.1.

10.3 Danmark

I Danmark trådte Investeringsscreeningsloven i kraft 1. juli 2021. Loven har som formål å hindre at utenlandske direkteinvesteringer og spesielle økonomiske avtaler utgjør en trussel mot nasjonal sikkerhet eller offentlig orden i Danmark. Med utenlandsk investering forstås erverv av kontroll eller betydelig innflytelse i et selskap som er hjemme i Danmark, ved direkte eller indirekte besittelse av eller kontroll over eierandeler eller stemmerett i selskapet eller tilsvarende kontroll på annen måte, inkludert kjøp av eiendeler og langsiktige uoppsigelige lån (såkalte *særskilte økonomiske avtaler*). Utenlandske investeringer omfatter også investeringer ved etablering av nytt selskap i Danmark (såkalte greenfield-investeringer) i en særlig sensitiv sektor, hvor tilsvarende kontroll eller betydelig innflytelse oppnås.

[123] https://www.isp.se/utlandska-direktinvesteringar

Screeningsordningen er utformet som en kombinasjon av et lovpålagt tillatelseskrav for *spesielt sensitive sektorer* og en frivillig meldingsordning for de øvrige sektorene. Etter reglene om det sektorspesifikke tillatelseskravet må du som utenlandsk investor innhente forhåndstillatelse fra Erhvervsstyrelsen dersom investeringen er innenfor spesielt sensitive sektorer og når terskelverdien på minimum 10 prosent eierandel. Den frivillige meldingsordningen gjelder for investeringer som når terskelverdien på minimum 25 prosent eierandel og som kan utgjøre en trussel mot nasjonal sikkerhet eller offentlig orden.

Det er den utenlandske investoren, altså en utenlandsk statsborger eller et selskap, som er pålagt å søke om tillatelse til å gjennomføre en investering eller inngå en særskilt økonomisk avtale. Det er utenlandske investorer som også kan benytte seg av den frivillige meldingsordningen. Det er forskjellig hvilke utenlandske statsborgere og selskaper som omfattes avhengig av om det er en utenlandsk investering eller en særskilt økonomisk avtale, og i forhold til hvilken sektor investeringen eller avtalen gjelder. For investeringer eller særskilte økonomiske avtaler som eksempelvis omfattes av den frivillige meldemuligheten, men som ikke er varslet, kan Erhvervsstyrelsen gå 5 år tilbake og undersøke og eventuelt iverksette tiltak mot investeringen.

Kontrollen eller innflytelsen som oppnås med investeringen kan være både direkte og indirekte, dvs. kontroll kan utøves gjennom andre selskaper og gjennom flere land og eierkjeder. Ved beregning av kvalifisert andel etter investeringsscreeningsloven medregnes eierandeler eller stemmerett som direkte eller indirekte tilhører den utenlandske investoren og eierandeler som den utenlandske investoren har innflytelse over gjennom nærstående.

Dersom eierandeler eller stemmerett i en investering er under terskelen på 10 prosent, har man som hovedregel ikke en kvalifiserende andel. Det kan imidlertid oppnås tilsvarende kontroll på andre måter som tilsvarer et erverv på 10 prosent eller mer. Det er derfor viktig at myndighetene undersøker om investoren oppnår en kvalifisert eierandel, eller om det oppnås tilsvarende kontroll på annen måte, da begge forhold kan ha betydning for om man har meldeplikt eller ikke. Kontrollen eller betydelig innflytelse oppnådd gjennom erverv av eierandeler eller stemmerett eller tilsvarende kontroll på andre måter kan være både direkte og indirekte. Indirekte kontroll eller påvirkning kan innebære at en investering foretatt for eksempel i et annet EU-land kan utløse krav om tillatelse etter investeringsscreeningsloven dersom selskapet det er investert i har et datterselskap i Danmark.

Kravet om tillatelse for utenlandske direkteinvesteringer gjelder kun dersom det danske selskapet man investerer i er innenfor sektorer og aktiviteter som er *spesielt sensitive med tanke på å kunne true nasjonal sikkerhet eller offentlig orden*. De spesielt sensitive sektorene og aktivitetene er generelt begrenset til følgende:

- Bedrifter innen forsvarssektoren
- Selskaper innen IT-sikkerhetsfunksjoner eller behandling av gradert informasjon
- Selskaper som produserer produkter med to bruksområder
- Bedrifter innen kritisk teknologi andre enn de som er nevnt i 1-3
- Bedrifter og offentlige myndigheter og institusjoner innen kritisk infrastruktur

I forhold til utvalgets mandat er det relevant å se på hvordan danske myndigheter definerer meldeplikten når det gjelder kritisk infrastruktur. I Danmark må du søke Erhvervsstyrelsen om tillatelse dersom selskapet *direkte eller indirekte eier eller råder over kritisk infrastruktur, har myndighetsansvar for kritisk infrastruktur eller utvikler eller produserer teknologi som utgjør kritisk infrastruktur*. Kritisk infrastruktur forstås som: «infrastruktur, inkludert fasiliteter, systemer, prosesser, nettverk, teknologier, eiendeler og tjenester, som er nødvendige for å opprettholde eller gjenopprette samfunnsviktige funksjoner». Hva som er konkret kritisk infrastruktur bestemmes av myndighetene ut fra en inndeling av samfunnet i samfunnsviktige sektorer, som videre omfatter en rekke underliggende samfunnsviktige funksjoner. De samfunnviktige sektorene inkluderer blant annet energisektoren, informasjons- og kommunikasjonsteknologi (IKT), transport, beredskap og sivilbeskyttelse, helsesektoren og finanssektoren. IKT-sektoren omfatter disse infrastrukturtypene:

- offentlig tilgjengelige elektroniske kommunikasjonsnett og -tjenester
- sentral datalagring (datalagringssentre)
- satellittradio og TV-overføring
- felles offentlige grunndata, herunder geodata, personregistrering og sentral virksomhetsregistrering. Domenenavnfunksjoner
- nyhetskringkasting
- sentral offentlig digital identifikasjon og kommunikasjon
- IT- og kommunikasjonsløsninger for å støtte kriseberedskap
- klassifisert kommunikasjon i staten
- lukkede kommunikasjonsnettverk og tjenester mellom myndigheter

Meldeplikten gjelder for utenlandske statsborgere, selskaper som ikke er hjemmehørende i Danmark (selv om det har fast driftssted i Danmark), selskaper hjemmehørende i Danmark som er et datterselskap eller en filial av et selskap utenfor Danmark, selskaper hjemmehørende i Danmark dersom en utenlandsk statsborger eller et selskap utenfor Danmark har kontroll eller betydelig innflytelse over det og nasjonale myndigheter og statlige organer i land utenfor EU og EFTA (herunder offentlige institusjoner og statseide investeringsfond, ideelle foreninger, ikke-kommersielle stiftelser og lignende juridiske personer utenfor EU og EFTA).

Den frivillige meldingsordningen gjelder for utenlandske statsborgere med unntak av statsborgere fra EU- og EFTA-land, selskaper hjemmehørende utenfor EU- eller EFTA-land, selskaper hjemmehørende i Danmark og andre EU- eller EFTA-land dersom selskapet kontrolleres av personer eller selskaper fra land utenfor EU eller EFTA og nasjonale myndigheter og statlige organer utenfor EU og EFTA (herunder offentlige institusjoner og statseide investeringsfond).

Danske myndigheter kan enten forby eller godkjenne investeringen. Dersom myndigheten vurderer at den mulige trusselen kan avbøtes med detaljerte vilkår for gjennomføring av investeringen eller avtalen, kan Erhvervsstyrelsen kontakte den utenlandske investoren for å forhandle det nærmere innholdet i slike vilkår. Eksempler på vilkår for tillatelse til utenlandske direkteinvesteringer eller særskilte økonomiske avtaler kan være:

- vilkår av økonomisk karakter, f.eks. begrensning av investors eierandel
- vilkår av ledelsesmessig karakter, f.eks. begrense investorens deltakelse i ledelsen av selskapet
- vilkår som tar sikte på å begrense investors mulighet til å få innsikt i selskapet på enkelte områder som f.eks. utvikling av kritisk teknologi
- vilkår om at den utenlandske investoren ikke kan bruke sin innflytelse til visse formål, som å stoppe forsyningen, flytte produksjon mv.
- vilkår vedrørende begrensninger i forhold til investors mulighet til å få tilgang eller innsikt i informasjon om visse deler av den danske enhetens/myndighets virksomhet eller fysiske lokaliteter
- vilkår om begrensninger i forhold til hvem den utenlandske investoren kan velge å utføre støttefunksjoner og lignende i avtaleperioden
- vilkår om restriksjoner i forhold til hvem den utenlandske investoren kan velge som underleverandør av f.eks. nærmere angitte produkter og software.[124]

10.4 Finland

I Finland er det «Act on the Screening of Foreign Corporate Acquisitions in Finland» fra 1. Juni 2012 som regulerer investeringskontrollen for utenlandske investeringer. Formålet med loven er å screene og begrense overføring av innflytelse til utenlandske statsborgere, organisasjoner og virksomheter – *hvis sentrale nasjonale interesser krever det.* En positiv holdning til utenlandske investeringer er lovens ledende prinsipp. Myndighetene kan imidlertid utøve kontroll over eierskapet til selskaper som anses *som vesentlige med tanke på forsyningssikkerhet og nasjonal sikkerhet* og om nødvendig begrense utenlandsk eierskap i slike selskaper. I praksis refererer sentrale nasjonale interesser hovedsakelig til *militært nasjonalt forsvar, funksjoner som er viktige for samfunnet* (inkludert sikring av kritisk infrastruktur og forsyningssikkerhet) og *nasjonal sikkerhet og offentlig orden*.

Investeringskontrollen for utenlandske investeringer behandles av Økonomi- og arbeidsdepartementet, som også ber om uttalelser fra andre myndigheter i den grad det er nødvendig. Overvåkingen av bedriftsoppkjøp støttes av et nettverk av myndigheter, ledet av departementet, som screener utenlandske oppkjøp og deltar i prosessene knyttet til disse. Departementet må godkjenne eierskiftet med mindre det kan sette en sentral nasjonal interesse i fare. Departementet må i så fall oversende saken til behandling i regjeringen. Økonomi- og arbeidsdepartementet er også det nasjonale kontaktpunktet for Europakommisjonen i henhold til EUs forordning (EU) 2019/452 om etablering av et rammeverk for screening av utenlandske direkteinvesteringer, på samme måte som ISP er i Sverige. Det nasjonale kontaktpunktets rolle er å styrke kommunikasjonen og samarbeidet mellom EUs medlemsland og Europakommisjonen.

[124] https://erhvervsstyrelsen.dk/vejledning-aktiviteter-omfattet-af-investeringsscreeningsloven

Screeningregelverket kommer til anvendelse i tilfeller hvor en utenlandsk eier får kontroll over minst en tidel, minst en tredel, eller minst halvparten av det samlede antall stemmer som er tillagt alle aksjer i selskapet, eller en eierandel som ellers tilsvarer beslutningsmyndighet i et aksjeselskap eller annen juridisk enhet som er gjenstand for screening. Dette gjelder også for disposisjoner som kan øke investors innflytelse i etterkant av en screening og som ikke overskrider terskelverdiene på nåværende tidspunkt. Meldeplikten ligger hos den utenlandske investoren.

I henhold til lovens del 4 krever erverv i *forsvars- og produktsektoren* (produkter med dobbelt bruksområde = forsvarsmateriellindustri) og i *sikkerhetssektoren* alltid forhåndstillatelse fra finske myndigheter. I *sivil sektor* overvåkes finske selskaper som anses som *kritiske for å sikre grunnleggende funksjoner i samfunnet*. Når det gjelder forsvarsmateriellindustrien omfatter screeningen alle utenlandske eiere. I andre sektorer gjelder screening kun for utenlandske eiere bosatt eller hjemmehørende utenfor EU eller EFTA.

Hva som regnes som kritiske funksjoner som er grunnleggende for samfunnet i Finland, vil variere avhengig av den rådende sikkerhetssituasjonen til enhver tid. Som regel er sikring av forsyningssikkerheten sentral uansett sikkerhetssituasjon. Loven spesifiserer ikke hvilke sektorer (privat eller offentlig) eller funksjoner i selskaper som er underlagt screeningen. Dette begrunnes med at det er vanskelig å forutsi hvilke sektorer og funksjoner som vil være kritiske for grunnleggende samfunnsfunksjoner. Selv om et selskap har virksomhet på et felt som er viktig for forsyningssikkerheten eller andre grunnleggende funksjoner, betyr det ikke nødvendigvis at det vil være gjenstand for screening etter loven. En rekke selskaper som ikke er kritiske for forsyningssikkerheten operer jo innen matforsyning og logistikk. Veiledning om lovens virkeområde finnes blant annet i Regjeringens offentlige veiledningsdokumenter om forsyningssikkerhet og nasjonal sikkerhet. En definisjon som her er relevant for ekomsektoren er definisjonen av kritisk infrastruktur. Her defineres kritisk infrastruktur som de *grunnleggende strukturer, tjenester og relaterte funksjoner som er avgjørende for å opprettholde de vitale funksjonene i samfunnet.* Kritisk infrastruktur inkluderer både fysiske virksomheter og strukturer samt elektroniske funksjoner og tjenester. Dette inkluderer *datakommunikasjonssystemer og nettverk og tjenester i det digitale samfunnet.*

Med forsvarsvirksomhet menes en virksomhet som produserer eller leverer forsvarsmateriell eller andre produkter eller tjenester som er avgjørende for det nasjonale forsvaret. I praksis vurderes betydningen av produktene eller tjenestene fra sak til sak ut fra eksisterende kontrakter med Forsvaret. For eksempel kan levering av essensielle programvareapplikasjoner, cyberapplikasjoner, skytjenester eller andre lignende produkter eller tjenester anses som et viktig produkt eller en viktig tjeneste. Et selskap som produserer varer med dobbelt bruksområde anses også som et forsvarsselskap. Eksempelvis vil et aksjeselskap som opererer i sivil sektor, men som importerer autorisasjonskrevende varer med dobbelt bruksområde til tredjeland, overfører sensitive varer innenfor EU eller som på annen måte har fått tillatelse eller melding eller vedtak fra myndighet for eksport av slike varer, regnes som et forsvarsselskap. Tilsvarende regnes et selskap i sivil sektor som bruker, utvikler eller på annen måte håndterer teknologi med to bruksområder, som et forsvarsselskap. Et sikkerhetsselskap er et selskap som leverer eller produserer produkter eller tjenester som er kritiske for sikkerheten i samfunnet til Finlands sentrale myndigheter i forhold til deres lovpålagte plikter. Disse sikkerhetsmyndighetene inkluderer det finske forsvaret, den finske grensevakten, det finske politiet, det finske tollvesenet, det nasjonale

nødforsyningsverket, den nasjonale sikkerhetsmyndigheten (NSA) og det finske transport- og kommunikasjonsbyrået (Traficom). Produkter eller tjenester hvis levering til sentrale finske sikkerhetsmyndigheter kan anses som kritiske inkluderer programvare (f.eks. krypteringsprogramvare), cybersikkerhetsapplikasjoner, sertifiseringstjenester, skytjenester, datasentertjenester og andre produkter og tjenester knyttet til vedlikehold av disse.

Dersom en utenlandsk investering gjelder et forsvars- eller sikkerhetsselskap, er det meldeplikt, og varselet skal alltid leveres til Økonomi- og arbeidsdepartementet på forhånd. Loven angir ingen frister for når Økonomi- og arbeidsdepartementet kan gripe inn i et oppkjøp av et forsvars- eller sikkerhetsselskap dersom det ikke er meldt inn til departementet. Loven angir heller ingen frister for hvor lang saksbehandlingen skal være etter en melding er sendt til departementet, men prosessen tar i gjennomsnitt to måneder. Gjelder ervervet et annet selskap enn et forsvars- eller sikkerhetsselskap, er meldingen frivillig, og den kan også sendes på forhånd. En forhåndsmelding kan imidlertid bare sendes inn i fasen rett før den endelige inngåelsen av forretningsavtalen (f.eks. en intensjonsavtale, som er bindende for partene, og som allerede er signert for det planlagte oppkjøpet). Økonomi- og arbeidsdepartementet screener sammen med sitt nettverk av andre relevante myndigheter gjennomførte bedriftsoppkjøp i screeningspliktige selskaper. På bakgrunn av screeningen kan departementet også selvstendig be om opplysninger om bedriftsoppkjøp som kan være gjenstand for screening etter loven.

Departementet kan enten forby eller godkjenne ervervet, eller eventuelt godkjenne på vilkår. Vilkårene stilles kun i visse situasjoner og må anses som nødvendige avbøtende tiltak som tar sikte på å redusere risikoen ved den utenlandske investeringen og sikre en sentral nasjonal interesse. Vilkår kan bare stilles dersom partene forplikter seg til å overholde dem. Vilkårene defineres i forhandlinger mellom oppkjøpspartene og kompetente myndigheter. Innholdet i vilkårene varierer avhengig av sak. For eksempel kan myndighetene kreve utelukkelse av en bestemt forretningsfunksjon eller andel fra oppkjøpet eller en forpliktelse til å sikre videreføring av tjenester under eksisterende produksjons- og leveringsavtaler. Et forbud kan kun gis i plenum i regjeringen.[125]

[125] https://tem.fi/en/acquisitions

10.5 Screeningregelverk i EU (eksisterende og nytt forslag)

10.5.1 Forordning (EU) 2019/452 om kontroll av utenlandske direkteinvesteringer (EUs gjeldende screeningregelverk)

Europaparlaments- og rådsforordning (EU) 2019/ 452 om kontroll av utenlandske direkteinvesteringer i unionen trådte i kraft i oktober 2020. Forordningen er omtalt i NOU 2023: 28 på side 58-59, og den følgende teksten som beskriver det gjeldende regelverket er hentet fra denne:

«**Bakgrunn og formål**
Forordningen er hjemlet i EU-traktaten avdeling II om felles handelspolitikk, og er ikke en del av EØS-avtalen. Forordningen gjelder for alle EUs medlemsland, uavhengig av om de har en investeringskontrollordning eller ikke. Formålet med forordningen er å etablere en felles tilnærming til kontrollen av investeringer fra land utenfor EU (tredjeland), som kan utgjøre en risiko for sikkerhet eller offentlig orden. Tolkningen av begrepene sikkerhet eller offentlig orden gjøres av den enkelte medlemsland, men må være i samsvar med EUs internasjonale forpliktelser og bestemmelsene i EU-traktaten om kapitalbevegelser fra tredjeland. Forordningen legger til rette for informasjonsutveksling og koordinering mellom medlemslandene i EU, og mellom medlemslandene og Europakommisjonen. Forordningen åpner for og understreker viktigheten av internasjonalt samarbeid om investeringskontroll med tredjeland. I forordningen fastsettes det at Europa er og skal fortsette å være åpent for utenlandske direkteinvesteringer ((EU) 2019/452).

Minstekrav til utformingen av nasjonale regelverk
EU-forordningen etablerer ikke en felles investeringskontroll for medlemslandene og den pålegger heller ikke medlemsland å opprette egne nasjonale kontrollordninger. Medlemslandene bestemmer selv hvordan deres nasjonale regelverk skal utformes. Beslutningen om hvilke investeringer som skal kontrolleres og eventuelt gripes inn i skal tas av medlemslandet der investeringen finner sted. Forordningen stiller likevel enkelte minstekrav til utformingen av nasjonale regelverk. Ifølge forordningens artikkel 3 skal ordningene være transparente og ikke-diskriminerende, og ha fastsatte frister for behandling av saker. Videre skal sensitiv informasjon behandles konfidensielt, det skal være klagemuligheter for investorer, og det skal finnes tiltak for å identifisere og avverge omgåelse av reglene. I artikkel 3 legges det vekt på at medlemslandenes regler skal være åpne og tilgjengelige og at reglene skal angi omstendighetene som utløser kontroll, begrunnelsen for kontroll, samt tilhørende detaljerte prosedyrer knyttet til prosessen.

Samarbeidet mellom Europakommisjonen og medlemsland
Forordningen pålegger EU-landene en plikt til å samarbeide innbyrdes og med Europakommisjonen. Samarbeidet varierer avhengig av om de utenlandske investeringene blir kontrollert på nasjonalt plan eller ikke.

Dersom en investering kontrolleres på nasjonalt plan, skal medlemslandet orientere Europakommisjonen og de andre medlemslandene om dette ved å dele opplysninger om investeringen. Hvis et annet medlemsland anser at investeringen sannsynligvis vil påvirke dets sikkerhet eller offentlige orden, kan

dette landet utstede en kommentar. Dersom Europakommisjonen anser at en investering sannsynligvis vil påvirke sikkerheten eller den offentlige orden i mer enn ett medlemsland, kan Kommisjonen gi en uttalelse. Kommentarer fra medlemslandene og Kommisjonens uttalelse rettes til medlemslandet der investeringen finner sted.

Medlemslandene og Kommisjonen kan også uttale seg om investeringer som ikke er underlagt investeringskontroll. Dette kan være tilfellet dersom medlemslandet hvor investeringen finner sted ikke har en kontrollordning, eller investeringer ikke omfattes av medlemslandets nasjonale ordning. Hvis et medlemsland eller Kommisjonen anser en ikke-kontrollert investering i et annet medlemsland for å være en risiko for flere medlemsland eller for hele unionen, kan man etterspørre informasjon fra vertslandet for investeringen. Vertslandet er da forpliktet til å bidra med et minimum av informasjon så raskt som mulig.

All utveksling av informasjon gjennom EUs samarbeidsordning er underlagt strenge regler om konfidensialitet. Kommentarer og uttalelser deles ikke med de andre medlemslandene, unntatt når uttalelsen gjelder en investering som kan påvirke fellesprosjekter eller programmer på EU-nivå. Europakommisjonen er forpliktet til å skaffe til veie et sikret og kryptert kommunikasjonssystem mellom medlemsland og Kommisjonen for dette formålet.

Generaldirektoratet for handel i Kommisjonen har laget et skjema for å forbedre informasjonsutvekslingen under EU-mekanismen. Informasjon som deles i EUs samarbeidsordning inkluderer informasjon om hvem som er investoren og målforetaket, hvilke sektorer disse opererer i og hvor, hva som er verdien av investeringen, hvor finansieringen kommer fra og når transaksjonen skal finne sted.

Effektiv informasjonsdeling skal bidra til at medlemslandet som melder om en investering, kan gjøre sine vurderinger uten forsinkelse. Medlemslandet hvor investeringen finner sted, oppfordres til å innhente nødvendige opplysninger fra investoren eller det berørte foretaket.

Veiledning til vurdering av saker

Forordningen gir en veiledende liste over kriterier som skal hjelpe medlemslandene og Europakommisjonen med å vurdere om en utenlandsk direkteinvestering vil kunne påvirke sikkerhet eller offentlig orden. Ifølge listen bør landene og Europakommisjonen vurdere virkningene av den utenlandske investeringen på:

- kritisk infrastruktur (fysisk eller virtuell, innen energi, transport, vann, helse, kommunikasjon, media, databehandling og -lagring, luft og romfart, forsvar, valgrelatert eller finansiell infrastruktur, samt investeringer i land og eiendom som er avgjørende for bruk av slike infrastrukturer)
- kritisk teknologi og elementer med flerbrukspotensiale (kunstig intelligens, robotikk, halvledere, cybersikkerhet, kvanteteknologi, romfart, forsvar, energilagring, kjernefysisk teknologi og nano- og bioteknologi)
- tilgang til kritiske leveranser (energi, råvarer og matsikkerhet)
- tilgang til eller muligheten til å kontrollere sensitiv informasjon (personopplysninger)
- mediefrihet og pluralisme

Forordningen viser til at forhold knyttet til investor også er relevante for vurderingen. Dette er forhold som knytter seg til om investoren er kontrollert eller påvirket av tredjeland, enten gjennom eierstrukturer eller gjennom betydelig finansiering, om investor tidligere har vært involvert i aktivitet som påvirket sikkerhet eller samfunnsorden eller om investor har vært involvert i internasjonal kriminalitet.

Ikke-diskriminering av investorer fra tredjeland (utenfor EU) er et sentralt prinsipp i forordningen. Risiko tilknyttet et utenlandsk oppkjøp skal vurderes i hver enkelt sak, uavhengig av den utenlandske kjøpers hjemland. EU-forordningen tillater ikke kontroll av utenlandske direkteinvesteringer basert på andre hensyn enn sikkerhet eller offentlig orden. Forordningen lister for øvrig opp flere EU-finansierte prosjekter og programmer som kan være relevante for sikkerhet eller offentlig orden, og hvor Kommisjonen særlig vil vurdere risikoen ved utenlandske investeringer. Denne listen inkluderer blant annet «Galileo», «Horizon 2020», «Trans-European Networks» og «European Defence Industrial Development Programme». Listen ble oppdatert i 2020 og ytterligere oppdateringer vil følge etter behov.

Ekspertgruppe for kontroll av utenlandske direkteinvesteringer i EU
Som ledd i arbeidet med å gjøre EU-forordningen operasjonell, er det opprettet en ekspertgruppe som skal gi råd til Kommisjonen. Alle medlemslandenes myndigheter deltar i gruppen, også de som i dag ikke har en nasjonal kontrollordning. Gruppen ledes av Europakommisjonen. Gruppens mandat er å drøfte spørsmål av felles interesse knyttet til utenlandske direkteinvesteringer, samt beste praksis og erfaringer fra investeringskontroll på nasjonalt nivå. Ekspertgruppen har også myndighet til å gi Kommisjonen råd om spørsmål knyttet til gjennomføringen av selve forordningen. Ekspertgruppen omtaler ikke individuelle investeringer.[126] »

10.5.2 Forslag til ny screeningordning i EU

Siden EUs screeningreleverk kom på plass i 2020, har den geopolitiske situasjonen forandret seg betraktelig og blitt mer tilspisset. Pandemien, Russlands invasjon av Ukraina og andre geopolitiske spenninger har forsterket behovet for å kunne identifisere risikoer knyttet til sikkerhetstruende økonomisk aktivitet og bedre beskytte eiendeler og virksomheter som er kritiske for Europa. Dette har også bidratt til en betydelig økning i antall medlemsland som har fått på plass en nasjonal screeningsmekanisme, og et større antall sektorer som er gjenstand for screening. Det er imidlertid en andel av direkte utenlandske investeringer (Foreign Direct Investments (FDI)) i EU som fortsatt går til medlemsland som ikke har en screeningmekanisme, noe som kan utgjøre en risiko for at potensielt sikkerhetstruende økonomisk aktivitet ikke blir oppdaget.

Europakommisjonen la i slutten av januar 2024 frem flere initiativer for å styrke EUs økonomiske sikkerhet i en tid med økende geopolitiske spenninger og betydelige teknologiske endringer. Blant initiativene var også et eget lovforslag om å styrke kontrollen med utenlandske investeringer i EU. I forbindelse med offentliggjøringen av lovforslaget viste Kommisjonen til at den har evaluert den gjeldende

[126] NOU 2023: 28 *Investeringskontroll – en åpen økonomi i usikre tider*

screeningforordningen og gjennomgått over 1200 transaksjoner med direkte utenlandske investeringer som har blitt meldt inn av medlemslandene de siste tre årene under det eksisterende regelverket (omtalt overfor). Basert på erfaringene fra gjennomgangen og evaluering av hvordan den nåværende kontrollen fungerer, ble det fremhevet at det er mangel på harmonisering som er det største problemet i EUs gjeldende screeningregelverk. Først og fremst er det ingen forpliktelse for medlemslandene til å ha en tilstrekkelig screeningmekanisme. Det finnes heller ingen klare retningslinjer for omfanget av medlemslandenes screeningsmekanismer. Hvis omfanget er for snevert definert, kan enkelte kritiske investeringer ikke bli fanget opp. Videre definerer medlemslandene nøkkelbegreper ulikt, noe som resulterer i forvirring og usikkerhet, og det er ingen felles minimumskriterier for å avgjøre hvilke investeringer som skal vurderes. Når det gjelder fristene for å svare, er de de samme for Kommisjonen og medlemslandene, noe som muligens gir Kommisjonen for kort tid til å vurdere eventuelle kommentarer fra medlemslandene. Prosessen med å sende inn kommentarer og tidslinjen i en screeningsak begynner først når den formelle screeningprosedyren har startet, og dette er i hendene på det berørte medlemslandet.

Kommisjonens forslag tar sikte på å adressere disse manglene, samt forbedre effektiviteten i screeningmekanismen på viktige områder, ved å sikre at *alle medlemsland har en mekanisme for screening* med bedre harmoniserte nasjonale regler. Det betyr at land som allerede har et screeningregelverk må harmonisere dette med den nye forordningen. Videre vil man i forslaget identifisere *et minimum av sektorer* som alle medlemsland må kontrollere utenlandske investeringer i, samt utvide EUs screening til å også omfatte investeringer fra europeiske investorer som i siste instans kontrolleres av enkeltpersoner eller virksomheter fra land utenfor EU. Kommisjonen ønsker også å inkludere investeringer ved etablering av nytt foretak, såkalt greenfield-investeringer, i screeningen. Når det gjelder åpenhet og transparens i de nasjonale screeningmekanismene, vil Kommisjonen blant annet kreve at medlemslandene publiserer en årlig rapport med aggregerte og anonymiserte data om screenede investeringer. I forslaget ønsker man også å la investorer få visse rettigheter i prosess. Eksempelvis før det tas en beslutning om forbud eller betinget godkjenning, vil screeningmyndighetene måtte informere utenlandske investorer om årsakene til å ta en slik avgjørelse, og gi dem en mulighet til å gi uttrykk for sine synspunkter.[127]

Samarbeidsmekanismen på EU-nivå

Forslaget til forordningens artikkel 5 gir bestemmelser om hvilke utenlandske investeringer som skal meldes fra om til Europakommisjonens samarbeidsmekanisme, og artikkel 6 angir prosedyrene for hvordan samarbeidsmekanismen skal fungere. Et eksempel på en utenlandsk investering som medfører en meldeplikt til EUs samarbeidsmekanisme er investeringer der den utenlandske investoren eller den utenlandske investorens datterselskap i unionen er direkte eller indirekte kontrollert myndighetene i et tredjeland. Meldeplikten inkluderer også investeringer der den utenlandske investoren eller noen av dens datterselskaper var involvert i en utenlandsk investering som tidligere er screenet av et medlemsland og ikke var godkjent eller kun godkjent på vilkår.

[127] https://www.crowell.com/en/insights/client-alerts/a-new-european-commission-proposal-on-foreign-direct-investment-screening-towards-greater-harmonization

Videre angir artikkel 6 prosedyrer for hvordan medlemslandene skal koordinere seg hvis flere land har mottatt samme melding om investering og det er snakk om en grensekryssende transaksjon. I forslaget ønsker Kommisjonen å strømlinjeforme samarbeidsmekanismen på EU-nivå ved å kreve at investorer som må varsle om sine investeringer i flere medlemsland, skal sende inn søknadene sine til dem alle samtidig (med henvisning til de andre meldingene), for så å kreve at nasjonale myndigheter koordinerer med hverandre og sender meldinger til Kommisjonen samtidig. Videre vil man stramme opp prosedyrene og fristene for samarbeidsmekanismen, samtidig som Kommisjonen får mer tid til å ta hensyn til kommentarer fra medlemslandene. Medlemslandene vil ha 15 kalenderdager, og Europakommisjonen 20 kalenderdager, til å informere medlemsland(ene) om at de har til hensikt å sende inn kommentarer eller avgi en mening om en investering. Medlemslandene vil da ha 35 dager på seg fra mottak av en fullstendig melding til å sende inn sine kommentarer, og Kommisjonen vil ha 45 dager på seg til å avgi sin uttalelse. Fristen for medlemslandenes meldeplikt til Kommisjonen er 60 dager hvis medlemslandet allerede har bestemt seg for på å foreta en grundig screening med dybdeundersøkelser.

Sikkerheten ved informasjonsutvekslingen mellom medlemslandene foreslås styrket. Etter artikkel 6 skal informasjonsutvekslingen mellom medlemslandene og Kommisjonen foregå gjennom et kryptert system. Hvert medlemsland må utpeke et kontaktpunkt og Kommisjonen vil sette opp et system for å muliggjøre kryptert kommunikasjon mellom kontaktpunktene. Forslaget inneholder også bestemmelser om beskyttelse av taushetsbelagte og graderte opplysninger. Det er viktig å merke seg at Kommisjonen ønsker å begrense bruk av EUs samarbeidsmekanisme til kun de mest kritiske tilfellene.[128]

Videre vil Kommisjonen innføre en «own-initiative procedure», som lar et medlemsland eller Kommisjonen iverksette en gjennomgang av en utenlandsk investering i et annet medlemsland dersom investeringen ikke er varslet under samarbeidsmekanismen. Et medlemsland vil være berettiget til å gjøre dette hvis den mener at investeringen vil ha en negativ innvirkning på dens sikkerhet eller offentlige orden; Kommisjonen vil være i stand til å gjøre dette hvis den anser at investeringen sannsynligvis vil påvirke sikkerheten eller den offentlige orden i mer enn ett medlemsland negativt.[129]

Hvilke investeringer er omfattet?

Forslaget til ny forordning omfatter eksplisitt investeringer mellom selskaper innenfor EU, hvor selskapene faktisk kontrolleres fra tredjeland. I dag er slike selskaper inkludert kun dersom de utelukkende og entydig er skapt med formål om å omgå screening. Forslaget omfatter investeringer som enten er direkte utenlandske investeringer eller investeringer innenfor EU med utenlandsk deltakelse. Direkte investeringer vil dekke et bredt spekter av investeringer som etablerer eller opprettholder varige og direkte forbindelser mellom investorer fra land utenfor EU og foretak som driver økonomisk virksomhet i en medlemsstat.

Med investeringer forstås i denne sammenheng erverv av aksjer som gir den utenlandske investoren rett til å kontrollere eller påvirke driften av foretaket i EU, eller etablering av virksomhet i EU (greenfield-investeringer). Utvalget oppfatter også at forslaget til ny EU-regulering vil omfatte investeringer i selskap utenfor EU, men som i realiteten rettes mot/har virkning for et datterselskap i EU. Forslaget vil også dekke investeringer

[128] Proposal for a new regulation on the screening of foreign investments (10).pdf

[129] https://www.crowell.com/en/insights/client-alerts/a-new-european-commission-proposal-on-foreign-direct-investment-screening-towards-greater-harmonization

foretatt i EU av den utenlandske investorens datterselskap i EU så lenge formålet med investeringen er å etablere eller opprettholde slike forbindelser som nevnt over.

Det fremgår av fortalen (16) i forslaget til ny regulering at porteføljeinvesteringer ikke omfattes av forslaget:

> «However, the framework should not cover the acquisition of company securities intended purely for financial investment without any intention to influence the management and control of the undertaking (portfolio investments)»

Forslaget inneholder videre en obligatorisk liste over sensitive sektorer. Disse sektorene skal som et minimum inkluderes i medlemslandenes nasjonale screeningordninger. Dette er selskaper som er aktive innen områder og teknologier som *inkluderer produkter med dobbelt bruksområde*, *militær teknologi og utstyr*, *finansiell infrastruktur* og *kritiske legemidler* (som er definert i EUs liste over kritiske legemidler fra desember 2023.

Mer spesifiserte undergrupper av teknologier, som Kommisjonen har i sin innstilling fra oktober 2023 oppnevnt som spesielt kritiske er følgende:

- Halvlederteknologier
- Teknologier knyttet til kunstig intelligens
- Kvanteteknologier
- Bioteknologi
- Avansert tilkobling, navigasjon og digital teknologi
- Avanserte sensorteknologier
- Rom- og fremdriftsteknologier
- Energiteknologier
- Robotikk og autonome systemer
- Teknologier knyttet til avanserte materialer, produksjon og resirkulering

Forordningen legger videre opp til at screeningen vil omfatte utenlandske investeringer i virksomheter som deltar i et prosjekt eller mottar midler fra et av EUs finansieringsprogrammer. Dette er eksempelvis programmer som Horizon 2020, Digital Europe Programme og EUs romprogram (uttømmende liste i forslagets vedlegg 1) eller European Investment Fund. Screeningen vil også omfatte utenlandske investeringer i virksomheter som er økonomisk aktive innenfor områder som er av særlig sikkerhetsmessig viktighet. Det kan eksempelvis være områder som har tilknytning til kritisk teknologi. Ellers er det er opp til hvert enkelt medlemsland å definere hva som er kritisk infrastruktur.[130]

Kriterier som skal vurderes i screening

Det foreslåtte regelverket beskriver hvilke faktorer eller kriterier som skal vurderes for å avgjøre om en utenlandsk investering negativt kan påvirke sikkerhet eller offentlig orden – se artikkel 13 «Determination of likely negative impact on security and public order» i forslaget til nytt regelverk.

Faktorer som skal vurderes inkluderer blant annet påvirkningen på sikkerheten, integriteten og funksjonen til kritisk infrastruktur, tilgjengeligheten av kritiske teknologier

[130] https://www.eu.dk/samling/20231/kommissionsforslag/KOM(2024)0023/bilag/2/2871851.pdf

(inkludert sentrale muliggjørende teknologier), fortsatt tilgang til kritiske innsatsfaktorer, beskyttelsen av sensitiv informasjon (inkludert personopplysninger) mv.

I vurderingen av eventuelle negative virkninger skal man også *vurdere forhold knyttet til den utenlandske investoren selv* (eller noen som kontrollerer denne), herunder for eksempel om vedkommende tidligere har vært involvert i investeringer som etter screening enten er blitt avslått eller godtatt på vilkår, om vedkommende tidligere har deltatt i aktiviteter som negativt har påvirket sikkerheten eller offentlig orden i en medlemsstat, eller for eksempel også har deltatt i kriminell virksomhet. Men det kanskje viktigste vurderingskriteriet, sett i lys av utvalgets mandat, fremgår av forslaget til ny artikkel 13 bokstav (e):

> (e) whether the foreign investor, a natural person or entity controlling the foreign investor, the beneficial owner of the foreign investor, any of the subsidiaries of the foreign investor, or any other party owned or controlled by, or acting on behalf or at the direction of the foreign investor is likely to pursue a third country's policy objectives, or facilitate the development of a third country's military capabilities. (utvalgets understrekning)

Viktig er det også at det fremgår av artikkel 14 at vurdering av den eventuelle negative virkningen vil gjelde direkte for den aktuelle medlemsstaten der investeringen er tenkt gjennomført, men også vil kunne omfatte negative virkninger i andre medlemsland. Dette vil for eksempel kunne gjelde dersom investering i et selskap i et EU-medlemsland negativt påvirker leveransesikkerheten/verdikjeden til selskap i en annen EU-stat og dermed påvirker sikkerheten der.

Forslaget til ny artikkel 14 inneholder også en egen bestemmelse i nr. 2 som sier at hvis investeringens negative påvirkning på sikkerhet eller offentlig orden kan løses med tilgjengelige tiltak i annen EU- eller nasjonal lovgivning så må myndigheten godkjenne investeringen uten vilkår.[131]

Forslaget innebærer krav til minimumsregulering

Forslagene til nytt screeningregelverk oppstiller minimumskrav. Dette innebærer at den enkelte medlemsstat fortsatt vil kunne utvide omfanget av sin nasjonale kontroll ved å inkludere andre typer utenlandske investeringer eller for eksempel også utenlandske investeringer i andre sektorer enn de som er dekket av forslaget til regulering.[132]

[131] Proposal for a new regulation on the screening of foreign investments (10).pdf

[132] Se for eksempel forslag til artikkel 1 nr. 3: Member States may adopt or maintain in force national provisions in fields not coordinated by this Regulation.

Foto: Adobestock

IV

Om målbilde for nasjonal kontroll og aktuelle tiltak

”

Det er nødvendig med en strukturert tilnærming til nasjonal kontroll gjennom en modell som etablerer et målbilde med konkrete styringsevner og handlefriheter, deretter å analysere aktuelle virkemidler for å nå målbildet og fastsette strategier og handlingsplaner.

Foto: Andreas Veggeland (Lyse)

11

En strukturert tilnærming til nasjonal kontroll

11.1 Proaktive og reaktive nivåer

Myndighetene har de siste årene måtte håndtere flere konkrete saker med betydning for nasjonal kontroll med digital infrastruktur, som nevnt i punkt 4.4.3. Tilnærmingen har vært å håndtere disse sakene enkeltvis og fra sak til sak. Det foreligger ikke i dag et overordnet og langsiktig *målbilde* for hva som er et tilstrekkelig nivå for nasjonal kontroll med kritisk digital infrastruktur.

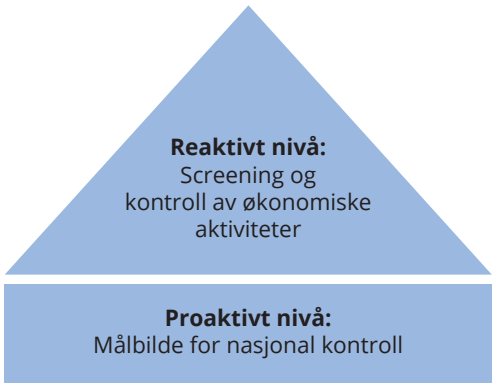
Sikkerhetsloven har verktøy for å ivareta nasjonal kontroll, for eksempel gjennom eierskapskontroll for selskapene underlagt loven. Slik utvalget vurderer det, er denne eierskapskontrollen imidlertid ikke tilstrekkelig for å identifisere og proaktivt håndtere en potensielt langsiktig svekkelse av nasjonal kontroll som kan følge av gradvise endringer i markedssituasjonen, i teknologiutviklingen, og i de digitale infrastrukturenes internasjonale verdikjeder. Meld. St. 9 (2022–2023) er i så måte et viktig steg i å sette i gang en mer helhetlig og langsiktig prosess rundt spørsmål om nasjonal kontroll.

Etter utvalgets syn er det behov for å etablere et målbilde for nasjonal kontroll. Med et definert målbilde kan myndighetene vurdere om det er tilstrekkelig å opprettholde dagens nivå av nasjonal kontroll over digital infrastruktur, om dagens nivå kan reduseres uten at det har betydning for nasjonale sikkerhetsinteresser, eller om det er behov for å styrke den nasjonale kontrollen gjennom *proaktive* strategier og handlingsplaner.

Parallelt med dette må staten ha evne til å *reaktivt* håndtere oppdukkende saker, herunder screening av utenlandske investeringer. Med et etablert målbilde vil myndighetene enklere kunne vurdere hvordan disse sakene konkret påvirker den

nasjonale kontrollen. Figur 11.1 illustrerer de proaktive og reaktive nivåene og beskrives nærmere under.

Figur 11.1 Illustrasjon av proaktivt og reaktivt nivå.



11.1.1 Det proaktive nivået – langsiktig målbilde, strategi og handlingsplaner

Det proaktive nivået innebærer at myndighetene etablerer et langsiktig mål på hvilke styringsevner og handlefriheter (jf. punkt 4.1.4) staten skal ha på ulike deler av den digitale infrastrukturen. Dette målbildet bør fastsettes etter føre-var-prinsippet, og være dimensjonert for scenarioer øverst i krisespekteret – krig og konflikt. Den proaktive tilnærmingen er viktig for å sikre at nødvendig styringsevne og handlefrihet over kritisk digital kommunikasjonsinfrastruktur allerede er etablert når det oppstår alvorlige situasjoner som utfordrer våre nasjonale sikkerhetsinteresser.

Målbildet må veies opp mot andre viktige samfunnshensyn. Dette presiseres også i Meld. St. 9 (2022–2023): «*Nasjonal kontroll som virkemiddel må brukes på en slik måte at det bidrar til forutsigbarhet og tillit, og at det ikke fører til unødvendige begrensninger for verdiskapning og utenlandske investeringer i Norge, eller for norsk markedsadgang i utenlandske markeder.*»

Når målbildet er definert, må gapet mellom dagens situasjon og målbildet identifiseres. En viktig forutsetning for dette er at myndighetene er i stand til å etablere en god oversikt over infrastrukturen, og løpende opprettholde oversikten gjennom teknologiske, markedsmessige og selskapsmessige endringer.

Myndighetene må etablere strategier og handlingsplaner for hvordan målbildet for nasjonal kontroll kan nås – og ivaretas – over tid. Dette kan gjøres gjennom å anvende en kombinasjon av hensiktsmessige virkemidler, nærmere omtalt i kapittel 9, overfor ulike deler av den digitale infrastrukturen. Virkemiddelapparatet spenner vidt, fra strategisk statlig eierskap til regulatoriske krav, tjenesteavtaler, tilskuddsordninger og internasjonalt beredskapssamarbeid.

Det er viktig å poengtere at målbildet *ikke* defineres i form av «utpeking» av enkeltselskaper som for eksempel må opprettholde nasjonalt eierskap. I sektoren for elektronisk kommunikasjon er markedet og risikobildet svært dynamisk, og

selskapsstrukturene endrer seg fortløpende gjennom oppkjøp, salg av eiendeler, sammenslåinger, partnerskap og teknologiendringer. Målbildet må i stedet defineres i form av hvilke styringsevner og handlefrihet staten har behov for innenfor de ulike kategorier av digital infrastruktur, som omtalt i figur 5.1.

11.1.2 Det reaktive nivået – screening og kontroll med økonomiske aktiviteter

Det reaktive nivået innebærer at staten kan kontrollere og potensielt gripe inn i økonomiske aktiviteter som kan skade nasjonale sikkerhetsinteresser, enten gjennom tap av nasjonal kontroll eller gjennom andre sikkerhetstruende forhold.

Det primære reaktive virkemidlet vil være screening av utenlandske investeringer for å vurdere om den økonomiske aktiviteten kan ha sikkerhetstruende effekt. I dag er det sikkerhetsloven som gir det rettslige grunnlaget for screening og eventuell inngripen. Videre fremgår det av Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen* punkt 8.2 at regjeringen er i gang med å videreutvikle dagens ordning for investeringskontroll til å gjelde også investeringer i virksomheter som ikke er underlagt sikkerhetsloven, blant annet gjennom en ny lov for kontroll av utenlandske investeringer.

I tillegg til screening av utenlandske investeringer, er det etter utvalgets syn også behov for at myndighetene har bedre oversikt og kontroll over andre økonomiske aktiviteter som påvirker nasjonal kontroll. Dette kan typisk være infrastrukturselskaper som velger nye partnerskap, driftskonsepter og teknologiløsninger som innebærer økt utenlandsk innflytelse og avhengighet. Dette trenger isolert sett ikke å ha en sikkerhetstruende effekt, men kan gradvis over tid bidra til å svekke statens styringsevner og handlefriheter over kritisk digital kommunikasjonsinfrastruktur. Eksempler på slik kontrollreduserende økonomisk aktivitet er nærmere beskrevet i punkt 4.3.

Ved hjelp av et etablert målbilde som omtalt over, vil myndighetene kunne vurdere hvilken konkret effekt slike økonomiske aktiviteter har på nasjonal kontroll. Om de økonomiske aktivitetene kan tillates eller ikke, avhenger blant annet av kravene i sikkerhetsloven, og kravene til forsvarlig sikkerhet og beredskap i ekomloven med forskrifter. I mange tilfeller vil aktivitetene i seg selv være lovlige, men samtidig bidra til å bringe staten lenger vekk fra målbildet om nasjonal kontroll. Denne erkjennelsen må da reflekteres tilbake inn i de proaktive strategiene og handlingsplanene som omtalt over, slik at kompenserende tiltak kan gjennomføres.

Kapittel 12 går nærmere inn på beskrivelsen av det reaktive nivået, og vurderingskriterier knyttet til screening av og kontroll med økonomisk aktivitet.

11.2 Definisjoner av styringsevner og handlefrihet som ivaretar nasjonale sikkerhetsinteresser

Utvalget har, jf. punkt 4.1.4, definert nasjonal kontroll som et produkt av statens selvstendige *styringsevne* til å ta effektive beslutninger, og statens *handlefrihet* til å gjennomføre beslutninger mest mulig uavhengig av utenlandske aktører.

I dette kapittelet drøfter utvalget nærmere hva slags styringsevne og hva slags handlefrihet staten bør ha for å ivareta nasjonale sikkerhetsinteresser knyttet til digital infrastruktur. Dette sees da i lys av utfordringsbildet beskrevet i punkt 4.2. Styringsevnene og handlefriheten utfyller hverandre, og påvirker hverandre, og utvalget presiserer at det også kan finnes andre sider av styringsevne og handlefrihet som ikke omtales her.

11.2.1 Statens styringsevner

Evne til å ta eller påvirke beslutninger om eierskapstransaksjoner
Denne styringsevnen handler om statens evne til å ta eller påvirke beslutninger om utenlandske eierskapstransaksjoner knyttet til selskaper som eier og forvalter kritisk digital kommunikasjonsinfrastruktur i Norge. Dette innebærer å kunne stoppe eller sette vilkår for transaksjoner som kan ha sikkerhetstruende effekt. Dette kan typisk være knyttet til at utenlandske aktører får tilgang til og kontroll med kunnskap, informasjon, infrastruktur eller eiendom, som kan utnyttes til for eksempel spionasje, påvirkningsoperasjoner, nedbygging av kapasitet, leveransenekt eller sabotasje.

Evne til å ta eller påvirke beslutninger om plassering av hovedkontorfunksjoner
Denne styringsevnen innebærer å kunne opprettholde nødvendig eierskapskontroll i statlig eide selskaper for å kunne ivareta de nasjonale sikkerhetsinteressene. Staten har ulike begrunnelser for statlig eierskap. I noen tilfeller er det å ivareta samfunnssikkerhet og beredskap det primære formålet. I andre tilfeller kan det være å ivareta hovedkontorfunksjoner i Norge. Utvalget mener at det å ivareta hovedkontorfunksjoner i Norge for strategisk viktige selskaper også har en betydning for nasjonal kontroll og derigjennom nasjonale sikkerhetsinteresser. Nasjonale sikkerhetsinteresser styrkes gjennom næringsklyngeeffekter, ved at norske hovedkontor gjerne tiltrekker seg kompetanse, forskningsressurser og investeringer, som sammen bygger opp et mer robust nasjonalt digitalt økosystem. Videre kan lokal tilstedeværelse bidra til å sikre tilgang til ekspertise i krisesituasjoner, og å styrke nasjonal beredskap gjennom tettere samarbeid med myndighetene.

Evne til å ta eller påvirke beslutninger om teknologi- og leverandørvalg
Statens evne til å ta eller påvirke beslutninger om teknologi- og leverandørvalg for kritisk digital infrastruktur kan være avgjørende for å sørge for at digital infrastruktur er pålitelig, trygg og i samsvar med nasjonale sikkerhetsinteresser. Styringsevnen handler om å kunne sette krav til hvilke leverandører og teknologier som tillates, basert på kriterier som sikkerhet og kvalitet, og som understøtter langsiktige strategiske mål. Dette innebærer også å redusere avhengigheten av utenlandske aktører som kan være underlagt fremmede staters interesser.

Evne til å ta eller påvirke beslutninger om driftskonsepter

Utkontraktering av kritiske funksjoner i tilknytning til digital infrastruktur til utlandet vil øke avhengigheten til utenlandske innsatsfaktorer. Videre kan driftskonsepter som opprettelse av fellesforetak eller konsortium sammen med utenlandske aktører øke den utenlandske innflytelsen på beslutninger som angår nasjonal kritisk digital infrastruktur. Statens styringsevne til å ta eller påvirke beslutninger om slike driftskonsepter handler da om å sørge for at den økte avhengigheten eller innflytelsen fra utlandet ikke får negativ påvirkning på nasjonale sikkerhetsinteresser. Aktuelle risikoer inkluderer blant annet redusert gjennomsiktighet og evne til å kontrollere sikkerhet hos de utenlandske tredjepartsaktørene, potensielle interessekonflikter mellom de samarbeidende partene i et fellesforetak eller konsortium, eller tap av strategisk nasjonal kunnskap og kompetanse.

Evne til å ta eller påvirke beslutninger om infrastrukturinvesteringer av strategisk interesse

Statens evne til å ta eller påvirke beslutninger om investeringer i digital infrastruktur som har strategisk og sikkerhetsmessig interesse, kan sees på fra to perspektiver. Det ene perspektivet er statens evne til å fremme infrastrukturinvesteringer som bygger opp under nasjonale strategiske sikkerhetsinteresser. Dette kan for eksempel være investeringer i fiberinfrastruktur for å bygge ut nasjonal redundans, styrke kapasitet og diversitet mellom Norge og utlandet, eller til Svalbard. Eller det kan være investeringer i sikkerhetsteknologi som skal styrke nasjonal digital infrastruktur.

Det andre perspektivet er statens evne til å kunne hindre infrastrukturinvesteringer i Norge («greenfield» investeringer) som svekker nasjonale sikkerhetsinteresser. Dette kan for eksempel være investeringer i fiberinfrastruktur til, eller i samarbeid med, land som Norge ikke har sikkerhetsmessig samarbeid med. Det kan være investeringer i nasjonal digital infrastruktur som skal benyttes til (fordekte) forskningsaktiviteter som kan true nasjonale sikkerhetsinteresser. Det kan også være investeringer i nye datasentre i Norge som direkte eller indirekte kan true nasjonale sikkerhetsinteresser, for eksempel på bakgrunn av hvem som eier eller er tenkt å ta i bruk datasenteret, hva datasenteret er tenkt å brukes til (f.eks. kryptoutvinning), eller omfanget av kraftressurser datasenteret beslaglegger.

Evne til å ta eller påvirke beslutninger om nasjonale beredskapstiltak for krise og krig

Denne evnen innebærer at staten kan ta beslutninger som legger til rette for at den nasjonale digitale infrastrukturen kan tåle påkjenninger i hele krisespekteret fred, krise og krig. Særlig i kontekst av stadig økende avhengighet til utenlandske innsatsfaktorer i den digitale infrastrukturen, så vil slike beslutninger ofte måtte handle om å sikre en nasjonal beredskap for krise og krig som kompenserer for avhengighetene som ligger utenfor nasjonal kontroll og jurisdiksjon. Men det kan også handle om å ta beslutninger om beredskapstiltak og -avtaler med internasjonale partnere og allierte, for å sikre tilgang til felles internasjonale innsatsfaktorer i krise og krig. Se for øvrig nedenfor om handlefrihet i punkt 11.2.2.

Evne til å ta eller påvirke beslutninger om prioritering av ressurser i krise og krig

I krise og krig må man legge til grunn at tilgjengeligheten til digital kommunikasjonsinfrastruktur og til ressursene for å drifte og vedlikeholde denne, kan bli kraftig redusert. Det er derfor viktig at staten har styringsevne til å ta eller påvirke beslutninger om hvordan begrensede ressurser skal prioriteres. Dette behovet kan forsterkes dersom man har sterk avhengighet til utenlandske ressurser

og innsatsfaktorer som man mister tilgang til. For eksempel kan det være snakk om å kunne ta beslutninger om trafikkstyring (f.eks. hvilke kommunikasjonstjenester som skal prioriteres), at enkeltaktører skal få prioritert tilgang til elektroniske kommunikasjonsnett (f.eks. Forsvaret), eller at staten overstyrer beslutninger om hvor tilgjengelig entreprenørkapasitet skal settes inn, for å ivareta nasjonale sikkerhetsbehov.

Evne til å beskytte skjermingsverdig informasjon om digital infrastruktur
Informasjon om norsk digital infrastruktur og norske forhold kan skade nasjonale sikkerhetsinteresser dersom den kommer på avveie. Staten må ha evne til å sette vilkår om hvordan slik informasjon skal kunne håndteres opp mot utenlandske eiere, partnere og underleverandører. For eksempel er det innenfor sikkerhetslovens domene klare krav knyttet til kontroll av skjermingsverdig informasjon. Imidlertid kan mange informasjonselementer om kritisk digital infrastruktur som ikke er skjermingsverdig, likevel være av stor verdi for utenlandsk etterretning. Dette kan være informasjonselementer knyttet til teknologi, arkitektur, driftskonsepter, beredskapstiltak osv., som samlet gir omfattende innsikt om norske forhold.

11.2.2 Statens handlefrihet

Tilgang til fysisk digital infrastruktur på norsk jord
Fysisk lokalisering av den digitale infrastrukturen på norsk jord gir myndighetene jurisdiksjon og kontroll over de rent fysiske innsatsfaktorene som ligger til grunn for f.eks. lagring av data og produksjon av elektroniske kommunikasjonstjenester. Noe slik infrastruktur, som f.eks. fiberkabler, vil implisitt være lokalisert på norsk jord. Annen infrastruktur, som f.eks. datasentre og tjenesteproduksjonsinfrastruktur for mobil- og internettjenester kan imidlertid være fysisk lokalisert utenfor landets grenser. Å ha fysisk kontroll på og jurisdiksjon over den fysiske infrastrukturen, kan være avgjørende for handlefriheten til f.eks. å kunne ta effektive beslutninger om prioriteringer om bruk av infrastrukturen i krise og krig. Tilgang til beredskapsmateriell og reserveutstyr plassert på norsk jord er også relevant i denne sammenheng.

Tilgang til fysisk digital infrastruktur i utlandet
For noen scenarioer kan det å ha fysisk digital infrastruktur plassert utenfor landets grenser, hos nære allierte, være fordelaktig. Dette gjelder særlig for sabotasje- og angrepsscenarioer der den nasjonale fysiske infrastrukturen blir fysisk ødelagt. Da vil det også å kunne nyttiggjøre seg tjenesteproduksjonsinfrastruktur som er fysisk plassert utenfor landets grenser, også bidra til å bygge opp under den nasjonale handlefriheten. For eksempel inngår det derfor i NSMs konseptvalgutredning om nasjonal sky, at data skal kunne evakueres til utlandet. Dette vil forutsette at det finnes tilgjengelig fysisk digital infrastruktur i utlandet for å migrere og oppbevare disse dataene.

Tilgang til nasjonale ressurser og kompetanse
Tilsvarende som for fysisk infrastruktur på norsk jord, vil også tilgang til nasjonale ressurser og kompetanse styrke statens handlefrihet i krise og krig. Slik tilgang er viktig for blant annet design, konfigurasjon, overvåkning, drift, utbygging og feilretting av den digitale infrastrukturen. Koronapandemien i 2020 er et nært eksempel på hvordan tilgang til ressurser fra utlandet, for eksempel entreprenørkapasitet, kan bli strupet. I en krise- eller krigssituasjon må man forvente at både tilgjengeligheten til utenlandske ressurser og kompetanse reduseres, og samtidig som behovet for de samme ressursene øker.

Tilgang til internasjonale ressurser og kompetanse
Gitt de komplekse og internasjonale verdikjedene som inngår i digital infrastruktur, vil det i praksis være umulig å ivareta handlefrihet utelukkende i form av tilgang til nasjonale ressurser og kompetanse for utvikling og drift. Derfor vil det være nødvendig å sikre handlefrihet også gjennom samarbeid med nære allierte, i Norden, NATO og EU. Et slikt samarbeid må ikke bare være basert på å ivareta behov i fredstid, men også ta inn over seg potensiell knapphet på ressurser og kompetanse, og tilhørende prioriteringer mellom allierte, i en krise- og krigssituasjon.

11.2.3 Samlet oversikt – forholdet mellom styringsevner og handlefrihet og nasjonale sikkerhetsinteresser

I tabell 11.1 og 11.2 oppsummerer utvalget drøftingene i punktene over, gjennom å kort beskrive hva som er de generelle sikkerhetsmessige begrunnelsene for de styringsevnene og handlefrihetene som staten har behov for. Dette danner igjen grunnlag for å definere konkrete målbilder som omtales i neste delkapittel.

Tabell 11.1 Styringsevner

Statens evne til å ta/ påvirke beslutninger	Sikkerhetsmessig begrunnelse
Eierskapstransaksjoner	Hindre at utenlandske aktører får kontroll med forvaltningen av infrastruktur på en slik måte at det innebærer risiko for spionasje, påvirkningsoperasjoner, leveransenekt, sabotasje, e.l.
Plassering av hovedkontorfunksjoner i Norge	Sikre tett myndighetsdialog med statlig eide selskaper som forvalter strategisk viktig digital infrastruktur. Næringsklyngeeffekter styrker tilgang til ekspertise i krisesituasjoner.
Teknologi- og leverandørvalg	Sikre pålitelighet og trygghet ved å sette krav til utenlandske leverandører og å redusere avhengighet av utenlandske aktører som kan være underlagt fremmede staters interesser.
Driftskonsepter (utkontraktering, fellesforetak, konsortium)	Unngå sikkerhetstruende utenlandske verdikjeder ved utkontraktering og negativ utenlandsk innflytelse eller interessekonflikter i samarbeid med utenlandske aktører.
Infrastrukturinvesteringer av strategisk interesse	Fremme infrastrukturinvesteringer som styrker nasjonal sikkerhet, robusthet og redundans, og hindre infrastrukturinvesteringer som truer nasjonale sikkerhetsinteresser.
Beredskapstiltak for krise og krig	Forberede nasjonal digital infrastruktur for krise og krig som kompenserer for avhengigheter til utenlandske innsatsfaktorer, for eksempel gjennom nasjonale beredskapslagre.
Prioritering av ressurser i krise og krig	Sikre at staten kan prioritere ressurser for digital infrastruktur, som kan være begrenset av avhengigheter til utenlandske innsatsfaktorer. Inkluderer trafikkstyring og tilgang til nett.
Beskytte skjermingsverdig informasjon	Sikre at skjermingsverdig informasjon om norsk digital infrastruktur beskyttes i møte med utenlandske eiere, partnere og underleverandører.

Tabell 11.2 Handlefriheter

Statens handlefrihet	Sikkerhetsmessig begrunnelse
Tilgang til fysisk digital infrastruktur på norsk jord	Jurisdiksjon og kontroll over de fysiske innsatsfaktorene som ligger til grunn for datalagring og produksjon av digitale tjenester, inkludert reservemateriell og utstyr.
Tilgang til fysisk digital infrastruktur i utlandet	Tilgang til fysisk digital infrastruktur hos allierte for dataevakuering og tjenesteproduksjon ved sabotasje og ødeleggelse av infrastruktur i Norge.
Tilgang til nasjonale ressurser og kompetanse	Jurisdiksjon og kontroll over ressurser og kompetanse for design, konfigurasjon, overvåking, drift, utbygging og feilretting av digital infrastruktur.
Tilgang til internasjonale ressurser og kompetanse	Samarbeid og planverk med allierte i Norden, NATO og EU for (gjensidig) utnyttelse av felles ressurser og kompetanse i krise og krig, som ikke kan oppnås gjennom nasjonale ressurser og kompetanse.

11.3 Utarbeidelse av konkrete målbilder

Med utgangspunkt i styringsevnene og handlefrihetene i tabell 11.1 og 11.2 i punkt 11.2.3, så vil det være mulig for staten å bygge et samlet målbilde for de ulike kategoriene av infrastrukturer som vist i figur 5.1 i punkt 5.2. Dette kan gjøres ved å vurdere hvordan styringsevnene og handlefrihetene bidrar til nasjonale sikkerhetsinteresser i tabellen over, med konkrete målsetninger for hver enkelt infrastrukturkategori. På denne måten kan behovet for nasjonal kontroll identifiseres på tvers av «økosystemet» for digital infrastruktur:

- Passiv infrastruktur (f.eks. fiberinfrastruktur, herunder sjøfiber)
- Støtteinfrastruktur (f.eks. datasentre, fortifikatoriske anlegg, mobiltårn, jordstasjoner, klokkeinfrastruktur, nummerportering og opprinnelsesmarkering)
- Tjenesteproduksjonsinfrastruktur (f.eks. transportnett, bredbåndsnett, internett-infrastruktur, mobilnett og satellittkommunikasjonsinfrastruktur)

I tillegg vil behovet for nasjonal kontroll med personellressurser og kompetanse tas med i beregningen. Rasjonalet for denne helhetlige tilnærmingen er å unngå blindsoner som kan oppstå ved å rette for mye oppmerksomhet mot å sikre nasjonal kontroll med én eller noen typer infrastrukturer og funksjoner, mens man «glemmer» andre.

Det ligger utenfor utvalgets mandat å etablere et komplett målbilde som omfatter alle relevante infrastrukturkategorier. Denne oppgaven bør gjennomføres av myndighetene og vil også, avhengig av detaljeringsgrad, sannsynligvis være skjermingsverdig. Utvalget inkluderer likevel et eksempel i tabell 11.3 på hvordan et delmålbilde kan bygges ut for en gitt infrastrukturkategori. I eksemplet har utvalget gått nærmere inn på (passiv) fiberinfrastruktur.

Tabell 11.3 Eksempel på styringsevner som kan inngå i et målbilde for fiberinfrastruktur

Statens evne til å ta/ påvirke beslutninger	Eksempel på aktuelle momenter til målbilde for kategori: fiberinfrastruktur
Eierskapstransaksjoner	Styringsevne til å gjennomføre investeringskontroll for fiberselskaper underlagt sikkerhetsloven og eventuelt andre fiberselskaper som forvalter strategisk viktige fiberforbindelser.
Plassering av hovedkontorfunksjoner i Norge	Styringsevne til å sikre at hovedkontorfunksjoner til statlig eide selskaper som råder over særlig strategisk viktig fiberinfrastruktur forblir i Norge.[133]
Teknologi- og leverandørvalg	Styringsevne til å ta eller påvirke beslutninger om valg av opprinnelsesland for fiberprodusenter som skal benyttes til kritisk fiberinfrastruktur. Styringsevne til å ta eller påvirke beslutninger om valg av opprinnelsesland for fiberleverandører som skal benyttes til kritisk fiberinfrastruktur.
Driftskonsepter (utkontraktering, fellesforetak, konsortium)	Styringsevne til å ta eller påvirke beslutninger om etablering av fellesforetak/konsortium med utenlandske aktører for utbygging av fiberinfrastruktur som har nasjonalt strategisk og sikkerhetsmessig interesse.
Infrastrukturinvesteringer av strategisk interesse	Styringsevne til å gjennomføre investeringskontroll av utenlandsk greenfield investeringer av fiberinfrastruktur i Norge. Styringsevne til å gjennomføre egne investeringsbeslutninger om å bygge nye fiberstrekk som styrker nasjonal robusthet og redundans nasjonalt eller mot utlandet.
Beredskapstiltak for krise og krig	Styringsevne til å ta eller påvirke beslutninger om fiberselskapers bestykking av beredskapslagre med fiber- og retteutstyr. Styringsevne til å gjennomføre egne investeringsbeslutninger om å bestykke nasjonale beredskapslagre med fiber- og retteutstyr.
Prioritering av ressurser i krise og krig	Styringsevne til å ta kontroll på fiberinfrastruktur for å disponere kapasitet etter statens behov i krise/krig, f.eks. for Forsvaret.
Beskytte skjermingsverdig informasjon	Styringsevne til å sikre beskyttelse av skjermingsverdig informasjon om fibertopologi og føringsveier overfor fiberutenlandske eiere, partnere og leverandører.

[133] Dette forutsetter at staten har tatt stilling til *hvilke* selskaper som bør være under statlig eierskap. Dette er en dynamisk vurdering, jf. kapittel 11.5

Tabell 11.4 Eksempel på handlefriheter som kan inngå i et målbilde for fiberinfrastruktur

Statens handlefrihet	Eksempel på aktuelle momenter til målbilde for kategori: fiberinfrastruktur
Tilgang til fysisk digital infrastruktur på norsk jord	Landsdekkende nasjonal fiberinfrastruktur med redundans, jf. Nkoms målbilder om robuste transmisjonsnett for Norge 2030.[134] Nasjonale beredskapslagre dimensjonert for relevante krise-/krigsscenario.
Tilgang til fysisk digital infrastruktur i utlandet	Redundans mellom Nord- og Sør-Norge via fiberføringer i Sverige, jf. Nkoms målbilde om fiberredundans gjennom Nordland.[135] Nordiske beredskapslagre dimensjonert for relevante konflikt-/krigsscenario, jf. anbefaling om digital sikkerhet i totalberedskapskommisjonen.
Tilgang til nasjonale ressurser og kompetanse	Nasjonal entreprenørkapasitet (fiberlegging, fiberretting) dimensjonert for relevante konflikt-/krigsscenario. Nasjonal rettekapasitet for kystnære sjøfiberkabler (kabelskip, utstyr og kompetanse). Nasjonal rettekapasitet for sjøfiberkabler på norsk kontinentalsokkel (kabelskip, utstyr og kompetanse).
Tilgang til internasjonale ressurser og kompetanse	Nordisk samarbeid om entreprenørressurser i krisesituasjoner. Internasjonalt samarbeid om rettekapasitet for sjøfiberkabler på norsk kontinentalsokkel.

11.4 Gap mellom nåsituasjon og målbildene

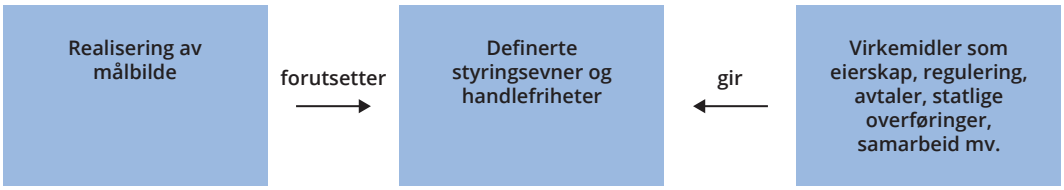
Mens utvalget i punkt 11.3 går nærmere inn på hvordan myndighetene kan etablere konkrete målbilder for hver infrastrukturkategori, drøfter utvalget her hvordan et eventuelt gap mellom målbildene og nåsituasjonen kan identifiseres.

At et målbilde er realisert innebærer at staten har – og evner å ta i bruk – egnede virkemidler som gir de nærmere definerte styringsevnene. Videre innebærer det at staten har benyttet virkemidlene til å etablere den nødvendige handlefriheten i form av de beskrevne tilgangene til infrastruktur, ressurser og kompetanse. Dette forholdet illustreres i figur 11.2.

[134] «Robuste transmisjonsnett for Norge mot 2030 – Målbilder og virkemidler», Nkom, 2022

[135] «Ekominfrastruktur i Nordland – Regional risiko- og sårbarhetsanalyse for Nordland», Nkom, 2023

Figur 11.2 Forholdet mellom målbilde og virkemidler.



Utvalget har i kapittel 9 gitt en beskrivelse av de virkemidlene staten rår over, som kan gi grunnlag for slik nasjonal kontroll. Disse kan oppsummeres som følger:

- Nasjonalt eierskap (statlig, kommunalt/fylkeskommunalt og privat)
- Regulering (f.eks. sikkerhetsloven, ekomloven, digitalsikkerhetsloven, beredskapslovgivning, lov om militære rekvisisjoner, mv.)
- Statlige overføringer
- Kontrakter og avtaler (statlig tjenestekjøp og andre privatrettslige avtaler)
- Informasjon, veiledning, dialog og samarbeid
- Internasjonalt samarbeid

Det er åpenbart at de forskjellige styringsevnene og handlefrihetene forutsetter ulike typer virkemidler. Utvalget vurderer at regulering vil være det mest sentrale i virkemiddelapparatet for nasjonal kontroll med digital kommunikasjonsinfrastruktur, men at de øvrige virkemidlene også er viktige for å utfylle målbildet. Ser man på eksempelet med fiberinfrastruktur i tabell 11.3, vil regulering være sentralt for mange styringsevner, men også en rekke andre virkemidler.

For eksempel vil «*styringsevne til å sikre at hovedkontorfunksjoner til statlig eide selskaper som råder over særlig strategisk viktig fiberinfrastruktur forblir i Norge*» måtte realiseres gjennom eierskap, ved at staten beholder over en tredel eierskap i de aktuelle selskapene. Se eksempel i tabell 11.5, jf. figur 11.2.

Tabell 11.5 Eksempel på gapvurdering, og hvor fastsetting av gap/avvik mellom målbildet og gjeldende tilstand kan representeres langs tre nivåer (begrenset/moderat/betydelig gap).

Realisering av målbilde (gap)			Definert styringsevne/ handlefrihet	Vurdering av virkemidler
Begrenset gap	Moderat gap	Betydelig gap		
			Plassering av hovedkontor-funksjoner i Norge Styringsevne til å sikre at hovedkontorfunksjoner til statlig eide selskaper som råder over særlig strategisk viktig fiberinfrastruktur forblir i Norge.	Norge har 100 % statlig eierskap i Space Norway AS som eier Svalbardfiberen, og ca. 38 % i Telenor Fiber AS (gjennom Telenor ASA) som er Telenors fiberselskap. Dette er tilstrekkelig til å sikre at hovedkontorfunksjonene forblir i Norge (mer enn 1/3 statlig eierskap).
x				

Tilsvarende må myndighetene vurdere statens virkemidler for de andre styringsevnene og handlefrihetene innenfor infrastrukturkategorien. Dersom man for eksempel ser på styringsevnen «*Beslutninger om fiberselskapers bestykking av beredskapslagre med*

fiber- og retteutstyr» kan dette realiseres gjennom regulatoriske krav – hovedsakelig beredskapskravene i ekomloven. Dersom staten har behov for beredskapsnivå ut over det fiberoperatørene er pålagt gjennom ekomloven å finansiere selv, kan det finansieres gjennom statlige overføringer, for eksempel tilskuddsordningen for telesikkerhet og beredskap.

Et annet eksempel er målsetningene om handlefriheter knyttet til fiberinfrastruktur. Når det gjelder «Internasjonalt samarbeid om rettekapasitet for sjøfiberkabler på norsk kontinentalsokkel», vil det primære virkemidlet være internasjonale avtaler. I dag samarbeider europeiske operatører av sjøfiberkabler blant annet gjennom Atlantic Cable Maintenance & Repair Agreement (ACMA) som er en avtale for vedlikehold og reparasjon av undersjøisk infrastruktur.[136] Altibox, Tampnet og Equinor er norske selskaper som inngår i dette samarbeidet. Hendelser den siste tiden i våre nærområder tyder på at kapasitetsbehovet og internasjonalt samarbeid bør styrkes på dette området, og det er allerede igangsatt flere initiativer med internasjonalt samarbeid, f.eks. mellom nordsjølandene[137], de nordiske landene[138], gjennom FN[139] og NATO[140], se omtale i punkt 9.7.

Når det gjelder handlefriheten «Nasjonal rettekapasitet for kystnære sjøfiberkabler (kabelskip, utstyr og kompetanse)», så vil regulering være det sentrale virkemidlet, gjennom blant annet sikkerhets- og beredskapskravene i ekomloven. For eksempel oppgir Telenor å disponere to kabelskip til formålet, stasjonert i henholdsvis Harstad og Bergen.[141] Det er også inngått samarbeidsavtale mellom elleve andre operatører om kabelskip langs store deler av kysten.[142] Samarbeid og dialog mellom operatører, og mellom operatører og myndigheter vil være et viktig supplement til de regulatoriske virkemidlene i krise- og krigssituasjoner.

For handlefriheten «Nasjonal rettekapasitet for sjøfiberkabler på norsk kontinentalsokkel (kabelskip, utstyr og kompetanse)», så kan dette kreve andre kapasiteter enn kabelskipene som opererer i kystnære områder. Utover regulatoriske virkemidler, kan aktuelle virkemidler for slik kapasitet under nasjonal kontroll både være statlig eierskap (f.eks. kapasitet gjennom Forsvaret), eller statlig tjenestekjøp.

Der de nødvendige virkemidlene ikke finnes eller ikke er fullt ut dekkende, så vil det være et gap mellom nåsituasjonen og målbildet. Da kan det for eksempel være behov for å endre gjeldende regulering eller fastsette nye regler.

Det kan også oppstå et gap dersom aktuelle virkemidler finnes, men ikke tas i bruk. Dette kan typisk skyldes mangel på ressurser hos myndighetene, manglende myndighetsfinansiering (for tilskuddsordninger), eller at handels- eller sikkerhetspolitiske forhold setter begrensninger for bruken. I en gapanalyse er det derfor viktig å identifisere slike potensielle begrensninger.

136 https://www.acma2017.com/

137 https://www.regjeringen.no/no/aktuelt/samarbeid-for-a-sikre-kritisk-undersjoisk-infrastruktur/id3033122/

138 https://www.norden.org/en/declaration/joint-statement-nordic-and-baltic-ministers-digitalisation

139 https://www.regjeringen.no/no/aktuelt/norge-slutter-seg-til-internasjonalt-initiativ-om-undersjoiske-kabler/id3075280/

140 https://www.nato.int/cps/en/natohq/news_225582.htm

141 https://www.telenor.no/om/presse-og-media/pressemeldinger/telenor-styrker-beredskapen-langs-finnmarkskysten.page

142 off_rapport_sarbarhetsanalyse_for_trondelag_2024-02-05.pdf

En komplett gapanalyse for kritisk digital kommunikasjonsinfrastruktur vil kunne være omfattende, men samtidig gjennomførbar når arbeidet brytes ned i delmålbilder for konkrete infrastrukturkategorier med tilhørende definerte styringsevner og handlefriheter. Gapanalysen av én infrastrukturkategori kan da også aggregeres og analyseres sammen med gapanalysene til de andre infrastrukturkategoriene. Dette vil gjøre det mulig for myndighetene å trekke ut overordnede observasjoner. Tabell 11.6 illustrerer hvordan en aggregert gapanalyse kan identifisere at én type infrastrukturkategori har svak nasjonal kontroll sett i forhold til andre kategorier, og at én type handlefrihet mangler på tvers av alle infrastrukturkategorier.

Tabell 11.6 Illustrasjon på en samlet gapanalyse som viser hvordan trender på tvers av infrastrukturkategorier kan identifiseres. Dette er et fiktivt eksempel.

	Infrastrukturkategori								
	A	B	C	D	E	F	G	H	I
Styringsevne									
Eierskaps-transaksjoner									
Hovedkontor-funksjoner									
Teknologi-/ leverandørvalg									
Driftskonsepter									
Infrastruktur-investeringer									
Beredskapstiltak									
Prioritering i krise og krig									
Beskyttelse av informasjon									
Handlefrihet									
Infrastruktur i Norge									
Infrastruktur i utlandet									
Ressurser/kompetanse i Norge									
Ressurser/kompetanse i utlandet									

Infrastrukturkategori C har generelt stort gap med tanke på nasjonal kontroll

Tilgang til ressurser og kompetanse i Norge er en generell utfordring for de fleste kategorier digital kommunikasjonsinfrastruktur

11.5 Strategier og handlingsplaner

Som beskrevet i punkt 11.1 anbefaler utvalget at det arbeides proaktivt med nasjonal kontroll, i tillegg til de reaktive kontrollene. Dette innebærer at det må etableres proaktive strategier og handlingsplaner for hvordan gap kan lukkes og målbildet for nasjonal kontroll nås – og ivaretas – over tid. Utvalget har pekt på at hvilken virkemiddelbruk som er best egnet, varierer på bakgrunn av både infrastrukturkategori, styringsevner og handlefriheter. Videre vil noen gap representere større risiko for nasjonale sikkerhetsinteresser enn andre. Det er derfor viktig å etablere overordnede strategier for virkemiddelbruken. Det kan for eksempel være at myndighetene ser behov for at staten tar en aktiv rolle gjennom eierskap på nye strategiske områder, slik Norge har gjort på satellittområdet. Eller det kan være det motsatte; at staten ser fordeler ved økt utenlandsk eierskap på visse områder, gjennom at det bidrar til styrket sikkerhet gjennom økte infrastrukturinvesteringer i Norge, og uten at det påviselig går på bekostning av styringsevnen og handlefriheten.

Etter utvalgets syn bør de proaktive grepene for å oppfylle målbilder for nasjonal kontroll integreres i eksisterende arbeid med strategier og handlingsplaner relatert til sikkerhet og beredskap. Utvalget vil særlig peke på følgende:

- **Nasjonal digitaliseringsstrategi**: Den nye strategien fra 2024 har et konkret tiltak om at regjeringen frem mot 2030 vil «sikre tilstrekkelig nasjonal kontroll med den delen av den digitale grunnmuren som understøtter kritiske samfunnsfunksjoner». Utvalget anser dette å være det overbyggende tiltaket som skal sikre oppfyllelse av et målbilde om nasjonal kontroll med digital kommunikasjonsinfrastruktur.
- **Statens eierskapsstrategi, jf. eierskapsmeldingen**: Statlig eierskap vil være et langsiktig virkemiddel som er aktuelt for å sikre nasjonal kontroll og kompetanse med de mest kritiske digitale kommunikasjonsinfrastrukturene. Dersom det avdekkes behov for å styrke det statlige eierskap på noen områder innenfor økosystemet for kritisk digital kommunikasjonsinfrastruktur, må dette integreres i statens eierskapsstrategi.
- **Sivilt beredskapssystem (SBS)**: SBS, som sammen med Forsvarets beredskapssystem (FBS) utgjør Nasjonalt beredskapssystem (NBS), vil være aktuelt å revidere i lys av tiltak for nasjonal kontroll. Dette kan være operasjonalisering av tiltak med hjemmel i ekomloven og sikkerhetsloven, og øvrige samarbeidstiltak.
- **Ny nasjonal datasenterstrategi**: Regjeringen har bebudet ny nasjonal datasenterstrategi i løpet av 2025. Utvalget mener at det i strategien bør tas høyde for at det kan etableres konkrete målbilder for nasjonal datasenterkapasitet herunder for fortifikatoriske datasentre, og for datasenterkapasitet i utlandet nødvendig for å ivareta nasjonal kontroll.
- **Nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT):** Strategien fra 2018 har mål om at samfunnets sårbarhet for svikt i satellittbaserte PNT-systemer skal reduseres, men peker på at tiltak må vurderes innenfor hver sektor. Et målbilde om nasjonal kontroll gjennom nasjonal tidstjeneste basert på bakkebasert infrastruktur vil være til dels sektorovergripende. PNT-strategien bør derfor oppdateres og klargjøres i lys av dette.
- **Langtidsplanen for Forsvaret og handlingsplaner som følger av Totalberedskapsmeldingen:** Jf. kapittel 4.4.2 kommer begge inn på forhold rundt nasjonal kontroll knyttet til digital infrastruktur. Det er naturlig at utvalgets anbefalinger sees i sammenheng med disse handlingsplanene.

- **Nasjonal sikkerhetsstrategi:** Ifølge totalberedskapsmeldingen arbeider regjeringen med å utarbeide en nasjonal sikkerhetsstrategi som skal se helhetlig på utenriks-, sikkerhets-, forsvars-, og beredskapspolitikken. Strategien skal legges frem før sommeren 2025. I denne sammenheng vil det være naturlig å vurdere eventuell overføringsverdi av dette utvalgets arbeid innenfor ekomsektoren til andre sektorer som forvalter kritisk infrastruktur, slik det også presiseres i totalberedskapsmeldingen.

11.6 Oppsummering og anbefalinger

I dette kapittelet har utvalget beskrevet en strukturert tilnærming til nasjonal kontroll, gjennom en modell for å etablere et målbilde med konkrete styringsevner og handlefriheter, analysere aktuelle virkemidler for å nå målbildet, og å fastsette proaktive strategier og handlingsplaner. Dette proaktive nivået vil da utgjøre et fundament for håndteringen av de reaktive screening- og kontrollmekanismene som beskrives i kapittel 12.

11.6.1 Etablere oversikt

Som et første steg må myndighetene ha oversikt over hvilken kritisk digital kommunikasjonsinfrastruktur det er viktig å sikre nødvendig nasjonal kontroll med, og hvilke virksomheter som forvalter denne. Digital kommunikasjonsinfrastruktur består av komplekse verdikjeder som er i dynamisk utvikling. Som det fremgår i punkt 5.4 mener Nkom å ha tilstrekkelig oversikt og informasjonstilgang knyttet til kritisk digital kommunikasjonsinfrastruktur gjennom den løpende forvaltningen og tilsynet med sektoren, selv om denne informasjonen ikke er strukturert i form av en konkret database/ oversikt per i dag.

Utvalget vil i denne sammenheng peke på at departementene etter sikkerhetsloven § 2-1 plikter å identifisere og holde oversikt over virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser innenfor sine ansvarsområder. Myndighetenes arbeid med dette bør også kunne utvides til å omfatte øvrig kritisk digital kommunikasjonsinfrastruktur og tilhørende virksomheter som det kan være viktig å sikre nødvendig nasjonal kontroll med. På denne bakgrunn mener utvalget følgende:

> **«Utvalget anbefaler at Digitaliserings- og forvaltningsdepartementet identifiserer og holder ved like en dokumentert oversikt over virksomheter i henhold til sikkerhetsloven § 2-1, samt øvrige virksomheter som forvalter digital kommunikasjonsinfrastruktur og funksjoner som anses samfunnskritiske.»**

11.6.2 Etablere målbilder

Som beskrevet i dette kapittelet bør vurderingen av hva som er nødvendig grad av nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur brytes ned til delmålbilder med konkrete styringsevner og handlefriheter som understøtter nasjonale sikkerhetsinteresser innenfor ulike typer infrastrukturkategorier.

Det er utenfor utvalgets mandat å definere disse målbildene, da dette vil være en myndighetsoppgave. Utvalget har likevel beskrevet et eksempel på hvordan konkrete styringsevner og handlefriheter kan defineres innenfor kategorien fiberinfrastruktur. På tilsvarende måte anbefaler utvalget at myndighetene etablerer delmålbilder innenfor de andre infrastrukturkategoriene:

> **«Utvalget anbefaler at Digitaliserings- og forvaltningsdepartementet etablerer og vedlikeholder et målbilde for nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur. Målbildet bør definere nødvendige nasjonale styringsevner og handlefriheter i fred, krise og krig, for de viktigste infrastrukturkategoriene i økosystemet for digital kommunikasjonsinfrastruktur, som inkluderer:**
> - ***Passiv infrastruktur*, herunder nasjonal fiberinfrastruktur og fiberkabler til utlandet**
> - ***Støtteinfrastruktur*, herunder nasjonal datasenterkapasitet, fortifikatoriske anlegg, mobiltårn, og nasjonal infrastruktur for nøyaktig tid/takt**
> - ***Tjenesteproduksjonsinfrastruktur*, herunder for bredbånd og transportnett, internettfunksjoner som DNS, ruting og samtrafikk, mobilkjernenett og basestasjoner, maritim kommunikasjonsinfrastruktur og bakkebasert satellittinfrastruktur**
>
> **Herunder bør målbildene beskrive behovet for personellressurser og kompetanse nødvendig for design og konfigurasjon, utbygging, drift og overvåking, feilretting og gjenopprettingsevne. Dette omfatter både infrastruktur på land til havs, herunder rettekapasitet for undersjøiske fiberkabler.»**

Utvalget mener det er noen infrastrukturkategorier som myndighetene bør følge opp relativt raskt. Disse kategoriene representerer områder hvor det pågår prosesser hvor et målbilde for nasjonal kontroll tidsmessig vil være relevant å ta hensyn til, og hvor samtidig nasjonal kontroll kan oppfattes særlig utfordrende på grunn av internasjonale verdikjeder.

Fiberinfrastruktur

Utvalget har i denne rapporten gitt et eksempel på hvordan et målbilde for nasjonal kontroll med fiberinfrastruktur kan utvikles. Denne infrastrukturen kan derfor være et naturlig utgangspunkt å starte med for myndighetenes målbildeutvikling. Som utvalget har vist til, så har myndighetene på dette området også satt i gang en rekke prosesser knyttet til fiberinfrastruktur, som sammenfaller godt med utviklingen av mål for nasjonal kontroll. Dette inkluderer allerede etablerte målbilder for robuste nett, regionale risiko- og sårbarhetsanalyser av fiberinfrastrukturen, og initiativer knyttet til kritisk undersjøisk fiberinfrastruktur.

Mobiltjenesteproduksjon

Mobilnettene er kanskje den mest samfunnskritiske kategorien kommunikasjonsinfrastruktur, ved at de understøtter svært mange kritiske samfunnsfunksjoner, og flere av GNF-ene innenfor elektronisk kommunikasjon. Samtidig er mobilnettene teknologisk svært komplekse og i kontinuerlig utvikling, gjennom virtualiserings- og skyteknologi, framvekst av nye leverandører og økosystemer, automatisering og integrasjon av kunstig intelligens. Denne kompleksiteten utfordrer

betydelig statens evne til å opprettholde nødvendig nasjonal kontroll. Samtidig kan det tenkes at staten, gjennom å etablere et konkret målbilde for nasjonal kontroll med mobilnett og mobiltjenesteproduksjon, proaktivt kan *utnytte* de nye teknologiene. For eksempel legger skybasert mobiltjenesteproduksjon (5G og i fremtiden 6G), virtualisering og automatisering til rette for at funksjonalitet, data, drifts- og støttesystemer «sømløst» kan flyttes mellom datasentre og produksjonsplattformer på norsk territorium og hos allierte land i en krisesituasjon. Et slikt beredskapstiltak forutsetter at staten på forhånd har den nødvendige styringsevnen til å pålegge mobiloperatørene å gjennomføre beredskapstiltaket når det behøves, for eksempel i en konflikt- eller krigssituasjon, og at statens handlefrihet er oppnådd ved at mobiloperatørene på forhånd har etablert de tekniske løsningene som behøves for å gjennomføre tiltaket raskt.

Nasjonal datasenterkapasitet, herunder fortifikatoriske datasentre og datasenterkapasitet i utlandet

Datasenternæringen får en stadig mer kritisk og integrert rolle i digital kommunikasjonsinfrastruktur, og understøtter den grunnleggende nasjonale funksjonen «evne til å ivareta datalagring og prosesseringskapasitet i Norge». Datasenter er også omfattet i ny lov om elektronisk kommunikasjon i kraft fra 2025. Et målbilde om nasjonal datasenterkapasitet, og datasenterkapasitet i utlandet for beredskap, må sees i sammenheng med kritiske samfunnsfunksjoners behov for slik datasenterkapasitet. Dette omfatter både sektorens egne behov, som blant annet fremkommer av målbilde om nasjonal kontroll for mobiltjenesteproduksjon beskrevet over, etableringen av sikker nasjonal skytjeneste, og behovet for fortifikatoriske anlegg/datasentre. Når det gjelder de fortifikatoriske anleggene i Norge så har Nkom, med bistand fra FFI, i 2023 og 2024 gjennomført en behovsvurdering. Myndighetene vurderer nå hvordan disse bør benyttes i fremtiden.[143] En konkretisering av mål for styringsevner og handlefriheter knyttet til fortifikatoriske anlegg, vil etter utvalgets vurdering være nyttig for beslutninger om fremtidig bruk og utvikling.

Infrastruktur for distribusjon av nøyaktig tid/nasjonal tidstjeneste

Mange samfunnsfunksjoner, herunder elektroniske kommunikasjonsnett, er avhengig av nøyaktig tid for blant annet synkronisering. Denne tidsreferansen hentes i mange tilfeller fra satellittbaserte systemer (blant annet GPS) og er derfor utenfor nasjonal kontroll. Dette kan utgjøre en sårbarhet, som blant annet omtalt i nasjonal PNT-strategi.[144] Både Totalberedskapskommisjonen[145] og Sikkerhetsfaglig råd fra NSM[146] har påpekt behovet for at det etableres en nasjonal tidstjeneste basert på sikrede, bakkebaserte atomklokker og distribusjon via elektroniske kommunikasjonsnett. I januar 2025 fikk Nkom og Justervesenet i oppdrag fra sine eierdepartementer å kartlegge behovet og utrede løsninger for en nasjonal infrastruktur for distribusjon av nøyaktig tid/klokkesignal.[147] Utredningen skal være ferdig innen utgangen av juni 2025. Utvalget mener at en etablering av et målbilde for nasjonal kontroll med infrastruktur for nøyaktig tid etter modellen beskrevet over, vil kunne være en nyttig del av denne behovsvurderingen.

143 Nkom årsrapport 2023

144 https://www.regjeringen.no/contentassets/abd1dec7647a4c22aaef7d93046e3f2b/pa-rett-sted-til-rett-tid.pdf

145 NOU 2023: 17

146 Sikkerhetsfaglig råd – Et motstandsdyktig Norge, NSM, https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglig-rad-et-motstandsdyktig-norge

147 Brev av 7. januar 2025 fra Digitaliserings- og forvaltningsdepartementet til Nkom.

11.6.3 Gjennomføring av gapanalyse

Utvalget har beskrevet en metodikk for å analysere aktuelle virkemidler for å nå målbildet, og å fastsette proaktive strategier og handlingsplaner for å bruke disse virkemidlene for nå målbildene. Dette arbeidet vil måtte være en integrert del av det øvrige forvaltningsarbeidet med å ivareta sikkerhet og beredskap for nasjonal kommunikasjonsinfrastruktur, og ikke et isolert arbeid. Derfor har utvalget også anbefalt at dette integreres inn i de eksisterende strategier og handlingsplaner. Likevel må det gjennomføres en initiell gapanalyse av målbildet og deretter løpende vedlikehold av denne. Utvalget anbefaler derfor:

> **«Utvalget anbefaler at når et målbilde for nasjonal kontroll er etablert bør Digitaliserings- og forvaltningsdepartementet utvikle og vedlikeholde en gapanalyse av målbildet som beskriver de aktuelle virkemidlene staten rår over, og eventuelle svakheter, begrensninger og hindre for å bruke disse for å sikre de nødvendig styringsevner og handlefriheter.»**

”

Screening eller kontroll forutsetter at myndighetene er kjent med at en økonomisk aktivitet er planlagt. Myndighetene kan få informasjon om den planlagte økonomiske aktiviteten gjennom at de involverte partene i transaksjonen har meldeplikt til myndighetene om dette, blant annet jf. kapittel 10 i sikkerhetsloven.

Foto: Ian Battaglia (Unsplash)

12

Nærmere om screening og kontroll med økonomiske aktiviteter

12.1 Innledning

Utvalget har i kapittel 11, jf. også trussel- og risikobildet beskrevet i kapittel 4, påpekt at det er behov for at myndighetene gjennomfører screening og kontroll med ulike kategorier kontrollreduserende økonomiske aktiviteter. Dette omtaler utvalget som det reaktive nivået, ettersom screeningen eller kontrollen først aktiveres idet en markedsaktør planlegger å gjennomføre en nærmere bestemt økonomisk aktivitet.

I dag kan myndighetene med hjemmel i sikkerhetsloven gripe inn i utenlandske investeringer som medfører en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Regjeringen har også foreslått å utvide denne screeningen til å omfatte virksomheter i kritiske sektorer som ikke er underlagt sikkerhetsloven, jf. Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen*. I tillegg har utvalget beskrevet et behov for at myndighetene har oversikt over og kontroll med også andre aktiviteter enn utenlandsinvesteringer som kan svekke nasjonal styringsevne og handlefrihet. Dette gjelder for eksempel salg av eiendeler i infrastrukturselskaper, og ulike endringer av driftskonsepter. Selv om slike økonomiske aktiviteter både kan være lovlige (og i tillegg ha positive sikkerhetseffekter) isolert sett, kan de samtidig være del av utviklingstrekk som over tid bidrar til å svekke nasjonal styringsevne og handlefrihet gjennom økt utenlandsk innflytelse. Utvalget mener derfor at myndighetene må ha evne til:

a. Screening av utenlandsinvesteringer (nyetablering og erverv av eierandeler)
b. Oversikt/kontroll over salg av eiendeler i kritiske infrastrukturselskaper
c. Oversikt/kontroll over aktiviteter knyttet til vesentlige endring av driftskonsepter (strategiske partnerskap, leverandørvalg og utkontraktering)

I punkt 12.2 drøfter utvalget overordnede prinsipper for gjennomføringen av slik screening og kontroll. Deretter går utvalget i punkt 12.3 nærmere inn på de pågående prosessene knyttet til nytt screeningregelverk, og hva dette vil bety for screening i sektoren for elektronisk kommunikasjon, jf. punkt a) i listen over. I punkt 12.4 vurderer utvalget det eksisterende regelverket for screening og kontroll, herunder kontroll med salg av eiendeler og endringer i driftskonsepter, jf. punkt b) og c) i listen over.

12.2 Overordnede prinsipper for screening og kontroll av økonomiske aktiviteter som kan ha kontrollsvekkende effekt

Som beskrevet i kapittel 11 vil et målbilde for kritisk digital kommunikasjonsinfrastruktur utgjøre et viktig fundament for den reaktive screeningen og kontrollen. Målbildet og gapanalyser vil kunne bidra til å identifisere behov for nye inngrepshjemler eller reaksjonsmidler, og ha disse på plass i forkant av kontrollreduserende endringer som er i ferd med å skje. Et målbilde vil også gi myndighetene et bedre grunnlag for å gjøre de nødvendige risikovurderingene når de økonomiske aktivitetene skal screenes eller kontrolleres.

Screening eller kontroll forutsetter at myndighetene er kjent med at en økonomisk aktivitet er planlagt. Myndighetene kan få informasjon om den planlagte økonomiske aktiviteten gjennom at de involverte partene i transaksjonen har meldeplikt til myndighetene om dette, blant annet jf. kapittel 10 i sikkerhetsloven. Myndighetene kan også få informasjon ved at aktøren på eget initiativ ber myndighetene om råd, eller at myndighetene på annen måte blir gjort kjent med dette, for eksempel ved tilsyn.

Meldeplikten i sikkerhetsloven, og eventuelt utvidet meldeplikt etter nytt screeningregelverk vil gjelde erverv av eierandeler i en virksomhet. Meldeplikten dekker dermed ikke andre mulige kontrollsvekkende økonomiske aktiviteter, som salg av eiendeler som medfører at deler av virksomheten flyttes ut av et foretak, og endring av driftskonsepter, eksempelvis utkontraktering til en utenlandsk leverandør. I de tilfellene antar utvalget at myndigheten må gjøres kjent med disse gjennom at aktørene selv orienterer myndighetene. Dette vil være sårbart med tanke på myndighetenes behov for oversikt og kontroll, og utvalget anbefaler derfor følgende:

> **«Utvalget mener at Digitaliserings- og forvaltningsdepartementet bør vurdere om sektorregelverket i tilstrekkelig grad sikrer tidlig informasjon til myndighetene om kontrollsvekkende økonomisk virksomhet fra selskapene som eier kritisk digital kommunikasjonsinfrastruktur, og bøte på eventuelle svakheter.»**

Forutsatt at myndighetene er gjort kjent med den økonomiske aktiviteten, må myndighetene ta stilling til om endringen vil representere en trussel mot nasjonale sikkerhetsinteresser, blant annet gjennom reduksjon av nasjonal kontroll. Dette innebærer at det må gjennomføres en helhetlig risikovurdering av hva den økonomiske aktiviteten kan innebære. Utvalget vil understreke at nasjonal kontroll er ett av flere *virkemidler* for å ivareta nasjonale sikkerhetsinteresser, og ikke et mål i seg selv. Derfor vil en risikovurdering først og fremst styres av hvordan den aktuelle økonomiske aktiviteten kan påvirke risikoen for at *nasjonale sikkerhetsinteresser* kan bli skadelidende. Dette kan skje gjennom reduksjon av nasjonal styringsevne eller handlefrihet, men det kan også være andre faktorer som spiller inn i risikovurderingen.

Utvalget tar ikke stilling til hva som er den mest egnede måten å gjennomføre risikovurderinger på, men vil i det følgende drøfte aktuelle vurderingsmomenter som det anbefales å ta stilling til i vurderingen. Disse er strukturert i henhold til en modell beskrevet i Moran (2009), men vurderingsmomentene er utvalgets egne. For øvrig vises det til kapittel 4 om det overordnede risiko- og trusselbildet og punkt 8.4 som nærmere beskriver risikofaktorer knyttet til utenlandsk eierskap.

Et første steg vil være en kritikalitetstest av den økonomiske aktiviteten, som kan bestå av følgende spørsmål:

- Hvilken strategisk fordel overfor Norge vil den utenlandske aktøren og dens nasjonale myndigheter få ved å gjennomføre den økonomiske aktiviteten?
- Hva vil konsekvensen være dersom den utenlandske aktøren utnytter kontrollen over den nasjonale kommunikasjonsinfrastrukturen til å hindre eller sette betingelser på tilgang til infrastrukturen eller tjenesteleveransen?
- Hvor stort vil skadepotensialet være dersom den utenlandske aktøren utnytter kontrollen til spionasje eller til å ramme infrastrukturens eller tjenestens integritet?

Utvalget presiserer at dersom myndighetene har etablert et målbilde for den aktuelle infrastrukturkategorien som den økonomiske aktiviteten er rettet mot, vil det være enklere å identifisere konkret hva som anses kritisk. Målbildet vil dermed være til hjelp i å gjennomføre denne vurderingen. Et eksempel kan være en planlagt utenlandsk investering i et norsk fiberselskap. Dersom det er snakk om passiv fiberinfrastruktur, kan myndighetene komme til at eierskapet *ikke* vil kunne utnyttes til å hindre eller sette betingelser i tilgangen til fiberinfrastrukturen (andre kulepunkt). Derimot kan vurderingen være at et definert målbilde om «styringsevne til å beskytte skjermingsverdig informasjon om nasjonal fibertopologi» kan svekkes. Da vil skadepotensialet først og fremst være knyttet til spionasje (tredje kulepunkt), som igjen kan gi en utenlandsk myndighet en strategisk fordel overfor Norge (første kulepunkt).

Dersom myndighetenes samlede vurdering på disse spørsmålene er at kritikaliteten er høy, så er neste vurderingsmoment hvor plausibelt det er at nasjonale sikkerhetsinteresser kan bli skadelidende. Et viktig spørsmål er da om det finnes aktuelle tilgjengelige substitutter for tjenestene man potensielt mister kontroll med. Det vil si, finnes det alternative aktører i markedet som kan tilby det samme, og til hvilken byttekostnad? Jamfør eksemplet over, vil denne vurderingen være avhengig av hvilken konkret fiberinfrastruktur det er snakk om. Er det snakk om en utenlandsk investering i et fiberselskap som forvalter et omfattende landsdekkende fibernett eller særlig strategiske fibernett, så vil byttekostnaden åpenbart være større enn om det er snakk om et regionalt/lokalt fibernett hvor det også finnes flere alternative substitutter. Når kritikaliteten er vurdert høy og det heller ikke finnes reelle substitutter dersom trusselen utløses, så vil dette kunne være et grunnlag for å blokkere den økonomiske aktiviteten.

Utvalget vurderer Morans modell å være for forenklet til å utgjøre det eneste grunnlaget for en risikovurdering i en screening eller kontrollsak. For eksempel viser utvalget til punkt 6.3 som også peker på behovet for landvurderinger av opprinnelseslandet til den utenlandske aktøren (herunder politisk system, stabilitet og gjennomsiktighet), og om eierskap og makt er konsentrert på enkeltpersoner. Ytterligere vurderingsmomenter vil være hvilket sikkerhetsmessig samarbeid Norge har med det aktuelle landet, hvilke bånd den utenlandske aktøren har til egen stats myndigheter, hvorvidt geografisk avstand til opprinnelseslandet har betydning for risikoen, og hvilke potensielle sikkerhetstruende

virkemidler aktøren vil få tilgang til gjennom den økonomiske aktiviteten (plassering av innsidere, tilgang til cybervirkemidler, økonomiske virkemidler, virkemidler for påvirkningsoperasjoner osv.).

I tillegg mener utvalget at myndighetene må se på disse vurderingsmomentene både i forhold til kortsiktige og langsiktige effekter, og hvordan effektene kan endre seg i krisespekteret fred-krise-krig.

Gitt at myndighetene konkluderer med at det er en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser kan bli skadelidende, finnes det ulike handlingsalternativer. Forenklet kan handlingsalternativene sorteres i tre kategorier:

- Blokkere aktiviteten
- Tillate aktiviteten på vilkår
- Tillate aktiviteten (uten vilkår)

En sentral forutsetning for å blokkere en økonomisk aktivitet er at det finnes en tydelig hjemmel til å gjøre dette. Det vil typisk være sikkerhetsloven § 10-3 når det er snakk om utenlandsinvesteringer som truer nasjonal sikkerhet, eller det kan være ekomloven § 3-1 eller § 3-7 dersom et er snakk om for eksempel et driftskonsept som bryter med kravet om forsvarlig sikkerhet. Unntaksvis kan også sikkerhetsloven § 2-5 benyttes.

Myndighetene kan vurdere at det ikke er nødvendig for å blokkere den økonomiske aktiviteten, men at den kan tillates på visse vilkår. Dette ble for eksempel gjort i saken fra 2023 hvor Mubadala Investment Company kjøpte en kvalifisert eierandel i GlobalConnect AS sitt svenske morselskap Nordic Connectivity AB. Vilkårene gikk da ut på å hindre at sensitiv informasjon om norske sikkerhetsmessige forhold skal tilflyte uvedkommende, at myndighetene skal varsles ved eventuelle fremtidige sikkerhetstruende eierskifter, og visse begrensninger for videresalg av aksjer.[148]

Det tredje handlingsalternativet er å tillate aktiviteten uten vilkår, det vil si at myndighetene godkjenner – alternativt ikke griper inn i – selve transaksjonen. Dette kan være på grunn av at det enten ikke er hjemmelsgrunnlag for å stoppe aktiviteten, eller at det ikke er hensiktsmessig å gjøre det av andre grunner. Utvalget vil presisere at sistnevnte kan være tilfelle selv om det er åpenbart at aktiviteten svekker den nasjonale kontrollen og øker gapet til det definerte målbildet. Bakgrunnen for dette kan typisk være at økonomiske aktiviteter følger internasjonale markedstrender og teknologiutvikling som det er uhensiktsmessig å motarbeide, fordi det vil innebære en betydelig svekkelse av selskapets konkurranseevne.

Når myndighetene må tillate økonomiske aktiviteter som bidrar til å svekke den nasjonale kontrollen, mener utvalget at det er viktig å se på andre aktuelle kompenserende tiltak for å lukke målbildegapet. Dette kan da skje gjennom å revurdere eksisterende strategier og handlingsplaner som omtalt i det proaktive nivået i kapittel 11, og som kan innebære alt fra revisjon av regelverk, styrking av nasjonale beredskapslagre, statlige overføringer, styrking av internasjonalt beredskapssamarbeid, og styrket informasjon og rådgivning. De aktuelle virkemidlene er omtalt nærmere i kapittel 9.

[148] https://www.regjeringen.no/no/aktuelt/regjeringen-setter-vilkar-knyttet-til-kjop-av-eierandel-i-globalconnect/id2970605/

12.3 Utredninger om behovet for og arbeid med nytt screeningregelverk

Investeringskontrollutvalget har utredet behovet for screening av økonomisk aktivitet mot virksomheter som ikke er underlagt sikkerhetsloven. Investeringskontrollutvalget mener at dagens investeringskontroll er for snever og fragmentert og at det er behov for en mer helhetlig investeringskontroll på tvers av dagens sektorer og regelverk. I NOU 2023: 28 foreslås derfor at det utarbeides et nytt regelverk som regulerer investeringskontroll ved en sektorovergripende investeringskontrollov.

Investeringskontrollutvalget gjør rede for flere utfordringer ved dagens investeringskontroll i kapittel 13 i sin NOU. Blant annet fremheves det at saker som kan innebære risiko for nasjonale sikkerhetsinteresser ikke fanges opp i tilstrekkelig grad, at dagens ordning etter sikkerhetsloven av flere grunner skaper uforutsigbarhet og at myndighetene kan mangle egnet hjemmelsgrunnlag til å gripe inn ovenfor sikkerhetstruende investeringer.

Investeringskontrollutvalget foreslår derfor at det innføres en bredere investeringskontroll, hvor man heller har meldepliktordning for virksomheter i såkalte sikkerhetssensitive sektorer, fremfor utpeking av konkrete virksomheter som i dag. Investeringskontrollutvalget sier videre i punkt 19.2 at: «*Selv om hensynet med investeringskontrollen vil være å ivareta nasjonale sikkerhetsinteresser, mener utvalget at regelverket bør utformes slik at det ligner på andre regelverk som regulerer lovlig næringsvirksomhet, fremfor regelverk som håndterer trusler mot nasjonale sikkerhetsinteresser. Dette er fordi hoveddelen av aktiviteten som regelverket skal kontrollere, er både lovlig og ønskelig*»

Investeringskontrollutvalget foreslår også at alle saker om investeringskontroll behandles av én myndighet, at denne myndigheten skal motta alle meldinger som er omfattet av den foreslåtte meldeplikten og fatte vedtak i disse sakene. Investeringskontrollmyndigheten må kunne trekke på opplysninger fra andre relevante etater og en investeringskontrollov må tydelig angi et eventuelt behov for samarbeid med andre myndigheter. I NOU 2023: 28 punkt 13.5 redegjør utvalget for hvordan praktisering av sektorprinsippet kan hindre en enhetlig behandling av investeringskontrollsaker og sier blant annet følgende: *Etter utvalgets syn er sektorprinsippet et viktig grunnlag for arbeidet med forebyggende sikkerhet i Norge. Sektorprinsippet fremstår imidlertid lite egnet til kompliserte investeringskontrollsaker, hvor det er behov for høy grad av enhetlig, effektiv og profesjonell analyse og saksbehandling.*

I etterkant av at Investeringskontrollutvalget fremla NOU 2023: 28 i desember 2023, la Europakommisjonen i januar 2024 frem et forslag til ny forordning om obligatorisk screening av utenlandske direkte investeringer i EU. Forslaget, og også gjeldende screeningregelverk i EU, er nærmere beskrevet i punkt 10.5.

Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen* ble lagt frem 10. januar 2025. I meldingens punkt 8.2 fremgår det at regjeringen har igangsatt et arbeid for å utarbeide forslag til en ny lov for kontroll av utenlandske investeringer og at dette arbeidet skal ses i sammenheng med regelverksutvikling i EU på området.

Ekomsikkerhetsutvalget mener som tidligere nevnt i kapittel 11, at det er nødvendig å konkret vurdere ulike kontrollreduserende økonomiske aktiviteter og kunne gripe inn dersom disse kan skade nasjonale sikkerhetsinteresser. Dette betyr at det er behov for at

myndighetene får kunnskap om mulig kontrollreduserende økonomiske aktiviteter og at det gjøres risikovurderinger av disse. For at det reaktive nivået, jf. punkt 11.1.2, skal kunne operasjonaliseres tilstrekkelig effektivt, må kontrollomfanget utvides sammenliknet med i dag. Dette gjelder både med hensyn til type materielle saker og kretsen av virksomheter.

For transaksjoner som påvirker eierskap synes de pågående regelverksprosessene, både nasjonalt og i EU, å kunne legge bedre til rette for den kontrollmulighet utvalget mener at myndighetene må ha, for å reaktivt kunne følge opp etablerte målbilder som skal ivareta nasjonal kontroll.

Når det gjelder utvikling av et nytt norsk regelverk for investeringskontroll har Ekomsikkerhetsutvalget merket seg at både Investeringskontrollutvalget og Eldringutvalget har fremhevet behovet for harmonisering og samarbeid med EU.

Investeringskontrollutvalget peker blant annet på muligheten til å ta EUs gjeldene forordning om kontroll av utenlandske direkteinvesteringer inn i EØS-avtalen gjennom et tillegg til protokoll 31 og sier: *«Uavhengig av om EU-forordningen om kontroll av utenlandske direkteinvesteringer tas inn i norsk rett, er forordningens krav til regelverk for investeringskontroll en hensiktsmessig ramme for innretningen av et norsk regelverk. Forordningen har vært toneangivende for EU-landene som har utarbeidet eller revidert sine nasjonale regelverk de siste årene. EU-forordningen kan følgelig fungere som veiledning for norsk regelverk uten at den er rettslig forpliktende. Dette vil gjøre samarbeidet med EU og EUs medlemsland enklere og regelverket vil være mer gjenkjennelig for investorer.»*

Eldringutvalget tilråder at Norge bør følge samme regler og prosedyrer som våre europeiske handelspartnere når det gjelder investeringsscreening, og søke et tett samarbeid med EUs screeningmekanisme.

Eldringutvalget viser blant annet til at:

> «I løpet av de siste årene har EU lansert handelspolitiske instrumenter, som CBAM[149] og investeringsscreening, som skal beskytte det indre marked og europeiske virksomheter. Flere av disse utfordrer EØS-avtalen, fordi de ligger i grenselandet mellom EUs felles handelspolitikk – som Norge ikke tar del i – og reguleringen av det indre marked. Der Kommisjonen velger å forankre de nye reglene i handelspolitikken, risikerer Norge å bli behandlet som et tredjeland. Det innebærer i ytterste konsekvens at tiltakene kan benyttes mot norske aktører. I den grad virkemidlene forankres i indre markedsbestemmelser, kan det nye regelverket påvirke Norges handelspolitikk, for eksempel dersom det er nødvendig å sikre like vilkår i det indre markedet gjennom identiske eller tilsvarende tiltak. Det åpner også for ulike variasjoner av «bakdør»-problematikk. Dette fordrer at myndighetene tidlig tar stilling til hvordan man skal forholde seg til denne typen regelverk, enten gjennom initiativ til å ta det inn i EØS-avtalen, eller gjennom initiativ til å tilpasse seg på andre måter. Som ledd i slike vurderinger, må ikke nye EU-regler kun vurderes isolert. Det må også vurderes om manglende tilpasning til EUs handelspolitiske virkemidler eventuelt kan få negative konsekvenser for adgangen for norske næringsaktører på det indre marked.

[149] Carbon Border Adjustment Mechanism

> Der EU har kommet lengst i utviklingen av nye handelspolitiske instrumenter, er screening av utenlandsinvesteringer. EUs regelverk for investeringsscreening fra 2019 handler om å etablere en felles tilnærming til kontrollen av investeringer fra land utenfor EU (tredjeland), som kan utgjøre en risiko for sikkerhet eller offentlig orden. Utvalget støtter forslaget fra investeringskontrollutvalget om at Norge på dette området følger regler og prosedyrer som tilsvarer det som blir gjort av våre europeiske handelspartnere.»

Ekomsektoren er en kapitalintensiv næring hvor investeringsandelen målt mot omsetning i en årrekke har ligget på over 1/3. jf. punkt 3.2. Ekomsikkerhetsutvalget viser videre til punkt 8.4.8 hvor utvalget redegjør for negative konsekvenser ved redusert tilgang til finansiell kapital, fysisk kapital (teknologi) og human kapital (ekspertise) og at i dialogen med ekomaktørene har disse påpekt bekymringer for redusert tilgang til alle tre typene kapital. I valget mellom ellers like land, vil investorer foretrekke det landet som har færrest begrensninger eller usikkerhet knyttet til sitt regelverk. Utvalget legger til grunn at særnorske regler om investeringskontroll kan ha negativ innvirkning på blant annet kapitaltilgang, teknologitilgang og innovasjon, og mener at et EU-harmonisert norsk regelverk på dette området vil skape færre hindringer for norsk ekomsektor enn særnorske regler.

Avslutningsvis vil utvalget bemerke at Europakommisjonens nye forslag til forordning om obligatorisk screening av utenlandske direkte investeringer, er hjemlet i både i TEUF artikkel 114 og artikkel 207. Dette i motsetning til gjeldende forordning, som kun er hjemlet i TEUF artikkel 207. Kommisjonen anser at det er nødvendig å hjemle det nye regelverket i TEUF artikkel 114, fordi forslaget pålegger medlemsstatene å screene visse investeringer i det indre marked og avhjelpe forskjeller i medlemsstatenes screeningmekanismer som kan være til hinder for de grunnleggende friheter i traktaten, og dermed ha en direkte innvirkning på det indre markeds funksjon. Et regelverk hjemlet i TEUF artikkel 114 vil normalt tilsi at regelverket vil bli ansett EØS-relevant. Dersom ny forordning blir vedtatt med hjemmel i TEUF artikkel 114, vil regelverket trolig måtte tas inn i EØS-avtalen og gjennomføres i nasjonal rett i EØS EFTA-landene.

På denne bakgrunn har utvalget følgende forslag til tiltak:

> **«Utvalget mener regjeringen ved utarbeidelse av ny lov for kontroll av utenlandske investeringer bør se hen til EUs nye regelverk om screening av utenlandske direkte investeringer, uavhengig av om regelverket anses EØS-relevant.»**

Utvalget tar ikke stilling til Investeringskontrollutvalget sitt forslag om det det bør opprettes én investeringskontrollmyndighet. Utvalget har gjennom sitt arbeid observert at spørsmål knyttet til hvilken nasjonal kontroll som er nødvendig over forskjellige arter av kritisk digital kommunikasjonsinfrastruktur vil ha en betydelig kompleksitet ved seg. Det vil derfor være vanskelig for en dedikert investeringskontrollmyndighet å gjøre gode vurderinger av dette spørsmålet uten betydelig støtte fra sektorspesifikk fagkompetanse.

> **«Utvalget mener at dersom Nærings- og fiskeridepartementet går videre med Investeringskontrollutvalget sitt forslag om én investeringskontrollmyndighet, må Nærings- og fiskeridepartementet sikre at sektorspesifikk fagkompetanse blir tilgjengeliggjort for en slik etat.»**

12.4 Utfordringer med gjeldene regelverk

12.4.1 Innledning

Utvalgets vurderinger av regulatoriske grunnlag for screening og kontroll, omfatter både dagens regelverk og pågående prosesser om screeningregelverk. De foreslåtte tiltakene og anbefalingene i punkt 12.3 og 12.4, vil til en viss grad kunne være tematisk overlappende. Utvalget mener likevel at både tiltak og anbefaling knyttet til dagens eierskapskontroll er nødvendige, siden disse antas å kunne bli gjennomført betydelig raskere enn etableringen av en ny investeringskontrollov.

12.4.2 Sikkerhetsloven § 10-3

Som tidligere nevnt i punkt 9.3.4.2 gir sikkerhetsloven § 10-3 Kongen i statsråd mulighet til å stanse eller sette vilkår for gjennomføring av kjøp av en kvalifisert andel i en virksomhet som er underlagt sikkerhetsloven, hvis det er en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet.

Som vist til i punkt 9.3.3 etablerer prinsippene om de fire friheter i EØS-retten at Norge i utgangspunktet ikke kan ha regler som behandler grenseoverskridende bevegelser og transaksjoner mellom Norge og andre EØS-stater strengere enn rent nasjonale bevegelser og transaksjoner. Slik forskjellsbehandling vil anses som en restriksjon på den frie bevegeligheten over landegrensene. Det er likevel en mulighet for å treffe visse tiltak gjennom artikkel 33 og 123 i EØS-avtalen. I Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet (sikkerhetsloven) s. 152 sier departementet følgende om forholdet mellom sikkerhetslovens regler om eierskapskontroll og EØS-avtalens regler om etableringsfrihet etter artikkel 31 og fri bevegelse av kapital etter artikkel 40:

> «Stans av et erverv i en virksomhet vil i utgangspunktet være i strid med EØS-avtalens regler om fri etableringsrett og den frie bevegelighet av kapital, jf. EØS-avtalens artikkel 31 og 40. Imidlertid vil et inngrep bare gjøres i særlige tilfeller, hvor formålet med inngrepet ikke kan oppnås på en mindre inngripende måte. Det må videre være forholdsmessighet mellom den konkrete risiko for skadevirkning for nasjonale sikkerhetsinteresser og negative konsekvenser for de involverte aktørene. Departementet antar at artikkel 123, men også i enkelte tilfeller artikkel 33, da vil kunne hjemle inngripen.»

Om muligheten til inngrep sier Investeringskontrollutvalget at: *«Virkeområdet til artikkel 123 er sannsynligvis ganske snevert i praksis. Bestemmelsen kan trolig kun brukes når det er snakk om en investering i et foretak som opererer i forsvarssektoren. Videre inneholder bestemmelsen krav om at det må foreligge alvorlig indre uro, fare for krig mv., hvilket gjør bestemmelsen lite anvendelig i fredstid. Artikkel 33 kan være et mer dekkende unntak for tiltak av hensyn til nasjonal sikkerhet, men kun når det gjelder brudd på forpliktelsen om retten til fri etablering».*

Å ikke godkjenne erverv eller stille vilkår for ervervet med hjemmel for inngrepet i EØS-avtalen artikkel 33, innebærer en vesentlig lavere terskel – «nødvendig tiltak for å ivareta nasjonal sikkerhet».

Det er imidlertid ikke tilstrekkelig at reglene er begrunnet i sikkerhetshensyn etter EØS-avtalen artikkel 33 eller andre lovlige allmenne hensyn. EØS-rettens regler om de fire friheter stiller også minstekrav til hvordan lovgivningen skal utformes for å gi forvaltningen hjemmel til å pålegge private parter plikter. Ifølge Eriksen (2024)[150] setter EØS-rettens hjemmelskrav først og fremst krav til lovhjemlers presisjon på de områdene lovgivningen anses som restriksjoner på fri bevegelse av varer, personer, tjenester og kapital. Ved denne vurderingen vil det være avgjørende om reglene er tilstrekkelig transparente, slik at investorene, ESA, Kommisjonen og andre land i EØS kan få innblikk i hvordan investeringer vil kunne bli screenet.

Ifølge Eriksen (2024) er reglene om eierskapskontroll i sikkerhetsloven kapittel 10 upresise fordi det verken i lov eller forarbeider er angitt noen klare kriterier for vurdering av om investeringer skal godkjennes, utover at disse vurderingene skal være forholdsmessig. Han sier at det derfor i praksis vil *«være svært krevende for domstoler å kontrollere lovligheten av avgjørelser om å stanse eller sett vilkår for godkjenning av investeringer. Det er klart at det er mulig å formulere klarere og mer presise kriterier både i lov og forarbeider. En kunne for eksempel presisert at investeringer skal godkjennes med mindre visse vilkår er oppfylt. Sett i lys av EU- og EFTA-domstolens praksis antar jeg derfor at mangel på åpenhet om hvem som er underlagt reglene i kapittel 10 og mangel på presise retningslinjer for adgangen til nekte eller stille vilkår for erverv, kan medføre at reglene i sikkerhetsloven kapittel 10 går lenger enn det som er nødvendig i å begrense etableringsretten og kapitalfriheten, jf. EØS-avtalen artikkel 31 og 40, og at mekanismen i lovens kapittel 10 neppe kan forsvares etter EØS-avtalen artikkel 33 eller læren om allmenne hensyn».* Eriksens konklusjon er at det er betydelig risiko for at reglene i sikkerhetsloven kapittel 10 er i strid med EØS-avtalen artikkel 31 og 40, noe som innebærer at vedtak om stans av erverv og vedtak om vilkår for erverv, kan være ugyldige.

Også Investeringskontrollutvalget peker på problemer med uforutsigbarhet knyttet til bruken av sikkerhetsloven § 10-3 om investerings- og eierskapskontroll, og viser i rapportens punkt 13.7 til at: *«Både OECDs prinsipper og EUs minimumskrav til medlemslandenes regelverk legger vekt på at man skal ha mest mulig åpenhet og forutsigbarhet både rundt hvilke investeringer som er omfattet av regelverket, og hvordan saker skal behandles. Prinsippene i EU-forordningen og OECDs retningslinjer bygger på de grunnleggende prinsippene i det multilaterale handelsregelverket, se kapittel 9. Dette er prinsipper som Norge har sluttet seg til».*

Ekomsikkerhetsutvalget erkjenner at det eksisterer ulike syn på hvorvidt sikkerhetsloven § 10-3 er i tråd med EØS-avtalen.

På denne bakgrunn har utvalget følgende forslag til tiltak:

> **«Utvalget anbefaler at Justis- og beredskapsdepartementet klarlegger om bestemmelsen i sikkerhetsloven § 10-3 er i tråd med EØS-avtalen».**

[150] Utredning av rettslige rammer for kontroll med kritisk digital infrastruktur s. 42.

12.4.3 Sikkerhetslovens regler om virksomheter med «vesentlig betydning»

Reglene i sikkerhetsloven kapittel 10 gjelder bare virksomheter som er underlagt sikkerhetsloven etter § 1-3. Sikkerhetsloven § 2-5 omfatter enhver aktivitet som kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet, herunder erverv av eierandeler i en virksomhet. Bestemmelsen har derfor blitt brukt for å stanse erverv av eierandeler i virksomhet som ikke er underlagt sikkerhetsloven.

Per i dag er det ingen meldeplikt for erverv av eierandeler i selskaper med mindre disse er underlagt sikkerhetsloven. Derfor er staten selv nødt til å fange dette opp, og vurdere inngripen etter § 2-5 dersom oppkjøpet kan innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet.

Sikkerhetslovens bestemmelser om eierskapskontroll kan med hjemmel i § 1-3 annet ledd utvides til å gjelde virksomheter som et departement vurderer å ha *vesentlig* betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser – altså en lavere terskel enn for virksomheter som skal utpekes fordi de har *avgjørende* betydning. Å bruke dette mulighetsrommet til å utvide meldeplikten, vil gi departementet informasjon om viktige eierskapstransaksjoner og adgang til å bruke sikkerhetsloven kapittel 10, og dermed ikke måtte vurdere ervervet etter § 2-5 som er ment som en sikkerhetsventil. I praksis kan dette brukes til å oppnå en meldeplikt ved erverv av andeler i virksomheter, for eksempel de selskapene som samlet sett har evnen til å ivareta kritiske digitale kommunikasjonsfunksjoner.

En utpeking av slike virksomheter, vil i tillegg til å utvide meldeplikten og gi muligheten til å anvende sikkerhetsloven § 10-3, også skape større forutsigbarhet for selskaper, eiere og potensielle investorer, om at eierskapstransaksjoner vil bli underlagt screening. I dag må som nevnt en slik screening eventuelt skje med hjemmel i § 2-5, og det gir aktørene lite veiledning om når myndighetene kan komme til å ta i bruk bestemmelsen.

Utvalget mener derfor at muligheten til å utvide kretsen av virksomheter som kan underlegges meldeplikt og eierskapskontroll bør prioriteres. Dette vil gi tilgang på nødvendig informasjon om potensielt kontrollsvekkende transaksjoner, inngrepsmulighet dersom transaksjonene svekker nasjonal kontroll i kvalifisert grad samt gi berørte virksomheter større forutsigbarhet for at erverv blir underlagt kontroll sammenliknet med å benytte sikkerhetsloven § 2-5.

12.4.4 Forholdet mellom sikkerhetsloven § 2-5 og ekomregelverket

Utenlandske direkte investeringer gjennom nyetablering

Utenlandsk eierskap kan oppnås gjennom erverv av eierandeler i eksisterende norske selskaper som er i drift («brownfield investment»), men også gjennom at utenlandske eiere oppretter norske datterselskaper og bygger opp en virksomhet fra bunnen av («greenfield investment»/nyetablering). Sistnevnte typer selskaper kan på lengre sikt vokse organisk i form av sin konkurransekraft og komme til å utgjøre en vesentlig, kanskje dominerende, aktør på sitt område i det norske markedet.

Utvalget anser det hensiktsmessig at også slike etableringer bør omfattes av en investerings-screening på linje med erverv av eierandeler etter sikkerhetsloven kapittel 10. Etter Kommisjonens forslag til nytt regelverk om screening av utenlandske direkte investeringer, skal også greenfield-investeringer underlegges slik kontroll.

Etter ekomloven § 2-1 skal tilbyder av offentlig elektronisk kommunikasjonsnett og offentlig elektronisk kommunikasjonstjeneste registrere seg hos departementet før virksomheten starter opp. Tilsvarende plikt til registrering av datasentre følger av ekomloven § 3-7. Det betyr at dersom det foretas en greenfield-investering ved at det etableres en ny virksomhet i Norge, vil myndigheten bli kjent med etableringen ved oppstart av slik virksomhet.

Det følger av ekomloven § 3-5 (omtalt i punkt 9.3.5) at myndigheten kan nekte en tilbyder adgang til markedet både ved oppstart av virksomhet og ved løpende virksomhet. Som sikkerhetsloven § 2-5, er bestemmelsen ment å være en sikkerhetsventil for særlige tilfeller og terskelen for å nekte noen adgang til markedet vil være høy. Forholdet mellom de to bestemmelsene er for utvalget noe uklart, bortsett fra at ekomloven § 3-5 åpner for å nekte adgang til markedet på grunnlag av svekket sikkerhet ut over nasjonale sikkerhetsinteresser, for eksempel offentlig sikkerhet, helse eller andre særlige forhold. Utvalget mener at det er behov for at forholdet mellom de to bestemmelsene klarlegges, og at rekkevidden av inngrepsmuligheten etter sektorregelverket tydeliggjøres.

Salg av eiendeler eller endring av driftskonsepter

Utvalget legger til grunn at både salg av eiendeler/ressurser og ulike typer driftskonsepter som kan føre til en nedbygging og overføring til virksomhet kontrollert av utenlandske eierinteresser, er aktiviteter som, hvis de innebærer en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet, kan være omfattet av sikkerhetsloven § 2-5. Bestemmelsen er imidlertid ment å være en sikkerhetsventil der terskelen for å ta i bruk bestemmelsen er høy. Det er heller ingen generell meldeplikt for slike disposisjoner.

Når det gjelder utkontraktering vil ekomloven §§ 3-1 og 3-7 kunne anvendes hvis for eksempel utkontraktering av funksjoner knyttet til drift, IT-sikkerhetstjenester og nettverksovervåking, vil medføre at virksomheten ikke lenger har forsvarlig sikkerhet og beredskap. Utvalget er imidlertid usikker på i hvilken grad nasjonale sikkerhetsinteresser kan vektlegges i vurderingen av §§ 3-1 og 3-7. Også her mener utvalget at det er behov for en avklaring av forholdet mellom de sektorspesifikke bestemmelsene ekomloven og sikkerhetslovens bestemmelser.

På denne bakgrunn har utvalget følgende forslag til tiltak:

> **«Utvalget mener Digitaliserings- og forvaltningsdepartementet bør avklare om det sektorspesifikke regelverket er i stand til å ivareta situasjoner der man står overfor kontrollsvekkende aktivitet i ekomsektoren. I første omgang er det behov for å vurdere rekkevidden av bestemmelsene i ekomloven §§ 3-1, 3-5 og 3-7 opp mot sikkerhetsloven § 2-5.»**

”

Kapittelet belyser infrastrukturer som er nødvendige for digital kommunikasjon, men som ikke er underlagt norsk jurisdiksjon. Da blir internasjonalt samarbeid viktig.

Foto: Adobestock

13

Kritikalitet i infrastruktur som ligger utenfor norsk jurisdiksjon

13.1 Innledning

En viktig del av utvalgets mandat er å beskrive status for nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur. En viktig del av dette bildet er at flere digitale tjenester er tilstrekkelig kritiske til at en grad av nasjonal kontroll kunne være ønskelig, samtidig som de virksomhetene som leverer disse tjenestene ligger utenfor norske myndigheters kontroll og norsk jurisdiksjon. Felles for disse er at de er utviklet utenfor Norge, at de kan tilby sine tjenester globalt uten behov for nasjonal fysisk tilstedeværelse og at deres kritikalitet for norske samfunnsfunksjoner har kommet gradvis og over tid.

Dette kapittelet går gjennom noen slike sentrale tjenester, og for hver av dem diskuterer utvalget både tjenestens kritikalitet og hvilke muligheter som foreligger for nasjonal kontroll.

13.2 IP-adresser

IP-adresser er den sentrale identifikatoren for internett og som muliggjør at datapakker kan flyte fra en avsendermaskin til en mottakermaskin. For å få det globale internettet til å fungere har det vært avgjørende at det eksisterer en internasjonal enighet om adressesystemet, og om hvilke deler av nettet som benytter hvilke adresser. Denne enigheten er organisert gjennom Internet Corporation for Assignet Names and Numbers (ICANN), som er en non-profit organisasjon som ligger under amerikansk jurisdiksjon. ICANN delegerer ansvaret til fem regionale internettregistre. Registeret

som dekker Europa, Midtøsten og deler av Sentral-Asia heter RIPE NCC[151]. RIPE NCC er en medlemsstyrt non-profit organisasjon, den er basert i Nederland og den ligger under nederlandsk jurisdiksjon.

RIPE NCC tilordner adresser til lokale internettregistrarer (gjerne kalt LIR) i Norge. Norge er i en god situasjon på dette området ved at vi har et godt antall av lokale internettregistrarer, og et tilstrekkelig antall IP-adresser til rådighet.

En standard for validering av IP-adresser er under rask utbredelse. Denne standarden kalles RPKI ROV[152], og hensikten med den er å gjøre internett sikrere ved at ingen kan påstå å eie IP-adresser som er i bruk hos andre. Denne utviklingen representerer en betydelig styrking av den strukturelle sikkerheten i internett. Samtidig representerer den en potensiell utfordring ved at standarden gir RIPE NCC verktøy som er rapportert å kunne invalidere IP-adresser som Norge er avhengig av.[153] Medlemmene i RIPE NCC er organisasjoner og selskaper som benytter IP-adresser og den norske staten har således ikke ingen naturlig plass som medlem i denne organisasjonen. Nkom er medlem i kraft av sitt eierskap til IP-ressurser. RIPE har imidlertid etablert en struktur for dialog med myndigheter og regulatører i sin region ved å jevnlig invitere disse til rundebordskonferanser.

13.3 Domenenavn

Domenenavn er sentrale ressurser for alle anvendelser av internett. I motsetning til IP-adresser er domenenavn lett leselige for mennesker, og de benyttes derfor i alle sammenhenger der mennesker er ment å interagere direkte med internettets struktur. E-postadresser og web-adresser er begge eksempler på bruk av domenenavn til et slikt formål. Domenenavn benyttes også til en rekke andre formål, og de er av avgjørende betydning for internettets funksjon både i Norge og i resten av verden.

DNS[154] er et globalt og standardisert system som oversetter domenenavn til IP-adresser. Dette systemet aktiveres ved enhver bruk av internett, og det er således en helt sentral ressurs. Systemet har en svært distribuert organisering, både hva gjelder teknisk implementering og hva gjelder beslutninger om hvem som har bruksrett til hvert enkelt domenenavn. Registeret for domenenavnene «.no» (Norge), «.sj» (Svalbard og Jan Mayen) og «.bv» (Bouvetøya) drives av Norid[155], som er et direkte eid selskap under DFD. ICANN har tildelt Norid kompetanse til å forvalte .no-domenet. ICANN har således innflytelse over både IP-adresser og domenenavn, og beslutninger som tas der har potensielt stor betydning i Norge. Gjennom Nkom spiller Norge en aktiv rolle i arbeidet i ICANN, og det er utvalgets syn at denne innsatsen er viktig for å ivareta norske interesser knyttet til domenenavn og IP-adresser. Arbeidet bør derfor fortsette å få prioritet.

[151] Forkortelsen står for *Réseaux IP Européens Network Coordination Centre.*

[152] Akronymene står for *Resource Public Key Infrastructure, Route Origin Validation*.

[153] Cooper, D., Heilman, E., Brogle, K., Reyzin, L., & Goldberg, S. (2013, November). On the risk of misbehaving RPKI authorities. In Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks (pp. 1-7).

[154] Domain Name System

[155] Det er så langt kun åpnet for registreringer under .no

Den tekniske løsningen for DNS har en kjerne bestående av 13 rot-servere. Det er utpekt totalt tolv operatører av rot-servere i verden, og hver av disse opererer mange servere verden over. Ifølge nettstedet http://root-servers.org har sju av disse en fysisk tilstedeværelse i Norge i form av en server som leverer den nødvendige tjenesten fra norsk territorium.[156] Ingen av dem er styrt av norske virksomheter, men det er verdt å merke seg at én av de tolv utpekte rot-serveroperatører er svenske Netnod.

Styring av domenene «.no», «.sj» og «.bv» gjøres som nevnt over av Norid. Ut over dette har vi som nasjon svært begrenset kontroll med utviklingen av DNS, da verken beslutningen om at Norge skal kontrollere disse domenene eller driften av rot-servere, gjøres av norske virksomheter. Den distribuerte naturen til DNS-systemet, og det faktum at den sentrale styringen av systemet gjøres fra land Norge har sikkerhetspolitisk samarbeid med, gjør at situasjonen fremstår som lite kritisk.

En større bekymring er knyttet til hvordan norske virksomheter og personer benytter DNS-systemet. Alt utstyr vil ha IP-adressen til den DNS-tjenesten de skal benytte kodet inn i seg. Kodingen av denne IP-adressen gjøres som regel av det nettverket som utstyret er koblet opp mot, og det foreligger ingen samlet oversikt over hvilke DNS-tjenester, norske eller utenlandske, som benyttes i norske nettverk.

Bruk av DNS-tjenere som ligger utenfor landets grenser har to sider ved seg som grenser opp mot nasjonal kontroll. Den første er knyttet til tilgjengelighet, da bortfall av DNS-tjenester vil få de aller fleste informasjonssystemer til å slutte å virke. Den andre er knyttet til faren for misbruk av informasjon om norske forhold som en lekkasje av DNS-oppslag vil kunne medføre. Utvalget mener derfor at en definert grad av nasjonal autonomi knyttet til DNS bør være en del av målbildet for nasjonal kontroll med kritisk digital infrastruktur. Målbildet bør være basert på et faktagrunnlag knyttet til hvordan DNS-systemet benyttes av norske virksomheter.

13.4 Digitale sertifikater

En sentral del av sikkerhetsregimet på internett består av å validere identiteten til enheter, til programkode og til dokumenter, samt å kryptere informasjon slik at den ikke kan leses av uvedkommende. Slik validering foregår i praksis ved at en sertifikatautoritet (CA) opererer som en tiltrodd tredjepart, og utsteder digitale sertifikater. Sertifikatene benyttes blant annet til følgende:

- For autentisering og kryptering av informasjon som flyter mellom to maskiner.
- Som kodesigneringssertifikater for digital signering av programvare.
- Som grunnlag for kryptering og autentisering av e-post.
- Som grunnlag for elektronisk signatur av dokumenter.

Sertifikatautoritetene har en struktur av tillit seg imellom. Denne strukturen er forankret i et antall rot-sertifikatautoriteter som antas å ha bred, eller endog global tillit. En slik rot-sertifikatautoritet har således betydelig myndighet til å validere, men også invalidere en stor mengde sertifikater. En invalidering av mange sertifikater vil over noen tid få alvorlige konsekvenser for de aller fleste tjenestene som nå går over internett. Hvor lang tid som

[156] Seks av disse ligger i Oslo, og en ligger i Trondheim

vil gå fra en invalidering til konsekvensene viser seg, vil variere fra sertifikat til sertifikat, og det vil avhenge av syklusen for fornyelse av sertifikatene. Sertifikater fornyes typisk hvert kvartal eller hvert år. Enkeltsertifikat kan også invalideres direkte ved å inkluderes i «certificate revocation lists» av sertifikatautoriteten, noe som kan stanse en digital tjeneste umiddelbart.

Det finnes flere norske sertifikatutstedere som er knyttet opp mot utenlandske rot-sertifikataktører. Buypass er den eneste rot-sertifikataktøren som er lokalisert i Norge og som kan sies å ha global tillit. Deres sertifikater er anerkjent og inkludert i rotsertifikat-programmene til både Apple, Google og Microsoft. Buypass er eid av Total Specific Solutions som har hovedkontor i Canada.

Dersom man ønsker nasjonal kontroll med en sertifikatstruktur, må den være forankret i en grad av nasjonal kontroll med en rotsertifikataktør. I EU har det i lengre tid vært oppmerksomhet rundt utfordringene knyttet til tjenester for digitale sertifikater. I april 2024 ble forordningen European Digital Identity Framework (eIDAS 2.0)[157] vedtatt i EU, som blant annet gjør det lettere for nasjonale myndigheter å pålegge leverandører av nettlesere å godkjenne nasjonale rot-sertifikater.

Utvalget mener at det bør skaffes oversikt over graden av nasjonal kontroll med de sertifikat-tjenestene som er i faktisk bruk i Norge, for på den måten å ha et godt beslutningsgrunnlag for hvorvidt det er behov for en nasjonal rot-sertifikattjeneste.

13.5 Nøyaktig tid

Sentrale deler av landets grunnleggende nasjonale funksjoner er avhengig av tilgang til en nøyaktig og synkronisert tidstjeneste. Behovet er spesielt uttalt i mobilnettene og i kraftdistribusjonen, der ny teknologi og nye bruksmønstre stiller helt andre krav til nøyaktig og synkronisert tidsangivelse enn tidligere.

Aktørene løser i dag behovet for nøyaktig tid på en av to måter. Telenor og Statkraft har etablert – eller er i ferd med å etablere – sine egne infrastrukturer for tidstjenester, med bakkebasert distribusjon av nøyaktig tid. Andre aktører med behov for tilgang til nøyaktig tid henter fra satellitt ved bruk av mottakere for satellittbaserte navigasjonssystemer (ofte forkortet til GNSS). GPS-systemet som drives av The United States Space Force er det mest kjente av disse. Alternative navigasjonssystemer som kan tilby eksakt tid er GLONASS (Russland), Beidou (Kina) and Galileo (EU).

Telenor og Statkraft sine løsninger for distribusjon av tidstjenester kan sies å ha en høy grad av nasjonal kontroll over seg. I den utstrekning de også gjør disse tidstjenestene tilgjengelig for andre aktører kan det også sies at effekten av denne nasjonale kontrollen går ut over grensene for Telenor og Statkraft sine egne virksomheter. Det er imidlertid verdt å merke seg at Norge ikke har noen nasjonal kontroll med de tidstjenestene som leveres fra satellitt. De installasjonene i Norge som henter nøyaktig tid fra satellittbaserte navigasjonstjenester har derfor en avhengighet til tjenester som ligger utenfor nasjonal kontroll. I noen tilfeller vil denne avhengigheten være av avgjørende karakter.

[157] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

Problemstillinger knyttet til nøyaktig tid er omtalt i Nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse[158]. I denne står det at Regjeringen vil «vurdere evnen til å opprettholde nøyaktig tid i digitale nett og om det er hensiktsmessig å innføre nasjonale krav til hvor lenge slike nett bør kunne fungere ved svikt i GNSS».

Det finnes i dag ingen samlet nasjonal infrastruktur for tidstjenester. Denne mangelen har vært behandlet av Totalberedskapskommisjonen[159] som skriver at «*... svært mange samfunnsfunksjoner er avhengige av nøyaktig tid fra satellitter som er utenfor nasjonal kontroll. En nasjonal tidstjeneste som sikrer nasjonal egenevne med tanke på nøyaktig tid, vil være et viktig virkemiddel for å redusere denne sårbarheten*». Videre anbefaler NSM i sitt sikkerhetsfaglige råd fra 2023 at det bør etableres en nasjonal tidstjeneste. I den samme rapporten påpekes det at Sverige allerede har etablert en statlig kontrollert tjeneste for distribusjon av nøyaktig tid. Utvalget støtter Totalberedskapskommisjonen sitt syn om at en nasjonal tidstjeneste vil være et viktig virkemiddel for å redusere sårbarhet.

Utvalget er kjent med at DFD har gitt Nkom og Justervesenet i oppdrag å kartlegge behovet for, og utrede løsninger for en nasjonal infrastruktur for distribusjon av presis tid/klokkesignal i Norge.

I den sammenheng bør det vurderes i hvilken grad den nasjonale tjenesten kan bygge på, eller dra nytte av infrastrukturer som allerede er etablert av virksomheter som staten har eierskap i. Videre bør det vurderes om det norske behovet kan dekkes gjennom et samarbeid med våre nordiske naboland.

13.6 Skytjenester

Noen få superskalære sky-leverandører – Google, Amazon og Microsoft – kontrollerer store deler av markedet for skytjenester. Felles for disse er at de er børsnoterte kommersielle selskaper med hovedkontor i USA. Kun Microsoft har foreløpig etablert skytjenester i Norge med et datasenter på Vestlandet og et på Østlandet, mens Google har startet bygging av et stort datasenter utenfor Skien. Ingen skytjenesteleverandør har foreløpig et komplett tjenestetilbud levert fra datasentre i Norge. Det betyr at norske kunder som ønsker å benytte de standardiserte tjenestene fra disse store leverandører i mange tilfeller er henvist til å legge sky-implementasjonen sin til utlandet.

Plassering av skytjenester utenfor Norge representerer ikke nødvendigvis en svekkelse av nasjonal sikkerhet. Nasjonal kontroll kan gjenopprettes avtalemessig gjennom en kontraktsposisjon som kunde, noe som gir god kontroll langt opp i krisespennet så lenge tjenesten er kontrollert fra et land Norge har sikkerhetspolitisk samarbeid med. I de helt øverste delene av krisespennet kan det også være et poeng i seg selv å produsere tjenester utenfor landets grenser.

Det er imidlertid to sider av denne saken som fortjener oppmerksomhet. Den ene er at skytjenester plassert utenfor landet kan gi tapt nasjonal kontroll over informasjon

[158] «På rett sted til rett tid», Samferdselsdepartementet, 2018.

[159] NOU 2023: 17

om norske individer og norske forhold. Denne problemstillingen er grundig belyst EU-domstolen gjennom to rettssaker.[160]

Det andre forholdet som er verdt å reflektere over er om totaliteten av tjenester som er lagt til utlandet samlet sett gir et uønsket tap av nasjonal kontroll. Merk at dette også gjelder såkalte «mikrotjenester» som f.eks. autentisering, lagring, databaser, osv. som ofte benyttes i moderne software-utvikling, og som gjør det vanskelig for tjenesteyter å holde oversikt over avhengigheter og verdikjeder. Det bør settes i gang et arbeid for å holde oversikt over slik utilsiktet tap av nasjonal kontroll.

Justissektoren har gjennomført et konseptvalgarbeid for en nasjonal skytjeneste for ugradert, skjermingsverdig informasjon og andre beskyttelsesverdige data. I totalberedskapsmeldingen sier regjeringen at de vil planlegge en nasjonal skytjeneste for å sikre økt nasjonal kontroll med kritisk digital infrastruktur, viktige samfunnsfunksjoner og digitale verdier, og de har valgt et konsept der det inngås avtale med én eller noen få leverandører som skal utvikle, drifte og forvalte en nasjonal skytjeneste. En nasjonal skytjeneste vil inngå i et målbilde for nasjonal kontroll med datasenterinfrastruktur, herunder nasjonale kapasitetsmål, geografisk spredning, eventuelle fortifikatoriske sikringsbehov og mål for beredskapskapasitet i utlandet.

> **«Utvalget ser behov for etablering av nasjonal skyløsning ut fra behovet for nasjonal kontroll, og mener at dette arbeidet bør gis høy prioritet. Det anbefales at Justis- og beredskapsdepartementet tydeliggjør videre ambisjonsnivå og plan, og gjør nødvendige midler tilgjengelig for arbeidet.»**

13.7 Internettsamtrafikk

For at internett i Norge skal fungere må de norske nettstrukturene utveksle trafikk med nettstrukturer i utlandet. Mesteparten av internettrafikken som går ut og inn i Norge formidles gjennom de to internasjonale transittleverandørene Arelion og Lumen, samt de større norske internettilbyderne Telenor, Telia, GlobalConnect og Altibox.[161]

Hverken Lumen eller Arelion har norsk eierskap, og virksomheten de driver fremstår som vanskelig tilgjengelig for norsk jurisdiksjon. Samtidig vil slike selskaper være helt sentrale aktører i verdikjeden til internettjenester som ble beskrevet i forrige avsnitt. Utvalget ser det som viktig at norske myndigheter holder oversikt over vår avhengighet av enkeltleverandører innen Internettsamtrafikk, og legger til rette for en grad av diversitet i leverandørbildet som sikrer at norsk internettsamtrafikk med utlandet er robust i hele krisespennet.

[160] Se Schrems I (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362) og Schrems II (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311&qid=1738086589197)

[161] «Internett i Norge – Årsrapport 2023». Nasjonal kommunikasjonsmyndighet.

13.8 Tjenester for kommunikasjon med befolkningen

I diskusjonen om kritisk digital infrastruktur har mobiltelefon som plattform for å kommunisere med- og mellom borgerne en sentral plass. Dette er gjenspeilet i at norske nummerserier som grunnlag for tale- og meldingstjenester er definert som en grunnleggende nasjonal funksjon etter sikkerhetsloven. Viktigheten av tale- og meldingstjenester er tilsvarende viktig utenfor sikkerhetslovens virkeområde, da det knapt er mulig å se for seg en virksomhet av betydning som ikke har en avhengighet til slike tjenester.

Det er imidlertid omfattende internasjonal kommersiell interesse i å tilby alternative meldings- og taletjenester. Eksempler på slike alternative tjenester som er mye i bruk er Instagram, Messenger, Snapchat, TikTok, FaceTime/iMessage, Skype, Google Meet og Teams. Felles for disse tjenestene er at de ikke ligger under noen form for nasjonal kontroll, at de ikke baserer seg på norske nummerserier og at de har stor utbredelse blant nordmenn.

Til tross for at internasjonale tjenester i noen grad ser ut til å fortrenge tale- og meldingstjenester basert på norske nummerserier, ser ikke utvalget at det er noen umiddelbare behov for tiltak på dette området. Grunnen til dette er at tale- og meldingstjenester basert på norske nummerserier fortsatt er tilgjengelige på alle mobiltelefoner som har utbredelse i Norge, og det er etablert systemer for masseutsending av nødvarsler i samarbeid med mobiloperatørene.[162]

13.9 Lavbanesatellitter

Det gjøres for tiden store investeringer i systemer av lavbanesatellitter for internett-tilgang. De mest kjente systemene er Starlink som opereres av SpaceX[163], og OneWeb som opereres av Eutelsat[164], men det finnes flere andre kommersielle systemer som er i drift. EU utvikler en europeisk konstellasjon av lavbanesatellitter ved navn Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²), og som planlegges å være fullt operativ i 2027.[165] Tilgang til IRIS er ikke omfattet av EØS avtalen. Programmet anses være av betydning for norsk samfunnssikkerhet og beredskap, Forsvaret, samt for utviklingen av norsk romindustri, og utvalget viser til at regjeringen arbeider for å muliggjøre norsk deltakelse i programmet.[166] Det pågår ingen utvikling av lavbanesatellitt-konstellasjoner som kan sies å være under noen form for nasjonal norsk kontroll.

Lavbanesatellitter har foreløpig svært liten utbredelse som plattform for nett-tilgang i Norge. Potensialet i teknologien er imidlertid stort. Spesielt vil den nærmest fullstendige flatedekningen et system av lavbanesatellitter gir samt den høye båndbredden som har blitt demonstrert gjøre slik teknologi til et attraktivt alternativ for nett-tilgang i områder

[162] https://www.regjeringen.no/no/aktuelt/nytt-system-for-nodvarsel-til-befolkningen-er-etablert/id2958586/

[163] https://www.starlink.com

[164] https://oneweb.net/about-us

[165] https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

[166] Regjeringens arbeidsprogram for EU- og EØS-saker 2024-2025 s. 17.

som er kostbare å nå med fiber. Lavbanesatellitter vil også kunne spille en betydelig rolle som backup-løsning i situasjoner der bakkebasert nettilgang har falt bort.

Utvalget er forsiktige med å spå i hvilken grad lavbanesatellitter vil være en disruptiv kraft i det norske telekom-markedet. Vi observerer likevel at de investeringene som gjøres i slike infrastrukturer er svært omfattende, og disse investeringene gjøres med en forventning om inntjening også fra norske brukere. Utvalget anbefaler derfor norske myndigheter om å følge utviklingen nøye, og at det søkes å spille en rolle i det pågående europeiske initiativet. Basert på ovennevnte støtter utvalget regjeringens mål om aktiv deltakelse i IRIS².

13.10 Oppsummering

Vi har i dette kapittelet belyst flere digitale infrastrukturer som er kritisk viktige for digital kommunikasjon, men som ikke er underlagt norsk jurisdiksjon. Disse infrastrukturene er svært mangeartede, og de tiltakene vi foreslår vil av den grunn falle i flere kategorier.

I diskusjonene knyttet til nasjonal sky og til nøyaktig tid er det både teknisk og økonomisk gjennomførbart å lage nasjonalt kontrollerte alternativer til de utenlandske infrastrukturene som nå benyttes. Slike løsninger vil kunne gi tilfredsstillende grad av handlefrihet ved at de gjør de virkemidlene som er beskrevet i kapittel 9 virksomme på områder der de tidligere ikke har hatt effekt.

Våre forslag om aktiv deltakelse i ICANN, samt å søke norsk deltakelse i IRIS² er av en annen karakter. Disse forslagene vil i noen grad sørge for at norske behov har plass i de vurderingene som skal gjøres på sentrale teknologiområder, og som vil kunne få effekt for Norge.

Den siste kategorien av tiltak er utvikling av faktagrunnlag knyttet til våre internasjonale avhengigheter. Institusjoner og individers avhengighet av skytjenester, mikrotjenester, DNS-servere, og digitale sertifikater utenfor landets grenser er i liten grad regulert. Det er en fare for at de samlet sett utgjør et betydelig tap av nasjonal kontroll både over systemers integritet og over lekkasje av informasjon om norske forhold. Likeledes er alle disse tjenenestene avhengig av velfungerende strukturer for internettsamtrafikk for å kunne fungere.

«**Digitaliserings- og forvaltningsdepartementet bør vedlikeholde et faktagrunnlag knyttet til nasjonal avhengighet av utenlandske innsatsfaktorer, herunder mikrotjenester, DNS-tjenere, sertifikattjenester, og internettsamtrafikk. Dette faktagrunnlaget bør danne basis for utvikling og vedlikehold av målbilde og virkemidler for nasjonal kontroll, og i den sammenheng vår avhengighet til infrastruktur som ligger utenfor norsk jurisdiksjon.»**

Foto: Gunnstein Myhre (Nkom)

14

Økonomiske og administrative konsekvenser

Utvalget legger i denne rapporten fram en rekke konkrete forslag for å øke myndighetenes evne til å styrke nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur, som vil få administrative og økonomiske konsekvenser for både myndigheter og virksomheter. De økonomiske og administrative konsekvensene er imidlertid usikre.

Enkelte av utvalgets anbefalinger som

- at alle myndigheter som har sektoransvar etter sikkerhetsloven, gis tilgang til opplysninger fra registeret over reelle rettighetshavere,
- at der det er finnes relevant EU-regelverk, sørger for at dette regelverket gjennomføres i Norge og i så nær tid som mulig med tilsvarende regulering i EU, og
- at der statlig eierskap er begrunnet i hensynet til samfunnssikkerhet og beredskap, bør være tydeligere hvordan det hensynet veies mot hensynet til avkastning, andre aksjonærer og for eksempel statsstøtteregler,

er anbefalinger som utvalget mener vil ligge under ulike departementers ordinære oppgaver. Utvalget mener disse oppgavene bør prioriteres, men vil etter utvalgets syn ikke medføre nevneverdig økning av administrative eller økonomiske kostnader.

Ekomsikkerhetsutvalget foreslår som et utgangspunkt at DFD bør definere og vedlikeholde en helhetlig oversikt over kritisk digital kommunikasjonsinfrastruktur og selskapene som eier denne Til dette arbeidet kreves ressurser. Det er grunn til å anta at det ved etableringen av en slik oversikt vil være behov for særlige ressurser både knyttet til å definere kritisk digital kommunikasjonsinfrastruktur og identifisere selskapene som eier den. I tillegg er det behov for ressurser som kan sikre tilstrekkelig beskyttelse av informasjonen både når det gjelder oppbevaring og behandling av den. For at denne oversikten skal ha verdi over tid, er det nødvendig at det også gis tilstrekkelige ressurser

for å vedlikeholde den. Departementet har allerede i dag plikt etter sikkerhetsloven til å utpeke virksomheter som har infrastruktur som har avgjørende eller vesentlig betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser. Utvalget antar at en utvidelse til å kartlegge infrastrukturer og virksomheter som anses samfunnskritiske og relevante i forhold til nasjonal kontroll, men som ikke er så kritiske at de skal utpekes etter reglene i sikkerhetsloven, vil medføre et ikke ubetydelig behov for ytterligere ressurser. Fordi departementet ennå ikke har identifisert virksomheter med vesentlig betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser, er det vanskelig å anslå omfanget av gjenstående kartlegging og konkretisere de årlige økte kostnadene.

Utvalget foreslår videre en strukturert metode for å etablere et målbilde med konkrete styringsevner og handlefriheter staten bør ha for å ivareta nasjonal kontroll av kritisk digital kommunikasjonsinfrastruktur. Når målbildet er definert, må det gjennomføres en analyse av aktuelle virkemidler som er nødvendig for å nå målbildet, for å avklare om de virkemidlene som finnes er tilstrekkelige. Arbeidet både med å etablere og vedlikeholde et slikt målbilde og å avklare om og eventuelt sikre at man har nødvendige virkemidler, vil åpenbart påføre kostnader for myndighetene. Utvalget finner det vanskelig å kvantifisere kostnadene fordi det ligger utenfor utvalgets mandat å definere disse målbildene og har kun foreslått en metodikk som kan anvendes. Samtidig vil utvalget peke på at når det etableres og vedlikeholdes et målbilde og gjennomføres gapanalyser av målbildet og virkemidler, må det være et mål at dette arbeidet blir en integrert del av det øvrige forvaltningsarbeidet for å ivareta nasjonal kontroll av kritisk digital kommunikasjonsinfrastruktur, og at det bygges videre på dette i arbeidet med strategier, handlingsplaner og regelverksarbeid. Målet er at et etablert målbilde vil forenkle videre arbeid med å ivareta nasjonal kontroll av kritisk digital infrastruktur, og dermed redusere ressursbehovet i slike prosesser.

Utvalget mener at kontrollomfanget knyttet til økonomiske sikkerhetstruende aktivitet må utvides sammenliknet med i dag både når det gjelder type sikkerhetstruende aktivitet og kretsen av virksomheter som har kritisk digital kommunikasjonsinfrastruktur. Utvalget viser i denne sammenheng til at regjeringen i Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen* punkt 8.2 mener det er behov for å videreutvikle dagens ordning for håndtering av potensielt sikkerhetstruende utenlandske investeringer i virksomheter som ikke er underlagt sikkerhetsloven, og at det er igangsatt et arbeid for å utarbeide forslag til en ny lov for kontroll av utenlandske investeringer. Etter utvalgets syn bør gjennomføringen av de nedenfor nevnte vurderinger, kartlegginger og avklaringer, bli en naturlig del av det arbeidet regjeringen har startet:

- vurdere om sektorregelverket i tilstrekkelig grad sikrer tidlig informasjon om kontrollsvekkende virksomhet fra de selskapene som er eier av kritisk digital infrastruktur.
- ved utarbeidelse av ny lov for kontroll av utenlandske investeringer se hen til EUs nye regelverk om screening av utenlandske direkte investeringer, uavhengig av om regelverket anses EØS-relevant.
- dersom det opprettes en investeringskontrollmyndighet, sikre at sektorspesifikk fagkompetanse blir tilgjengeliggjort for en slik etat.
- klarlegge om bestemmelsen i sikkerhetsloven § 10-3 er i tråd med EØS-avtalen.
- avklare om det sektorspesifikke regelverket er i stand til å ivareta situasjoner der man står overfor kontrollsvekkende aktivitet i ekomsektoren. I første omgang er det behov for å vurdere rekkevidden av bestemmelsene i ekomloven §§ 3-1, 3-5 og 3-7 opp mot sikkerhetsloven § 2-5.

Siden utvalget ikke tar konkret stilling til hvordan en ny ordning med kontroll av utenlandske investeringer skal utformes, men viser til at det er behov for å utvide kontrollen av økonomisk aktivitet samt at regjeringen må se hen til det arbeidet med et nytt screeningregelverk som er satt i gang i EU, har ikke utvalget grunnlag for å konkretisere hvilke økte kostnader dette vil medføre verken for virksomhetene eller myndighetene. Det er likevel klart at en bredere kontroll av økonomisk aktivitet vil gi flere transaksjoner som skal kontrolleres, og dermed økte kostnader både for virksomhetene og for myndighetene. For myndighetene vil de økte kostnadene særlig være knyttet til større veiledningsbehov overfor investorer om regelverk og prosedyrer for meldepliktige saker, økte kostnader knyttet til saksbehandling av meldingene, samt økte kostnader med oppfølging særlig av vedtak der det er stilt vilkår for at transaksjonen kan gjennomføres. For næringslivet vil økte kostnader følge av at flere transaksjoner skal meldes og gjennomgå investeringskontroll, samt knyttet til tidstapet fra melding er sendt til myndighetene har truffet en beslutning, og det blir klart om en transaksjon kan gjennomføre eller ikke.

Utvalget har foreslått et arbeid med å etablere et faktagrunnlag knyttet til avhengighet av internasjonale infrastrukturer som mikrotjenester, DNS-tjenere, sertifikattjenester og internettsamtrafikk.

Dette er et tiltak av vesentlig betydning for å holde oversikt over hvilke land og aktører som har kontroll over kritisk digital infrastruktur som ligger utenfor norsk jurisdiksjon. Kostnadene ved å opprette og vedlikeholde et slikt faktagrunnlag vil være avhengig de behovene som fremkommer under utarbeidelsen av et målbilde, og av den grunn er det ikke mulig å tallfeste kostnadene. Utvalget er imidlertid ikke kjent med at det foregår vesentlig arbeid på dette området fra før, og man må forvente at en meningsfull dimensjonering og gjennomføring av dette tiltaket vil kreve tilleggsbevilgninger, og i noen grad også oppbygging av teknisk ekspertise. Utvalget bemerker at flere nærliggende land står overfor samme utfordring, og at et internasjonalt samarbeid om dette fremstår som en mulighet som også vil kunne påvirke kostnadsbildet.

Foto: Anders Martinsen (Nkom)

15

Referanseliste

Aftenposten 2023, https://www.aftenposten.no/verden/i/zE3RRq/starlink-systemet-gir-elon-musk-stor-makt-det-skaper-bekymring

ANALYSIS Perspectives on the Economic Effects of FDI and Investment Screening (2022), https://www.kommerskollegium.se/globalassets/publikationer/rapporter/2022/perspectives-on-the-economic-effects-of-fdi-and-investment-screening.pdf

A New European Commission Proposal on Foreign Direct Investment Screening: Towards Greater Harmonization? (2024), Crowell & Moring LLP, https://www.crowell.com/en/insights/client-alerts/a-new-european-commission-proposal-on-foreign-direct-investment-screening-towards-greater-harmonization

Atlantic Cable Maintenance and Repair Agreement (ACMA), https://www.acma2017.com/

BEREC Report (2023) on the impact of Artificial Intelligence (AI) solutions in the telecommunications sector on regulation, https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-the-impact-of-artificial-intelligence-ai-solutions-in-the-telecommunications-sector-on-regulation

BEREC Report (2024) on Cloud and Edge Computing Services, https://www.berec.europa.eu/en/all-documents/berec/reports/berec-report-on-cloud-and-edge-computing-services

Cai, D., og J. Li (2019) «To favor more or less? Corporate lobbying over preferential treatment to state-owned enterprises,» *Journal of Regulatory Economics* 55, 334–57

Cooper, D., Heilman, E., Brogle, K., Reyzin, L., & Goldberg, S. (2013, November). On the risk of misbehaving RPKI authorities. In Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks (pp. 1-7)

Datasenterindustrien i Norge 2023-2024, Rapport Norsk datasenterindustri, https://static1.squarespace.com/static/6129463e215bea534c574c7f/t/65a92c45d4a60f02b227271f/1705585734796/Datasenterindustrien+i+Norge+2023-2024.pdf

Diesen, Karlsen, Kosiander, Løvik, Nyhamar (2024), Erfaringer fra krigen i Ukraina – læringspunkter etter tusen dager med krig, FFI-rapport 24/01299 https://www.ffi.no/publikasjoner/arkiv/erfaringer-fra-krigen-i-ukraina-laeringspunkter-etter-tusen-dager-med-krig

Digi.no (2024), https://www.digi.no/artikler/starlink-vil-levere-1-gbit-s-fra-satellittene/551895

Digi.no (2024), https://www.digi.no/artikler/nsm-etter-crowdstrike-still-kritiske-sporsmal-om-programvareutviklingen/549154

e-Estonia (2019), https://e-estonia.com/data-embassy-the-digital-continuity-of-a-state/

Ekominfrastruktur i Nordland Regional risiko- og sårbarhetsanalyse for Nordland (2023), Nkom, file:///C:/Users/DFD1112/Downloads/Risiko%20og%20s%C3%A5rbarhetsanalyse%20for%20Nordland%20-%20Offentlig%20rapport.pdf

Ekominfrastruktur i Trøndelag Regional risiko- og sårbarhetsvurdering for Trøndelag (2024), Nkom, https://www.regjeringen.no/contentassets/4b9d05c6dd134d8aa67dfbe576605a45/off_rapport_sarbarhetsanalyse_for_trondelag_2024-02-05.pdf

eidsiva.no, https://www.eidsiva.no/om-eidsiva/eiere/

erhvervsstyrelsen.dk, https://erhvervsstyrelsen.dk/vejledning-aktiviteter-omfattet-af-investeringsscreeningsloven

(EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (NIS-direktivet), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

(EU) 2018/151 av 30. januar 2018 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2016/1148 med hensyn til ytterligere spesifisering av de elementene som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer, og av parametrene for å avgjøre om en hendelse har en betydelig innvirkning, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0151

(EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions cybersikkerhetsbyrå), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

(EU) 2019/452 av 19. mars 2019 om kontroll av utenlandske direkteinvesteringer, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452

(EU) 2021/694 av 29. april 2021 om opprettelse av programmet for et digitalt Europa, og om oppheving av beslutning (EU) 2015/2240, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0694

(EU) 2022/2555 av 14. desember 2022 om tiltak for å sikre et høyt felles nivå for sikkerhet i nett- og informasjonssystemer i hele Unionen og om oppheving av direktiv (EU) 2016/1148 [NIS2], https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

Europakommisjonen, https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Europakommisjonen, https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

Europakommisjonen, WHITE PAPER How to master Europe's digital infrastructure needs? (2024). White_Paper__Ho_to_master_Europes_digital_infrastructure_needs_CkoePennGJi1hpdkuARxMGuH5s_102533.pdf

Europakommisjonen, The future of European competitiveness (2024), https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf

EU – Security and Defence Partnership between the European Union and Norway, https://www.regjeringen.no/contentassets/abc084fe921e403791ddb505622ba365/eu-norway-security-and-defence-partnership.pdf

Felles redegjørelse NSM og Nkom, https://www.regjeringen.no/contentassets/17dba73e91354368aad3d53d600a18b0/tilsyn-med-nodnett---felles-redegjorelse-nsm-nkom.pdf

Finnish government – breakdown of state ownership, https://valtioneuvosto.fi/en/government-ownership-steering/breakdown

Fokus 2024, Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer, https://www.etterretningstjenesten.no/publikasjoner/fokus/Fokus24_innhold

Fremtidens digitale Norge, Nasjonal digitaliseringsstrategi 2024-2030, Digitaliserings- og forvaltningsdepartementet (2024), https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf

Gerbl, M., McIvor, R., & Humphreys, P. (2016). Making the business process outsourcing decision: why distance matters. International Journal of Operations & Production Management, 36(9), 1037-1064

Helsedirektoratet, https://www.ehelse.no/velferdsteknologi-og-digital-hjemmeoppfolging

Internett i Norge – Årsrapport 2023, Nkom, file:///C:/Users/DFD1112/Downloads/Internett%20i%20Norge%20-%20%C3%85rsrapport%202023.pdf

Internett i Norge – Årsrapport for 2024, Nkom, file:///C:/Users/DFD1112/Downloads/Internett%20i%20Norge%20-%20%C3%85rsrapport%202024.pdf

Innst. 8 S fra næringskomiteen, behandlet i Stortinget 15. desember 2023 punkt 13, https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2023-2024/inns-202324-008s/?all=true

Innst. 123 S (2023–2024) kap. 922 post 95, https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2023-2024/inns-202324-123s.pdf

Innst. 182 S (2015–2016) side 7, https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2015-2016/inns-201516-182.pdf

Innst. 247 S (2022–2023), https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2022-2023/inns-202223-247s.pdf

ISP – https://www.isp.se/utlandska-direktinvesteringar

Johan Røed Steen (2022). Skytjenester for offentlig sektor – Avveininger og internasjonale erfaringer. Fafo-rapport 2022:22, https://www.fafo.no/images/pub/2022/20825.pdf

Joint statement, Nordic and Baltic Ministers of Digitalisation (2024), https://www.norden.org/en/declaration/joint-statement-nordic-and-baltic-ministers-digitalisation

Journal Officiel du Grand-Duche de Luxembourg, https://legilux.public.lu/eli/etat/leg/loi/2017/12/01/a1029/jo

Kartlegging av offentlige myndigheters mulige bruk av opplysninger om eierskap til aksjer og fast eiendom (2023), Skatteetaten, https://www.regjeringen.no/globalassets/departementene/fin/2024/kartlegging-eierskapsopplysninger-v-1.0.pdf

Kommunale inntekter fra kraftsektoren Inntekter fra kommunalt og fylkeskommunalt eierskap i kraftsektoren og som vertskommune for slik virksomhet, samt anvendelse av inntektene. På oppdrag fra TBU, https://www.regjeringen.no/contentassets/d28f4297bf6c4fd89c5b099d7a89f79c/kommunale-inntekter-fra-kraftsektoren-thema.pdf

Kongelig resolusjon, ref. nr. 47, saksnr.: 21/1898, av 26. mars 2021, https://www.regjeringen.no/contentassets/e775dc91a33e4713a090da7398e6f3f5/endelig-godkjent-kgl.res.-stans-av-salget-av-bergen-engines-as.pdf

Konseptvalgutredning for nasjonal skytjeneste (2023), NSM, https://nsm.no/getfile.php/1313330-1696430485/NSM/Filer/Dokumenter/Rapporter/Nasjonal%20skytjeneste%20-%20konseptvalgutredning%20-%20KVU%202023.pdf

Lagen om granskning av utländska direktinvesteringar (2023:560) av 1. desember 2023 (Sverige), https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2023560-om-granskning-av-utlandska_sfs-2023-560/

Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven), https://lovdata.no/dokument/NL/lov/1967-02-10

Lov om elektronisk kommunikasjon (ekomloven), https://lovdata.no/dokument/NL/lov/2024-12-13-76

Lov om endringer i sikkerhetsloven (eierskapskontroll og lovens virkeområde), https://lovdata.no/dokument/NL/lov/2023-06-20-77

Lov om digital sikkerhet (digitalsikkerhetsloven), https://lovdata.no/dokument/LTI/lov/2023-12-20-108

Lov om militære rekvisisjoner (rekvisisjonsloven), https://lovdata.no/dokument/NL/lov/1951-06-29-19

Lov om nasjonal sikkerhet (sikkerhetsloven), https://lovdata.no/dokument/NL/lov/2018-06-01-24

Lov om næringsberedskap (næringsberedskapsloven), https://lovdata.no/dokument/NL/lov/2011-12-16-65

Lov om register over reelle rettighetshavere, https://lovdata.no/dokument/NL/lov/2019-03-01-2

Lov om screening af visse udenlandske direkte investeringer m.v. i Danmark (investeringsscreeningsloven), https://www.retsinformation.dk/eli/lta/2021/842

Lov om særlige rådgjerder under krig, krigsfare og liknende forhold (beredskapsloven), https://lovdata.no/dokument/NL/lov/1950-12-15-7

Lysekonsern.no, https://www.lysekonsern.no/om-oss/eierskap-og-historie/

Meld. St. 6 (2022–2023) Et grønnere og mer aktivt statlig eierskap — Statens direkte eierskap i selskaper, https://www.regjeringen.no/contentassets/b45b4a63e301435293bd1b10d1ede45b/no/pdfs/stm202220230006000dddpdfs.pdf

Meld. St. 8 (2019–2020) Statens direkte eierskap i selskaper — Bærekraftig verdiskaping, https://www.regjeringen.no/contentassets/44ee372146f44a3eb70fc0872a5e395c/no/pdfs/stm201920200008000dddpdfs.pdf

Meld. St. 9 (2022–2023) Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – Så åpent som mulig, så sikkert som nødvendig, https://www.regjeringen.no/contentassets/d256b455415c4cae8a710f62cc97d4f9/no/pdfs/stm202220230009000dddpdfs.pdf

Meld. St. 9 (2024–2025) Totalberedskapsmeldingen – Forberedt på kriser og krig, https://www.regjeringen.no/contentassets/c24e6978185f4a49a7d2689a4741a9b1/no/pdfs/stm202402250009000dddpdfs.pdf

Med. St. 28 (2020–2021) Vår felles digitale grunnmur, https://www.regjeringen.no/contentassets/e8441e5b035a4e18bbebf74737530c2f/no/pdfs/stm202020210028000dddpdfs.pdf

Microsoft blog (2022), https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Ministry of Economic Affairs and Employment of Finland, https://tem.fi/en/acquisitions

Moran, Theodore H. (2009). *Foreign Acquisitions and National Security: What are Genuine* Threats*? What are Implausible Worries? A Framework for OECD Countries, and Beyond*. (Post OECD draft December 14, 2009; https://www.usitc.gov/research_and_analysis/documents/Moran_OECD_Analysis_5b_0.pdf)

Much more than a market – speed, security, solidarity (2024), Enrico Letta, https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf

Nasjonal kontroll av IKT-tjenester (2023), NSM, https://nsm.no/getfile.php/1313327-1696336231/NSM/Filer/Dokumenter/Rapporter/Nasjonal%20kontroll%20av%20IKT-tjenester.pdf

Nasjonal trusselvurdering 2024, PST. https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2024/

NATO (Marcom) 2024, Allied Maritime Command – NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure

NATO (2024), NATO – News: NATO holds first meeting of Critical Undersea Infrastructure Network, 23-May.-2024, https://www.nato.int/cps/en/natohq/news_225582.htm

Nkom årsrapport 2023, file:///C:/Users/DFD1112/Downloads/Nkom%20%C3%85rsrapport_2023.pdf

Noregs Bank Memo 1/2023, https://www.norges-bank.no/aktuelt/nyheter-og-hendelser/Publikasjoner/Norges-Bank-Memo-/2023/memo-12023-betalingsformidling/nettrapport-memo-12023-betalingsformidling/

Norge som datasenternasjon (2018), strategi, Nærings- og fiskeridepartementet, https://www.regjeringen.no/globalassets/departementene/nfd/dokumenter/strategier/strategi-nfd-nett-uu.pdf

Norske datasenter – berekraftige, digitale kraftsenter (2021), strategi, Kommunal- og distriktsdepartementet, https://www.regjeringen.no/contentassets/0eabdbcbfb2540699466a4a1a801d737/nn-no/pdfs/norske-datasenter.pdf

Notat Folketingets Europaudvalg – Forslag til Europa-Parlamentet og Rådets forordning om screening af udenlandske investeringer i Unionen og om ophævelse af EuropaParlamentets og Rådets forordning (EU) 2019/452 KOM (2024) 23, https://www.eu.dk/samling/20231/kommissionsforslag/KOM(2024)0023/bilag/2/2871851.pdf

NOU 2018: 5 Kapital i omstillingens tid — Næringslivets tilgang til kapital, https://www.regjeringen.no/contentassets/62f6dd4e0274432da6475e53f4b14d44/no/pdfs/nou201820180005000dddpdfs.pdf

NOU 2023: 14 Forsvarskommisjonen av 2021 – Forsvar for fred og frihet, https://www.regjeringen.no/contentassets/8b8a7fc642f44ef5b27a1465301492ff/no/pdfs/nou202320230014000dddpdfs.pdf

NOU 2023: 17 Nå er det alvor – rustet for en usikker fremtid (Totalberedskapskommisjonen), https://www.regjeringen.no/contentassets/4b9ba57bebae44d2bebfc845ff6cd5f5/no/pdfs/nou202320230017000dddpdfs.pdf

NOU 2023: 28 Investeringskontroll- En åpen økonomi i usikre tider (Investeringskontrollutvalget), https://www.regjeringen.no/contentassets/d48b7fedaa21484cb1f33e118bcd1162/no/pdfs/nou202320230028000dddpdfs.pdf

NOU 2023: 4 Tid for handling — Personellet i en bærekraftig helse- og omsorgstjeneste, https://www.regjeringen.no/contentassets/337fef958f2148bebd326f0749a1213d/no/pdfs/nou202320230004000dddpdfs.pdf

NOU 2024: 7 Norge og EØS: Utvikling og erfaringer (Eldringutvalget), https://www.regjeringen.no/contentassets/15ef86ab491f4856b8d431f5fa32de98/no/pdfs/nou202420240007000dddpdfs.pdf

NRK (2022), https://www.nrk.no/tromsogfinnmark/rodt-krever-svar-etter-at-bredbandsfylket-avtalte-samarbeid-med-russiske-megafon-1.16183441

NRK (2024), https://www.nrk.no/vestfoldogtelemark/google-bygger-enormt-datasenter-i-skien-1.16749861

NSM, Hva er sikkerhetstruende økonomisk virksomhet? https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/handtering-av-sikkerhetstruende-okonomisk-virksomhet/hva-er-sikkerhetstruende-okonomisk-virksomhet/

NTB (2021), https://kommunikasjon.ntb.no/pressemelding/17920407/telenor-og-google-cloud-inngar-strategisk-partnerskap?publisherId=4954260

NTB (2022), https://kommunikasjon.ntb.no/pressemelding/17942689/telenor-etablerer-fiberselskap-i-norge?publisherId=4954260

NTB (2024), https://kommunikasjon.ntb.no/pressemelding/18052346/telenor-group-announces-collaboration-with-nvidia-to-support-its-ai-first-ambition?publisherId=4954260

NTB (2024), https://kommunikasjon.ntb.no/pressemelding/18037732/eidsiva-kjoper-etablert-datasenter-vi-skal-tilby-trygg-lagring-med-100-percent-nasjonalt-offentlig-eierskap?publisherId=17848064&lang=no

OECD (2024) Shaping Norway's Digital Future. https://www.oecd.org/en/publications/shaping-norway-s-digital-future_d3af799c-en/full-report.html

OneWeb, https://oneweb.net/about-us

Privat eierskap i Norge 2021, Menon Economics, https://menon.no/prosjekter/privat-eierskap-i-norge-2021

Prop. 11 L (2024–2025) Endringer i sivilbeskyttelsesloven (sivil arbeidskraftberedskap), https://www.regjeringen.no/contentassets/5512d3505ad240e08bd772795b0f8370/no/pdfs/prp202402500110000dddpdfs.pdf

Prop. 25 S (2023–2024) Endringar i statsbudsjettet 2023 under Nærings- og fiskeridepartementet, https://www.regjeringen.no/contentassets/f8065596bce74356b5249bd67d716ee4/nn-no/pdfs/prp202320240025000dddpdfs.pdf

Prop. 87 S (2023–2024) Forsvarsløftet – for Norges trygghet, https://www.regjeringen.no/contentassets/27e00e5acc014c5ba741aacfff235d99/no/pdfs/prp202320240087000dddpdfs.pdf

Prop. 93 LS (2023–2024) Lov om elektronisk kommunikasjon, https://www.regjeringen.no/contentassets/096a9d827c8f48c3ae8b7817fe463a25/no/pdfs/prp202320240093000dddpdfs.pdf

Prop. 97 L (2015–2016) Endringer i sikkerhetsloven, https://www.regjeringen.no/contentassets/69a229ce36cd40beb7cfba3f1f2af6e8/no/pdfs/prp201520160097000dddpdfs.pdf

Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet (sikkerhetsloven), https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/

Prop. 143 L (2016–2017) Endringar i statsbudsjettet 2017 under Finansdepartementet og Kommunal- og moderniseringsdepartementet, https://www.regjeringen.no/contentassets/94770ac58f8e4975beb27f031f5e3402/nn-no/pdfs/prp201620170143000dddpdfs.pdf

Prop. 1 S (2024–2025) For budsjettåret 2025 under Digitaliserings- og forvaltningsdepartementet, https://www.regjeringen.no/contentassets/e628c0d8c3a44971bb48bd5a487cb52d/nn-no/pdfs/prp202420250001dfddddpdfs.pdf

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452 of the European Parliament and of the Council, Proposal for a new regulation on the screening of foreign investments (10).pdf

På rett sted til rett tid – Nasjonal strategi for posisjonsbestemmelse, navigasjon og tidsbestemmelse (2018), Samferdselsdepartementet, https://www.regjeringen.no/contentassets/abd1dec7647a4c22aaef7d93046e3f2b/pa-rett-sted-til-rett-tid.pdf

Regjeringens arbeidsprogram for EU- og EØS-saker 2024-2025, https://www.regjeringen.no/contentassets/a6636bfa850f4add822ba8ac7ecb2014/regjeringens-arbeidsprogram-for-eu-saker.pdf

Regjeringen.no (2023), Space Nor https://www.regjeringen.no/no/aktuelt/space-norway-med-avtale-om-kjop-av-telenor-satellite/id3014624/way med avtale om kjøp av Telenor Satellite – regjeringen.no

Regjeringen.no (2023), https://www.regjeringen.no/no/aktuelt/green-mountain-vert-underlagt-sikkerheitslova-og-far-etablere-datasenter-i-innlandet/id2989926/

Regjeringen.no (2023), https://www.regjeringen.no/no/aktuelt/nytt-system-for-nodvarsel-til-befolkningen-er-etablert/id2958586/

Regjeringen.no (2024), https://www.regjeringen.no/no/aktuelt/okt-sikkerhet-for-kritisk-infrastruktur-pa-norsk-sokkel/id3023761/

Regjeringen.no (2024), Nytt n https://www.regjeringen.no/no/aktuelt/skal-sikre-tryggere-havbunn/id3083648/orsk-tysk initiativ skal styrke kritisk undersjøisk infrastruktur i Europa – regjeringen.no

Regjeringen.no (2024), https://www.regjeringen.no/no/aktuelt/samarbeid-for-a-sikre-kritisk-undersjoisk-infrastruktur/id3033122/

Regjeringen.no (2024), https://www.regjeringen.no/no/aktuelt/norge-slutter-seg-til-internasjonalt-initiativ-om-undersjoiske-kabler/id3075280/

Regjeringen.no (2025), Skal sikre tryggere havbunn – regjeringen.n https://www.regjeringen.no/no/aktuelt/skal-sikre-tryggere-havbunn/id3083648/o

Risiko 2023 Økt forutsigbarhet krever høyere beredskap, NSM, https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

Risiko 2024 Nasjonal sikkerhet – et felles ansvar, NSM, https://nsm.no/getfile.php/1313477-1719434219/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf

Risiko- og sårbarhetsanalyse for ekomsektoren (2024), Nkom. file:///C:/Users/DFD1112/Downloads/EkomROS%202024%20-%20offentlig%20versjon.pdf

Robuste transmisjonsnett for Norge mot 2030 Målbilder og virkemidler (2022), Nkom, file:///C:/Users/DFD1112/Downloads/Nkomrapport%2001.2022%20-%20Robuste%20transmisjonsnett%20for%20Norge%20mot%202030-ENKLE%20SIDER.pdf

Samfunnets kritiske funksjoner (2016), DSB. https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Schrems I og Schrems II, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362

Sikkerhetsfaglig råd – Et motstandsdyktig Norge (2023), NSM. https://nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20r%C3%A5d%20-%20Et%20motstandsdyktig%20Norge.pdf

Spørsmål til skriftlig besvarelse nr. 18 fra stortingsrepresentant (1463202), https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qnid=67684

Starlink, https://www.starlink.com/

Statens eierrapport (2023) – Statens direkte eierskap i selskaper, https://www.regjeringen.no/contentassets/1a9b9fca3f5542c08bd576c844f6034b/no/pdfs/statens-eierrapport-2023.pdf

Stortinget – Møte torsdag den 18. april 2024, Sak nr. 3 [14:38:04], https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Referater/Stortinget/2023-2024/refs-202324-04-18?m=3

Tampnet.com (2021), https://www.tampnet.com/press/tampnet-and-oneweb-sign-agreement-to-further-develop-the-next-generation-of-offshore-connectivity-capabilities

Telenor.no (2017), https://www.telenor.no/om/presse-og-media/pressemeldinger/telenor-styrker-beredskapen-langs-finnmarkskysten.page

Telia.no (2024), https://presse.telia.no/pressreleases/telia-tar-sitt-nordiske-partnerskap-med-microsoft-til-det-norske-markedet-forenkler-hverdagen-for-bedriftskundene-3357446

Waage, K., Kvalvik, S. N., & Lindgren, P. Y. (2021). *Utenlandske investeringer og andre økonomiske virkemidler-når truer de nasjonal sikkerhet?* FFI-RAPPORT 20/03149. (http://18.195.19.6/handle/20.500.12242/2832)

Foto: Anders Martinsen (Nkom)

16

Vedlegg

Vedlegg 1: Utvalgets samlede forslag til tiltak

Vedlegg 2: Fremtidsanalyse foretatt av Oslo Economics og Norsk Utenrikspolitisk Institutt

Vedlegg 3: Analyse av eierstrukturer foretatt av Menon Economics

Vedlegg 4: Juridisk utredning foretatt av professor Christoffer Conrad Eriksen (UiO)

Vedlegg 5: Tilbakemeldinger fra tilbyderne knyttet til nasjonal kontroll med kritisk digital infrastruktur

Vedlegg 6: Informasjonsinnhenting april 2024 offentlige ekomtilbydere

Vedlegg 1

Utvalgets samlede forslag til tiltak

Vedlegg 1 Utvalgets samlede forslag til tiltak

1. *Utvalget mener at Finansdepartementet må klargjøre hvem som etter dagens regelverk vil kunne få adgang til registeret over reelle rettighetshavere, knyttet til oppgaver etter sikkerhetsloven. Hvis dagens regelverk ikke åpner for at et departement som har sektoransvar etter sikkerhetsloven får tilgang til opplysninger, bør forskriften til lov om register over reelle rettighetshavere endres, slik at alle myndigheter som har sektoransvar etter sikkerhetsloven, gis tilgang til opplysninger fra registeret.*

   Forslaget er omtalt og begrunnet i punkt 8.3 i rapporten.

2. *Utvalget mener at Digitaliserings- og forvaltningsdepartementet og Justis- og beredskapsdepartementet bør se til at EØS-relevant regelverk for digital kommunikasjonsinfrastruktur gjennomføres i Norge og at det skjer i så nær tid som mulig med tilsvarende regulering i EU.*

   Forslaget er omtalt og begrunnet i punkt 9.8 i rapporten.

3. *Utvalget mener at når staten begrunner eierskap med å ivareta samfunnssikkerhet gjennom eierskap, må staten i forvaltningen av eierskapet være tydeligere på hvordan hensynet til samfunnssikkerhet og beredskap veies mot hensynet til avkastning, andre aksjonærer og for eksempel statsstøtteregler.*

   Forslaget er omtalt og begrunnet i punkt 9.8 i rapporten.

4. *Utvalget anbefaler at Digitaliserings- og forvaltningsdepartementet identifiserer og holder ved like en dokumentert oversikt over virksomheter i henhold til sikkerhetsloven § 2-1, samt øvrige virksomheter som forvalter digital kommunikasjonsinfrastruktur og funksjoner som anses samfunnskritiske.*

   Forslaget er omtalt og begrunnet i punkt 11.6.1 i rapporten.

5. *Utvalget anbefaler at Digitaliserings- og forvaltningsdepartementet etablerer og vedlikeholder et målbilde for nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur. Målbildet bør definere nødvendige nasjonale styringsevner og handlefriheter i fred, krise og krig, for de viktigste infrastrukturkategoriene i økosystemet for digital kommunikasjonsinfrastruktur, som inkluderer:*

   - ***Passiv infrastruktur**, herunder nasjonal fiberinfrastruktur og fiberkabler til utlandet*

***- Støtteinfrastruktur**, herunder nasjonal datasenterkapasitet, fortifikatoriske anlegg, mobiltårn, og nasjonal infrastruktur for nøyaktig tid/takt*

***- Tjenesteproduksjonsinfrastruktur**, herunder for bredbånd og transportnett, internettfunksjoner som DNS, ruting og samtrafikk, mobilkjernenett og basestasjoner, maritim kommunikasjonsinfrastruktur og bakkebasert satellittinfrastruktur*

Herunder bør målbildene beskrive behovet for personellressurser og kompetanse nødvendig for design og konfigurasjon, utbygging, drift og overvåking, feilretting og gjenopprettingsevne. Dette omfatter både infrastruktur på land til havs, herunder rettekapasitet for undersjøiske fiberkabler.

Forslaget er omtalt og begrunnet i punkt 11.6.2 i rapporten.

6. *Utvalget anbefaler at når et målbilde for nasjonal kontroll er etablert bør Digitaliserings- og forvaltningsdepartementet utvikle og vedlikeholde en gapanalyse av målbildet som beskriver de aktuelle virkemidlene staten rår over, og eventuelle svakheter, begrensninger og hindre for å bruke disse for å sikre de nødvendig styringsevner og handlefriheter.*

   Forslaget er omtalt og begrunnet i punkt 11.6.3 i rapporten.

7. *Utvalget mener at Digitaliserings- og forvaltningsdepartementet bør vurdere om sektorregelverket i tilstrekkelig grad sikrer tidlig informasjon til myndighetene om kontrollsvekkende økonomisk virksomhet fra selskapene som eier kritisk digital kommunikasjonsinfrastruktur, og bøte på eventuelle svakheter*.

   Forslaget er omtalt og begrunnet i punkt 12.2 i rapporten.

8. Utvalget mener regjeringen ved utarbeidelse av ny lov for kontroll av utenlandske investeringer bør se hen til EUs nye regelverk om screening av utenlandske direkte investeringer, uavhengig av om regelverket anses EØS-relevant.

   Forslaget er omtalt og begrunnet i punkt 12.3 i rapporten.

9. *Utvalget mener at dersom Nærings- og fiskeridepartementet går videre med Investeringskontrollutvalget sitt forslag om én investeringskontrollmyndighet, må Nærings- og fiskeridepartementet sikre at sektorspesifikk fagkompetanse blir tilgjengeliggjort for en slik etat.*

   Forslaget er omtalt og begrunnet i punkt 12.3 i rapporten.

10. *Utvalget anbefaler at Justis- og beredskapsdepartementet klarlegger om bestemmelsen i sikkerhetsloven § 10-3 er i tråd med EØS-avtalen.*

    Forslaget er omtalt og begrunnet i punkt 12.4.2 i rapporten.

11. *Utvalget mener Digitaliserings- og forvaltningsdepartementet bør avklare om det sektorspesifikke regelverket er i stand til å ivareta situasjoner der man står overfor kontrollsvekkende aktivitet i ekomsektoren. I første omgang er det behov for å vurdere rekkevidden av bestemmelsene i ekomloven §§ 3-1, 3-5 og 3-7 opp mot sikkerhetsloven § 2-5.*

    Forslaget er omtalt og begrunnet i punkt 12.4.4 i rapporten.

12. *Utvalget ser behov for etablering av nasjonal skyløsning ut fra behovet for nasjonal kontroll, og mener at dette arbeidet bør gis høy prioritet. Det anbefales at Justis- og beredskapsdepartementet tydeliggjør videre ambisjonsnivå og plan, og gjør nødvendige midler tilgjengelig for arbeidet.*

    Forslaget er omtalt og begrunnet i punkt 13.6 i rapporten.

13. *Digitaliserings- og forvaltningsdepartementet bør vedlikeholde et faktagrunnlag knyttet til nasjonal avhengighet av utenlandske innsatsfaktorer, herunder mikrotjenester, DNS-tjenere, sertifikattjenester, og internettsamtrafikk. Dette faktagrunnlaget bør danne basis for utvikling og vedlikehold av målbilde og virkemidler for nasjonal kontroll, og i den sammenheng vår avhengighet til infrastruktur som ligger utenfor norsk jurisdiksjon.*

    Forslaget er omtalt og begrunnet i punkt 13.10 i rapporten.

Vedlegg 2

Fremtidsanalyse foretatt av Oslo Economics og Norsk Utenrikspolitisk Institutt

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

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 dokumentgjennomganger. 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 kommunikasjons-myndighet
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 ekommarkedet og den nasjonale kontrollen i verdikjeden.
- Hvordan geopolitiske trender og internasjonale reguleringer påvirker aktøren, men også ekommarkedet 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.

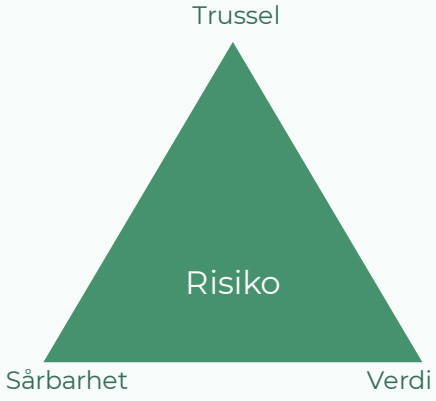
Krigen i Ukraina og de økte spenningene mellom Kina og USA har løftet sikkerhetspolitikk høyere på agendaen, og illustrert i hvor stor grad økonomiske og teknologiske avhengigheter kan bli brukt som 0strategiske instrumenter i en potensiell konflikt. Politisk interesse for verdikjeder og økonomisk sikkerhet 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 kommunikasjons-infrastruktur

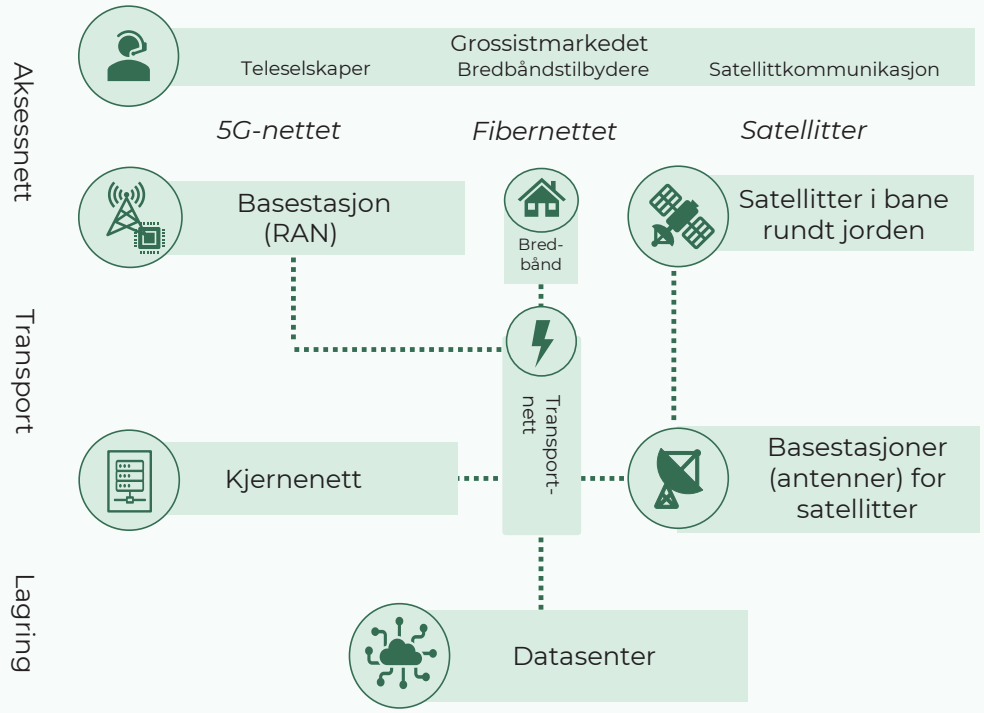
Det benyttes ofte ulike begreper for å definere digital infrastruktur. I dette prosjektet er formålet å vurdere kritisk infrastruktur for elektronisk kommunikasjon. Innledningsvis er det derfor nyttig å først klargjøre enkelte begreper og hva vi definerer som infrastruktur for elektronisk kommunikasjon 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 kjernettet, og er kritiske deler av deres respektive nett.

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

2.1.2 Aksessteknologier

Aksessnettet defineres som de punktene hvor sluttbrukere kan aksesseres transportnettet med ulike teknologier. Vi skiller mellom tre ulike aksessteknologier; kablet bredbånd, mobilnettverk og satellitteknologi. Aksess via bredbånd er den fiber- eller kobberkabelen som kobler brukeren til transportnettet. 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 transportnettet via **radiobølger** til basestasjoner som igjen er koblet til transportnettet 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 videresender 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 datasenter:** 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 datasenter:** Mindre datasentre som plasseres lengere ute i nettverkene for å være nær sluttbruker for å ivareta krav til latens[1], 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 løsere 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

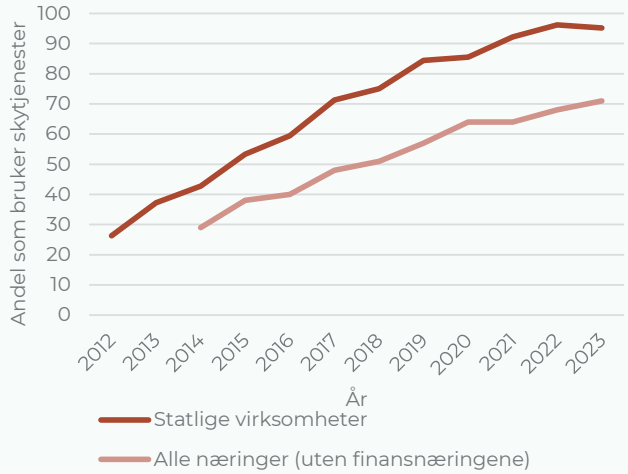
Den neste digitaliseringsbølgen kom med oppfinnelsen av smarttelefoner og skyteknologi. Skytjenester (cloud computing) er en samlebetegnelse på alt fra dataprosessering og datalagring til programvare på servere som er tilgjengelig fra eksterne serverparker tilknyttet internett (Datatilsynet, 2018). Selskaper 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.

Dette 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 undersøkelen.

igjen bidratt til at mobiltelefonen i dag benyttes til stadig flere oppgaver som tidligere ble gjennomført manuelt, som for eksempel betalingsmiddel, 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

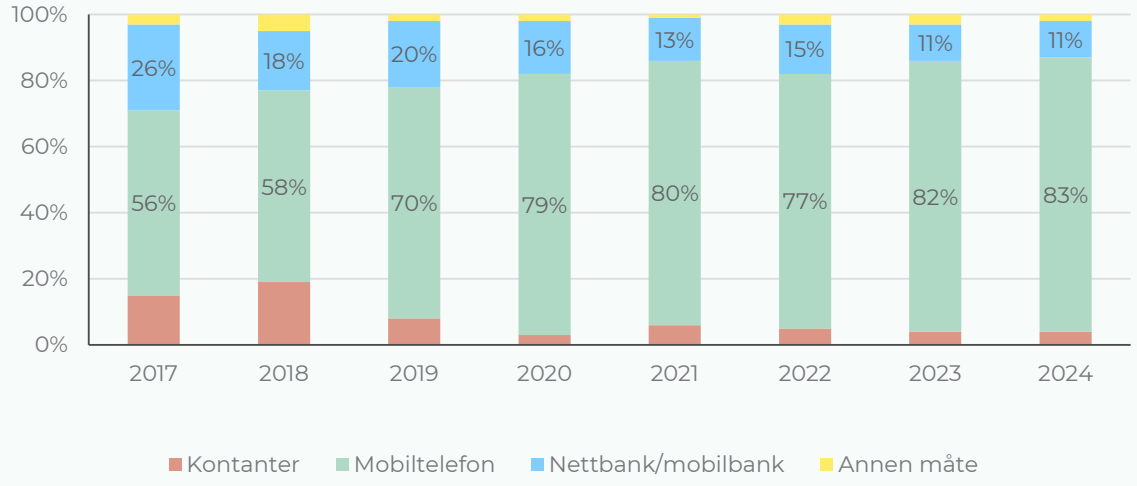
En utfordring fremover er at veksten i antallet personer i yrkesaktiv alder er ventet å stagnere, samtidig som antallet eldre vil øke betydelig. Disse demografiske endringene skaper betydelige utfordringer. Perspektivmeldingen 2024 fremhever viktigheten av å øke arbeidstilbudet for å møte disse utfordringene. 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 Helsepersonellkommisjonen, 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.



Kilde: (Norges Bank, 2024 (1))

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 1av 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 fysisk 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 smarthøyttalere 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 departmentsfelleskapet 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 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 sluttkunder 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 styreformer 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 amerikanskeide 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 monopoltendenser 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 teknologier, 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 skjerme, 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 samfunnssikkerhet blir tilstrekkelig ivaretatt 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 risikoer 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 teknologiutviklingen.

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 vanskelige 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 risikoer, 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» geoøkonomiske 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

teknologiutvikling 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 Huaweis 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 kabeler 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 teknologiuavhengighet 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 teknologiuavhengighet 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 tiltak[3] 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 oppfattingen 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 jevnlige 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, tariffer 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 markedskontroll (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 oppføringer[4] 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

telekommarkedet. 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 flaskehalser 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 gjennomførbar 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 verks 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 budsjettramme 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 teknologiuavhengighet 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 datalagringssentre 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

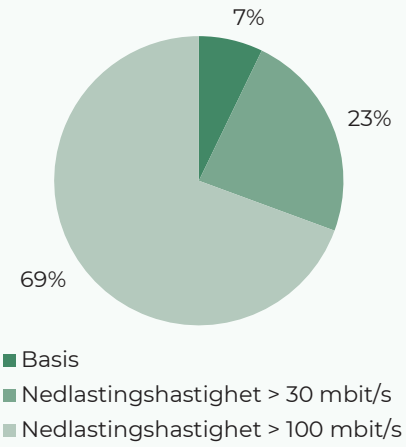
Som drøftet tidligere driver høyere krav til den digitale infrastrukturen frem et behov for investeringer. Overgangen til et femte generasjons mobilnettverk (5G) er sentral for at flere smarte gjenstander kan fungere optimalt. Overgangen til et 5G-nett krever imidlertid store investeringer fra teleoperatørene som eier og drifter 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 fibernettet.

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

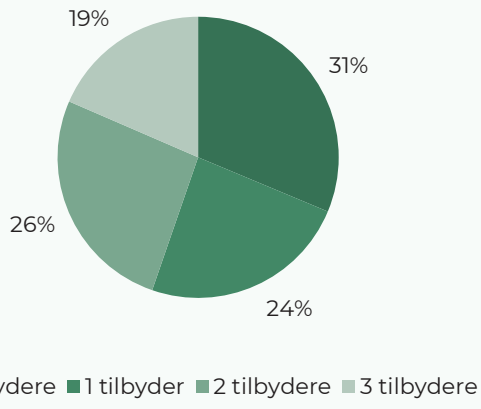
Figur 4-1: Husholdningers internetthastighet og tilgang til tilbydere

a) Hastighet



Mbit/s og % antall husholdninger

b) Tilgang til tilbydere per husstand



Tilbyder 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 utrullingen 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 dekningen for fibernett. 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 tårnselskap i Sverige (Net4Mobility, 3GIS) og Danmark (TTT) (Telenor Towers, 2024). Telenors fibernett ble skilt ut i et eget selskap med Telenor som majoritetseier (70%) og to andre finansielle medeiere. [5] Transaksjonen verdsatte fibernettet 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 spørsmålstegn 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 mobilselskaper 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.

[5]

[6] Alecta er et av Sveriges største pensjonsfond. Brookfield er et internasjonalt investeringsselskap.

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 e 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. A1 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 nedsalg og fraksjoneringer 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 telekomtjenester 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 helintegrerte tilbyderne 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 utforfordrere 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 kjernettfunksjoner. 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 Deutche 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.

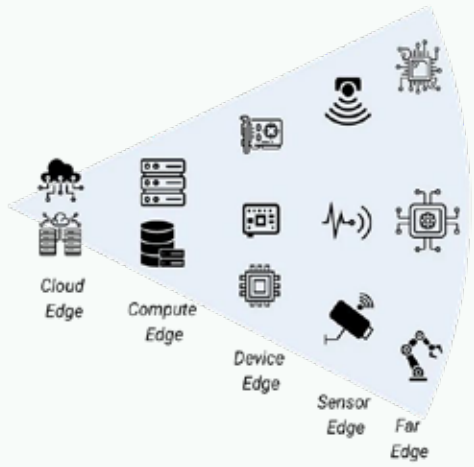
Open-RAN

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 hyllevare 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 arkitektur[7] 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. Vodaphone har implementert arkitekturen på flere hundre basestasjoner i Storbritannia, og planlegger å utvide dette til flere tusen. Tilsvarende planlegger Deutche 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 utrullingen, 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 utrullingen av Open-Ran kan vise seg å bli mer en gradvis overgang til en mer åpen og kostnadseffektiv arkitektur, enn en revolusjonær disrupsjon av de tradisjonene 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 sluttkunder.

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.

sluttkunder 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 regulerbar 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 lavbanesatelitter kunne være et supplement til bakkebaserte bredbåndsnett i områder uten mobildekning, og i situasjoner med utfall i mobilnettene.

Lavbanesatelitter har også mulighet til å koble seg direkte til mobiltelefoner og IoT-instrumenter (direct-to-device). Fremfor å måtte bruke dedikerte satelittelefoner 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 lavbanesatelitt-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 sattelitttilkobling (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 kapittelet.

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 telekomselskap. 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 majoritetseide datterselskap. Telenor, Telia og ICE har henholdsvis staten som majoritetseier, svenske stat som kontrollerende minoritetseier 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 fibernett 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 minoritetseier 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 minoritetseiendelen 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) Deutche 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 datasenter. 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 telekomoperatørenes 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 vet 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 datalagringssentre 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 datalagringssentrene 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 er 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 1 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 Comission.

Edmonstone, G., 2024. *Economic security policies compared: The United States, it's 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 20024].

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/nasjonal-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. & Farell, 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 Interdependece 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-

15/
[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

Vedlegg 3

Analyse av eierstrukturer foretatt av Menon Economics

MENON ECONOMICS

RAPPORT

EIERSKAP I KRITISK DIGITAL KOMMUNIKASJONSINFRASTRUKTUR

MENON-PUBLIKASJON NR. 156/2024

Av Linn Skyum, Aria Khosravi, Per Fredrik Johnsen, Jonas Erraia og Caroline Wang Gierløff

Forord

På oppdrag for Digitaliserings- og forvaltningsdepartementet har Menon Economics kartlagt og analysert eierskapet i kritisk digital kommunikasjonsinfrastruktur. Formålet med oppdraget var å få en oversikt over hvem som eier infrastrukturen, med et særlig fokus på utenlandsk eierskap gjennom flere ledd i eierskapskjeden. Videre er det gjort vurderinger av risiko knyttet til utenlandsk eierskap, og sårbarheten knyttet til eierskap hvor man ikke har lykkes med å identifisere reelle rettighetshavere.

Prosjektet har vært ledet av Per Fredrik Johnsen, med Linn Skyum og Aria Khosravi som prosjektmedarbeidere. Ansvarlig partner er Caroline Wang Gierløff. Ulf Sverdrup (BI) har vært sparringspartner og Jonas Erraia har vært kvalitetssikrer og ekspertressurs.

Menon Economics er et forskningsbasert analyse- og rådgivningsselskap i skjæringspunktet mellom foretaks-økonomi, samfunnsøkonomi og næringspolitikk. Vi tilbyr analyse- og rådgivningstjenester til bedrifter, organisasjoner, kommuner, fylker og departementer. Vårt hovedfokus ligger på empiriske analyser av økonomisk politikk, og våre medarbeidere har økonomisk kompetanse på et høyt vitenskapelig nivå.

Vi takker Digitaliserings- og forvaltningsdepartementet for et spennende oppdrag. Forfatterne står ansvarlig for alt innhold i rapporten.

November 2024

Caroline Wang Gierløff
Prosjektansvarlig
Menon Economics

November 2024

Per Fredrik Johnsen
Prosjektleder
Menon Economics

Innhold

1 Innledning og bakgrunn

Etter hvert som samfunnet blir gradvis mer avhengig av digitale tjenester, legger vi stadig mer makt i hendene på aktørene som eier og forvalter tjenestene og infrastrukturen vi benytter oss av. Dette gjelder særlig i Norge, som er et av verdens mest digitaliserte land. Der fysisk kontroll over infrastrukturen tidligere kunne være tilstrekkelig, gjør digitaliseringen av infrastrukturen eierskapet stadig mer relevant fra et sikkerhets- og beredskapsperspektiv. Uten tilstrekkelig nasjonal kontroll, vil det norske samfunnet være sårbare for trusler fra eksterne aktører. I den nasjonale trusselvurderingen fra 2024 skriver PST at de forventer at Russland og Kina vil benytte seg av oppkjøp og investeringer i norske virksomheter for å sikre seg ulike strategiske fordeler. Slike investeringer kan utgjøre en trussel mot grunnleggende nasjonale interesser når de sees i sammenheng med hverandre.[1]

Nasjonal kontroll over kritisk infrastruktur er derfor essensielt for å unngå at uønskede aktører påvirker vårt politiske eller økonomiske handlingsrom. Nasjonal kontroll innebærer å kunne forebygge at uønskede aktører får innflytelse på vårt eget politiske eller økonomiske handlingsrom. Det betyr også at nasjonal kontroll ikke trenger å være ensbetydende med offentlig eierskap, men kan ivaretas gjennom helt eller delvis nasjonalt eierskap, der norske private virksomheter eller personer eier selskapene. Det kan også oppnås gjennom internasjonalt samarbeid når eierskapsstrukturene er tilstrekkelig transparente.

Det skjerpede sikkerhetspolitiske bildet, både i Europa og globalt, har fremhevet behovet for nasjonal kontroll over kritisk digital infrastruktur. Som en konsekvens ble ekomsikkerhetsutvalget nedsatt i januar 2024 for å vurdere hvordan staten best kan ivareta nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur.

Ekomsikkerhetsutvalget skal på et overordnet nivå identifisere kritisk digital kommunikasjonsinfrastruktur og selskaper som eier eller råder over slik infrastruktur og deres bakenforliggende eierforhold. I tillegg skal selskaper som er av avgjørende betydning for utbygging, drift og vedlikehold av infrastrukturen, og deres eiere, identifiseres. Utvalget har tre delmål:

- Identifisere kritisk infrastruktur på et overordnet nivå
- Status for nasjonal kontroll og dagens virkemidler
- Vurdere tiltak for styrket nasjonal kontroll

Som et ledd i deres arbeid har utvalget gitt Menon Economics i oppdrag å kartlegge eierskap i selskaper som i dag har kontroll over, kan ha kontroll over, eller er leverandører til kritisk digital infrastruktur. Denne rapporten gir en oversikt over dagens eierforhold og eierstrukturer i selskaper som eier eller kontrollerer kritisk digital kommunikasjonsinfrastruktur i Norge, eller selskaper som er av avgjørende betydning for utbygging, vedlikehold eller drift av infrastrukturen. I kartleggingsarbeidet har vi hatt et særskilt fokus på å nøste opp i utenlandske eierstrukturer for å vise bakenforliggende utenlandsk eierskap i flere ledd der dette er relevant.

Rapporten er organisert på følgende måte: I kapittel 2 beskriver vi informasjonskilder og metode for kartlegging av eierskap. I kapittel 3 presenterer vi eiere av, og leverandører til, kritisk digital kommunikasjonsinfrastruktur og deres kjennetegn, før vi i kapittel 4 analyserer vi eierskapet til selskapene. I kapittel 5 oppsummerer vi funnene og drøfter mulige risikoelementer.

[1] *PST. (2024). Nasjonal trusselvurdering 2024. Tilgjengelig her.*

2 Metode og informasjonskilder

I dette kapittelet beskriver vi vår metodiske tilnærming til oppdraget og informasjonskilder. Informasjonsinnhentingen har bestått av tre steg, med gradvis økende kompleksitet, samt færre selskaper og datapunkter. I det første steget kartlegger vi norsk eierskap, mens de to siste stegene gikk ut på å kartlegge utenlandsk eierskap. Den stegvise tilnærmingen er som følger:

1. **Norsk eierskap:** Standardisert selskaps- og eierskapsinformasjon fra Menons databaser
2. **Utenlandsk eierskap:** Undersøkelser i andre databaser og offentlig tilgjengelig informasjon
3. **Utenlandsk eierskap:** Detaljert gravearbeid i gjenstående selskaper

I det første steget benyttet vi standardisert informasjon som Menon allerede har tilgjengelig i våre databaser, før vi går videre i mer detaljerte undersøkelser i de selskapene der det er behov for det. Etter hvert som informasjonen har blitt vanskeligere å oppdrive, har også metodene vi har benyttet gradvis blitt mindre standardiserte og strukturerte, og i økende grad tilpasset hvert enkelt selskap.

Boks 2-1: Begrepsforklaring og definisjoner

Direkte eierskap: Direkte eierskap er eierskapet i en virksomhet uten noe mellomledd. Det omfatter *ikke* eierskap som er organisert gjennom holdingselskap og lignende selskapsstrukturer med flere eierledd.

Indirekte eierskap: Indirekte eierskap er eierskap organisert gjennom en eller flere andre enheter/eierledd, eksempelvis et holdingselskap, som utgjør et mellomledd.

Effektivt eierskap: Det effektive eierskapet er den reelle eierandelen til en eier, som inkluderer både direkte og indirekte eierskap.

Ultimat eier: Ultimate eiere er de personene, stiftelsene/selveiende virksomheter eller det offentlige som er øverst i et eierskapshierarki og har en eierandel i virksomheten.

Reell rettighetshaver: Reell rettighetshaver er en fysisk person som, alene eller sammen med andre, kontrollerer virksomheten. Reell rettighetshaver har med andre ord innflytelse på virksomheten.

2.1 Metode for kartlegging av norsk eierskap

I første steg har vi kartlagt den etterspurte selskapsinformasjonen. Dette inkluderer i hovedsak to ulike typer informasjon. Den første er selskaps- og regnskapsinformasjon, mens den andre er eierskapsinformasjon. For begge informasjonstyper benytter vi regnskaps- og eierskapsdata fra Menons egne databaser. I tekstboksen beskriver vi kort de to viktigste databasene vi bruker i første steg.

Ved hjelp av Menons eierskapsdatabase har vi kartlagt det fulle hierarkiet av norsk eierskap inklusiv ultimate eier. Eierskap i norsk næringsliv er komplekst og mye av eierskapet er organisert gjennom eierskapsstrukturer som kan gjøre det uoversiktlig å kartlegge hele eierskapet i enkeltselskaper. I Menons eierskapsdatabase løser vi dette, og ender opp med noen definerte ultimate eierskapstyper. Se Vedlegg A: Metode for identifisering av ultimate eiere for en detaljert beskrivelse av databasen.

Boks 2-2: Beskrivelse av Menon

Menons eierskapsdatabase

Menons eierskapsdatabase består av en fullstendig kartlegging av hele eierskapshierarkiet til norske selskap, der eierskapshierarkiet rulles tilbake til vi står igjen med det som kategoriseres som ultimat eier. Ultimat eier er i norsk sammenheng enten en norsk privatperson, en offentlig aktør, en selveid organisasjon eller stiftelse eller en utenlandsk aktør. Databasen dekker eierskapet i alle norske foretak fra 2005 til 2023.

Menons regnskapsdatabase

Menons regnskapsdatabase inneholder all regnskapsdata for alle norske regnskapspliktige selskap tilbake til 1992. Databasen oppdateres løpende, og er en viktig grunnsten i mye av Menons empiriske arbeid. Databasen omfatter over 600 000 selskap, og inneholder informasjon om omsetning, driftsresultat, verdiskaping, antall ansatte, lokasjon for hovedkontor og avdelinger, styremedlemmer, andre styreforhold, direkte eierskap, næring, og mye mer.

Eierskapsdatabasen og regnskapsdatabasen kobles gjennom selskapenes organisasjonsnummer.

2.2 Metode for kartlegging av utenlandsk eierskap

Ettersom første eier i utlandet ofte et holdingselskap eller andre ikke-personlige eiere, er det ikke nødvendigvis samsvar mellom landet disse selskapene er lokalisert i og landet til morselskapet eller ultimate personlige eier.[2] Som en direkte konsekvens av dette, har vi anvendt andre informasjonskilder for å få dypere innsikt i utenlandske eierforhold.

[2] Dette blir ikke gjort enklere av at enkelte av landene der holdingselskapene er plassert, ofte har lite informasjon tilgjengelig om eierskap. De mest typiske blant disse landene er Irland, Nederland, Luxembourg, Sveits, samt en lang rekke mindre land som fungerer som skatteminimerende jurisdiksjoner for selskaper.

For å kartlegge disse strukturene har vi i det andre steget gjort systematiske gjennomganger av utenlandske eierskapsregistre, internasjonale databaser og øvrig tilgjengelig selskapsinformasjon. De viktigste kildene er gjengitt i boksen under.

Boks 2-3: Beskrivelse av øvrige eierskapsregistre og internasjonale databaser

Orbis – En internasjonal selskapsdatabase som dekker selskaper over hele verden, med omfattende informasjon om eierskap og eierskapsstrukturer. Orbis nøster opp i internasjonale eierstrukturer for å finne «globale ultimate eiere». Orbis kartlegger eierskapet ledd for ledd tilbake til siste ledd med majoritetseierskap, kalt «global ultimat eier». Det kan være både et selskap og en enkeltperson. Videre har Orbis i mange tilfeller informasjon om minoritetsaksjonærer lenger bak i eierskapshierarkiet. Det er imidlertid ikke alltid lett å finne ut hvem som er den ultimate eieren av et selskap, ettersom selskapsstrukturer kan være komplekse og eierskap kan bevisst skjules.

Nasjonale og private eierskapsdatabaser – Mange land tilbyr åpent tilgjengelige registre over eierskap og/eller reelle rettighetshavere for selskap registrert i landet. Slike registre finnes blant annet i Sverige, Danmark, Storbritannia og USA, og muliggjort sporing av eierskapskjeder i utlandet med samme metode som vi benytter på norske eierskapsdata.

Offentlig tilgjengelige regnskaps- og årsrapporter – I tilfeller der informasjon om eierskap ikke er systematisert i åpent tilgjengelige registre, vil det fremdeles ofte være mulig å hente ut nødvendig informasjon direkte fra selskapenes dokumenter. Denne informasjonen inkluderer både eiere, samt informasjon om styremedlemmer. Et eksempel på dette er amerikanske selskapers SEC-dokumenter, som publiseres på det amerikanske SECs nettsider.

I de to første stegene har vi anvendte strukturerte databaser og data fra systematiserte kilder, som innebærer at de er transparente og etterprøvbare. I det tredje steget har vi gjennomført en manuell «desk research» for å dykke dypere ned i eierstrukturen til de ulike utenlandske majoritetseierne. Det kan være flere årsaker til at det er vanskelig å finne eierskapsinformasjon – eksempelvis kan eieren være registrert i land med få krav til transparens, eller eierskapsformen kan være vanskelig å spore, der selskapet benytter seg av skallselskaper eller er eid av investeringsselskaper.

Metodene vi har anvendt for å avdekke eierskap i komplekse eierstrukturer avhenger av hvilke selskaper det er snakk om, og under er en kort oppsummering av anvendte tilnærminger:

- **Gjennomgang av åpne kilder**: Vi har benyttet oss av åpne kilder som nyhetsartikler, selskapsrapporter og ulike offentlige registre for å finne opplysninger om de aktuelle eierne. Dette har gitt en bredere forståelse av eierskapet, spesielt som supplement når offisielle databaser ikke gir tilstrekkelig informasjon.
- **Bruk av lister over viktige selskap og eierstrukturer.** Flere land og regioner har lister over selskaper som enten kan utgjøre trusler eller som det er forbud mot å handle med. Eksempler på slike lister er USAs Entity List[3] som oppdateres jevnlig. Disse kan brukes til å identifisere selskaper som av eksempelvis USA eller EU er vurdert som særlig problematiske.
- **Sosiale medier og profesjonelle nettverk**: Enkelte eiere er kartlagt gjennom plattformer som LinkedIn, X/Twitter og lignende. Disse kanalene er nyttige for å identifisere eiere og deres nettverk, særlig dersom de er involvert i flere selskaper eller har en offentlig profil. I tilfeller hvor eiere er identifisert gjennom slike kilder, er de bekreftet gjennom alternative kilder for verifisering.

[3] *Tilgjengelig her: https://www.dhs.gov/uflpa-entity-list*

2.3 Usikkerhet

Eierskaps- og selskapsinformasjon er i all hovedsak basert på selskapers egenrapportering til myndigheter og offentligheten. Slik egenrapportering medfører en viss risiko for feilkilder, særlig av to årsaker:

- **Utdatert informasjon:** Informasjonen var korrekt ved registrering, men det har senere blitt gjort endringer som ikke er plukket opp. Dette kan eksempelvis skyldes manglende innmeldingsrutiner hos selskapet, eller at enkelte nasjonale registre ikke gjennomfører løpende oppdateringer.
- **Feilinformasjon:** Informasjonen er nylig oppdatert, men ukorrekt. Dette kan både være ubevisste misforståelser av regelverk, og bevisste handlinger for å f.eks. skjule reelle rettighetshavere. Her kan det også finnes mer komplekse tilfeller hvor informasjonen på papiret er korrekt, men hvor det kan virke som andre personer eller enheter utøver makt over de registrerte rettighetshaverne.

For å redusere usikkerhet har vi anvendt metodetriangulering, det vil si å sammenstille informasjon fra flere kilder, slik at vi har kunnet danne oss et mer sannsynlig bilde av eierskapet. Når data fra selskapsregistre, økonomiske rapporter og tredjepartsanalyser peker i samme retning kan vi med større sikkerhet trekke slutninger knyttet til eierskapet. Dette gir et mer pålitelig grunnlag for å forstå de reelle eierforholdene. En begrensning ved kartleggingen er at ulike kilder har informasjon på ulikt tidspunkt. Det kan være endringer i eierforhold etter siste tilgjengelige informasjon om eierskapet i det enkelte selskap. Dette er særlig en begrensning knyttet til det utenlandske eierskapet.

Det er viktig å understreke at det i enkelte tilfeller faktisk ikke er mulig å identifisere reelle eiere. Eksempelvis er har det i enkelte tilfeller vært krevende å finne informasjon om investorer i ulike typer investeringsfond. Tilsvarende har eierskap sporet til lavskatteland vært krevende å finne reelle rettighetshavere bak. I disse tilfellene har vi forsøkt å undersøke *hvorfor* det er krevende å kartlegge strukturene, slik at vi kan vurdere risikoprofilen til selskapet. Eksempelvis er det ofte skattemessige årsaker til at selskaper er registrert i land med lav transparens knyttet til eierforhold. I tillegg har vi brukt informasjon om siste eiertype og nasjonalitet til siste identifiserte eierledd inn i sammenstillingen av eierskapsinformasjon.

3 Om eiere av kritisk digital infrastruktur og deres leverandører

I dette kapittelet presenterer vi selskapene som eier og forvalter kritisk digital infrastruktur og deres leverandører. Først presenterer vi selskapene, før vi går nærmere inn på kjennetegnene til selskapene. For å få en idé om de økonomiske størrelsene, presenterer vi statistikk for selskapene samlet og gruppert etter relevante dimensjoner.

3.1 Selskapene som inngår i analysen

Analysene i denne rapporten baserer seg på selskapene som ekomsikkerhetsutvalget har identifisert som relevante eiere og forvaltere av kritisk digital kommunikasjonsinfrastruktur (kategori 1), og deres leverandører (kategori 2). Leverandører omfatter også entreprenører og leverandører som er av avgjørende betydning for utbygging, drift og vedlikehold av infrastrukturen. Leverandørene kan videre deles inn i to grupper. Den første gruppen er sentrale leverandører hvor vi har gjennomført en full kartlegging av eierskapet i selskapet (kategori 2A), på lik linje med eiere av infrastrukturen. Den andre består av selskap der det ultimate eierskapet vurderes å være av mindre interesse, og det derfor bare er gjort en kartlegging av eierskapet i norske aksjonærregistre (kategori 2B). Tabellen under oppsummerer antall selskap per kategori.

Tabell 3-1: Antall selskap fordelt på kategorier

Kategori	Antall
Kategori 1: Eiere og forvaltere av infrastruktur	35
Kategori 2: Leverandører	15
➔ **Kategori 2A**: Leverandører (full kartlegging)	9
➔ **Kategori 2B**: Leverandører (begrenset kartlegging)	6
Totalt	**50**

Det er en betydelig bredde i selskaper som eier og forvalter infrastrukturen. Det omfatter alt fra eiere av satellitter som Kongsberg Satellite Services AS til datasentre som Green Mountain AS, og fra store virksomheter som Telenor ASA som omsetter for titalls milliarder kroner hvert år, til mindre virksomheter som KystTele AS som omsetter for under 20 millioner kroner.

I tabellene under har vi listet opp selskapene som undersøkes med en kort beskrivelse av virksomheten. Tabell 3-2 viser eiere og forvaltere av kritisk digital infrastruktur (kategori 1), mens Tabell 3-3 viser leverandørene (kategori 2).

Tabell 3-2: Oversikt over eiere og forvaltere av kritisk digital infrastruktur

Selskap	Beskrivelse
Arelion Norway AS	Selskapet etablerer og driver telenett, både jordbundne og eterbaserte. Selskapet tilbyr også transmisjonstjenester og andre telekommunikasjonstjenester. Kilde: Brønnøysundregisteret
Bredbåndsfylket AS	Selskapet eier og drifter nettverk for kommunene i Troms og Finnmark, og yter tilknyttede tjenester. Kilde: Bredbåndsfylket

Bulk Infrastructure Holding AS	Selskapet etablerer, utvikler og drifter datasentre, fibernettverk og industrirelatert eiendom. Kilde: Bulk Infrastructure
De-Cix Management Gmbh	Selskapet er en internasjonal plattform som tilbyr operatør- og datasenternøytrale internett-utvekslinger. Kilde: De-Cix
Eidsiva Bredbånd AS	Selskapet bygger, selger og drifter bredbåndstjenester på Østlandet. Kilde: Eidsiva
Eviny Digital AS	Selskapets formål er å etablere og drifte bredbåndsinfrastruktur, samt drive virksomhet knyttet til dette. Kilde: Brønnøysundregisteret
Exa Infrastructure Norge AS	Exa Infrastructure er et internasjonalt konsern som forvalter digitale infrastrukturtjenester, inkludert fiberoptiske nettverk som støtter kommunikasjon på tvers av kontinenter. Selskapet forvalter blant annet infrastruktur som benyttes av De-Cix i Norge. Kilde: Exa Infrastructure / De-Cix
GlobalConnect AS	Selskapet eier og forvalter fibernettverk og tilbyr tilknyttede kommunikasjonsløsninger. Kilde: GlobalConnect
Green Mountain AS	Selskapet driver med datasentervirksomhet og relaterte aktiviteter. Kilde: Brønnøysundregisteret
Infrastructure Nordics 4 AS	Selskapet er morselskapet til de norske datasentrene som driftes av Stack Infrastructure. Kilde: Proff.no
Inmarsat Solutions AS	Selskapet tilbyr informasjons- og kommunikasjonsløsninger til skipsfartøy. Kilde: Brønnøysundregisteret
Ishavslink AS	Selskapet bygger ut, eier og drifter bredbåndsinfrastruktur i Finnmark, og driver virksomhet med naturlig tilknytning til dette. Kilde: Brønnøysundregisteret / Ishavslink
Kongsberg Satellite Services AS	Selskapet tilbyr bakkestasjonstjenester og infrastruktur for satellitter. Kilde: KSAT
KystTele AS	Selskapet eier, bygger og driver bredbåndsinfrastruktur og tilbyr tilknyttede tjenester. Kilde: Kysttele
Lefdal Mine Datacenter AS	Selskapet driver med datasentervirksomhet og relaterte aktiviteter. Kilde: Lefdal Mine
Lumen Technologies Norway AS	Selskapet tilbyr telekommunikasjonsløsninger og tilknyttede tjenester. Kilde: Brønnøysundregisteret
Lyse Tele AS	Selskapet representerer Lyse-konsernets televirksomhet. Selskapet har ansvar for utbygging av mobilnett, 5G og fiber, samt tilknyttede tjenester. Kilde: Lyse
N0r5ke Fibre AS	Selskapet investerer i, eier og leier ut optiske fiberkabler både nasjonalt og internasjonalt, og driver også investeringsvirksomhet ved å investere i og yte lån til selskaper innen disse virksomhetsområdene. Kilde: Brønnøysundregisteret
Nasjonal Referansedatabase AS	Selskapet driver med utvikling og drift av en nasjonal referansedatabase for porterte nummer, samt effektiviserende fellesløsninger for tilbydere og andre kunder innen eller med tilknytning til ekomnæringen. Kilde: Brønnøysundregisteret
Norid AS	Selskapet drifter registeret for norske domenenavn, og har ansvaret for toppdomenene .no, .sj, og .bv. Selskapet behandler søknader om abonnement på domenenavn. Kilde: Norid
NTE Telekom AS	Selskapet driver utbygging av fiberbredbånd og salg av fiberkapasitet og -innhold. Kilde: NTE
OneWeb Norway AS	Selskapet leverer satellittbaserte kommunikasjonstjenester. Kilde: OneWeb
Orange Business Digital Norway AS	Selskapet tilbyr digitale tjenester og tilknyttede konsulenttjenester til bedriftskunder. Kilde: Orange Business
Space Norway AS	Selskapet forvalter og videreutvikler sikkerhetskritisk og kostnadseffektiv romrelatert infrastruktur for å dekke viktige norske samfunnsbehov. Kilde: Brønnøysundregisteret
Space Norway Satcom AS	Selskapet driver med satellittbasert kommunikasjonsvirksomhet både i Norge og utlandet. Kilde: Brønnøysundregisteret
Stamfiber AS	Selskapet driver utleie av disposisjonsrett til mørk fiber og annet som står i naturlig forbindelse med dette. Kilde: Brønnøysundregisteret
Starlink Norway AS	Selskapet driver med satellittvirksomhet og tilknyttede aktiviteter. Kilde: Brønnøysundregisteret
Tampnet AS	Selskapet eier, opererer og utvikler kommunikasjonsnettverk, og tilbyr kommersielle kommunikasjonstjenester basert på sitt nettverk. Kilde: Brønnøysundregisteret
Telenor ASA	Selskapet er morselskapet i Telenor-konsernet, som tilbyr et bredt spekter av tjenester telekommunikasjonsvirksomhet og tilknyttede områder. Kilde: Brønnøysundregisteret / Telenor

Telenor Fiber AS	Selskapet driver med utbygging og utleie av fiberinfrastruktur og tilhørende virksomhet, men det skal ikke ha tilgang til informasjon om sluttbrukere eller annen skjermingsverdig informasjon om infrastrukturen. Kilde: Brønnøysundregisteret
Telenor Towers Norway AS	Selskapet forvalter og leier ut plass i master, tårn og annen passiv infrastruktur. Kilde: Telenor Towers
Telia Norge AS	Selskapet driver med elektronisk kommunikasjonsvirksomhet, inkludert utbygging, drift og vedlikehold av landsdekkende data-, tele- og TV-distribusjonsnett, samt produksjon og levering av lyd, bilder og elektroniske signaler, inkludert digital TV, og innholdsproduksjon for distribusjon i disse nettverkene, i tillegg til annen relatert virksomhet. Kilde: Brønnøysundregisteret
Telia Towers Norway AS	Selskapet driver med drift av og tilbyr plass i master, tårn og lignende strukturer for trådløs mobilteknologi. Kilde: Brønnøysundregisteret / Telia Towers
Tårnselskapet AS	Selskapet eier, drifter og leier ut plass i tårn og annen infrastruktur til mobiloperatører og andre selskaper som trenger tilgang til høydemaster for å bygge ut sine nettverk og tjenester. Selskapet er en del av Lyse-konsernet. Kilde: Lyse
Viken Fiber AS	Selskapet bygger og drifter fibernett på Østlandet. Kilde: Viken Fiber

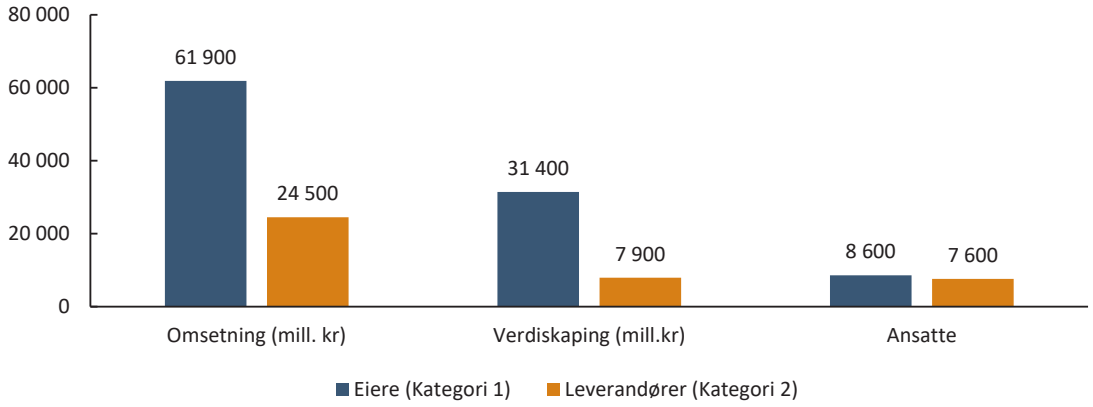
Tabell 3-3: Oversikt over leverandører til kritisk digital infrastruktur

Selskap	Beskrivelse	Type kartlegging
Caverion Norge AS	Selskapet er en teknisk totalleverandør for bygg og industri, med fokus på smarte og bærekraftige løsninger. Kilde: Caverion	Fullstendig
Cisco Systems Norway AS	Selskapet tilbyr produkter og tjenester knyttet til datamaskiner (hardware og software). Kilde: Brønnøysundregisteret	Begrenset
Eltel Networks AS	Selskapet driver med bygg, drift og vedlikehold av kritisk infrastruktur innen energi og telekommunikasjon. Kilde: Eltel	Fullstendig
Ericsson AS	Selskapet leverer nettverksutstyr og -tjenester. Kilde: Ericsson	Begrenset
Huawei Technologies Norway AS	Selskapet leverer utstyr, løsninger og tjenester innen IT og telekommunikasjon. Kilde: Brønnøysundregisteret	Begrenset
Juniper Networks Norway AS	Selskapet driver med salg, markedsføring og tjenester innen IT, data og telekommunikasjon. Kilde: Brønnøysundregisteret	Begrenset
Netel AS	Selskapet bygger og vedlikeholder infrastruktur for tele- og datakommunikasjon. Kilde: Netel	Fullstendig
Nexans Norway AS	Selskapet driver med utvikling, produksjon og markedsføring av kabler og kablingssystemer, inkludert kraft- og telekabler. Kilde: Nexans	Fullstendig
Nokia Solutions and Networks Norge AS	Selskapet driver med telekommunikasjon og elektronisk industri, inkludert implementering av systemer og tjenester som nettverksplanlegging, vedlikehold, brukerstøtte og konsulenttjenester. Kilde: Brønnøysundregisteret / Palo Alto Networks	Begrenset
OneCo Networks AS	Selskapet driver med svakstrøm- og sterkstrøminstallasjon, prosjektering, samt forvaltning av andeler i selskaper med lignende formål. Kilde: Brønnøysundregisteret	Fullstendig
Palo Alto Networks (Norway) AS	Selskapet er en del av det internasjonale konsernet Palo Alto Networks, som tilbyr cybersikkerhetsprodukter og tilhørende tjenester. Kilde: Brønnøysundregisteret	Begrenset
Prysmian Group Norge AS	Selskapet utvikler og produserer kabler til en rekke segmenter, inkludert datakabler, telekom og fiber. Kilde: Prysmian	Fullstendig
Seaworks AS	Selskapet driver med bulktransport og sjøkabeltjenester. Kilde: Seaworks	Fullstendig
Seaworks Management AS	Selskapet forvalter personell hos Seaworks AS, som driver med bulktransport og sjøkabeltjenester. Kilde: Seaworks	Fullstendig
Site Service AS	Selskapet installerer, drifter og vedlikeholder fiber-, elektro-, tele- og kommunikasjonsnettverk. Kilde: Site Service	Fullstendig

3.2 Selskapenes økonomiske størrelse

Selskapene som undersøkes spenner seg fra mindre, lokale aktører til store, internasjonale konserner. Eiere av, og leverandører til, kritisk digital kommunikasjonsinfrastruktur hadde i 2023 en samlet omsetning på 86 milliarder kroner og 39 milliarder kroner i verdiskaping. Selskapenes verdiskaping utgjør derved 1,1 prosent av norsk fastlands-BNP. Videre sysselsetter selskapene samlet 16 200 arbeidstakere, som utgjør 0,9 prosent av sysselsetting i norsk næringsliv. Figuren under viser hvordan selskapenes omsetning, verdiskaping og antall ansatte fordeler seg på eiere og forvalter av infrastruktur og leverandører i 2023.

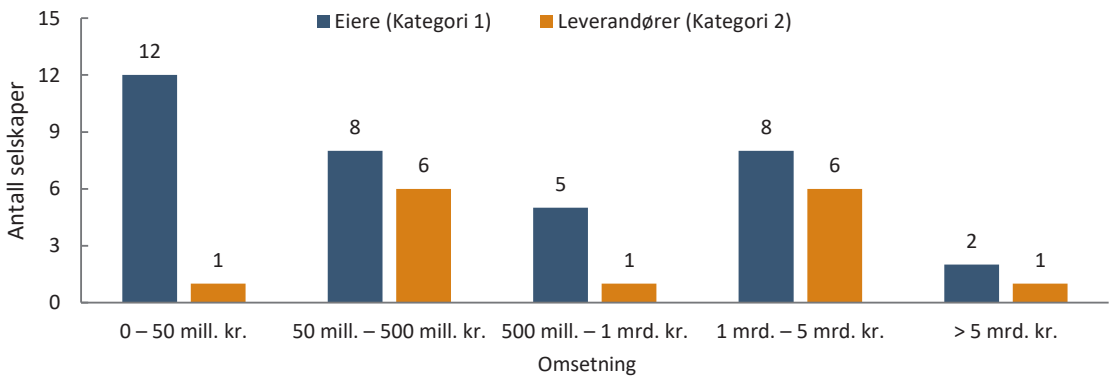
Figur 3-1: Omsetning, verdiskaping og antall ansatte fordelt på eiere og forvaltere av infrastruktur og leverandører i 2023. Kilde: Menon Economics



Eiere av infrastrukturen stod for majoriteten av omsetning og verdiskaping, med henholdsvis 72 og 80 prosent av totalen for alle selskapene. Når det kommer til sysselsetting stod leverandørene for nesten halvparten, som illustrerer at både omsetning og verdiskaping per ansatt er langt høyere blant eiere av infrastrukturen enn for leverandørene.

Telenor ASA og Telia Norge AS er de klart største aktørene blant selskapene. Disse to selskapene står alene for nær halvparten av verdiskapingen og omsetningen blant selskapene. Med to så store og dominerende aktører, er det hensiktsmessig å se hvordan selskapene fordeler seg på ulike størrelseskategorier. I de to påfølgende figurene nedenfor viser vi hvordan antall selskaper som henholdsvis eier og er leverandører til digital nasjonal kommunikasjonsinfrastruktur fordeler seg etter størrelse på omsetning og ansatte.

Figur 3-2: Fordeling av selskaper etter størrelse på omsetning i 2023. Kilde: Menon Economics

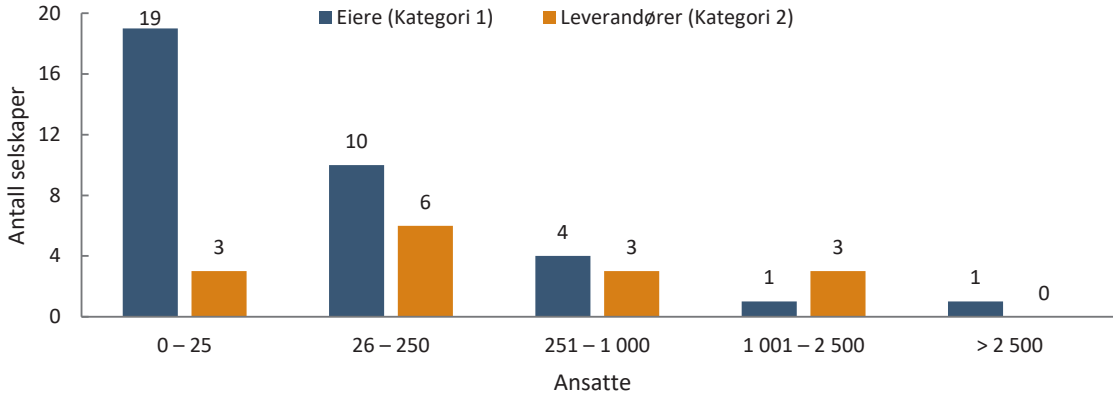


Blant eiere av infrastruktur er det relativt god spredning blant selskapene. 12 selskaper har mindre med mindre enn 50 millioner kroner i omsetning, og man finner mellom fem og åtte selskap i hver størrelseskategori fra 50 millioner kroner til fem milliarder kroner i omsetning. I gruppen med mer enn fem milliarder kroner i omsetning finner vi nevnte Telenor ASA og Telia Norge AS.

Blant leverandører finner vi kun ett selskap med mindre enn 50 millioner i omsetning. 12 av 15 selskaper har enten mellom 50-500 millioner kroner eller én til fem milliarder kroner i omsetning. Det eneste selskapet med mer enn fem milliarder kroner i omsetning er Nexans Norway AS, som har 10,7 milliarder kroner i omsetning i 2023. Det betyr at Nexans Norway AS alene utgjør 44 prosent av omsetningen blant leverandørene.

Fire eiere av infrastruktur har negativ verdiskaping[4], og ytterligere 13 har under 50 millioner kroner i verdiskaping (se Vedlegg B: Figurer). Til sammen 12 eiere har mellom 50 millioner og 1 milliard kroner i verdiskaping. Seks eiere har over én milliard kroner i verdiskaping, hvorav to har mer enn fem milliarder kroner i verdiskaping. Blant leverandørene er det kun to av selskapene som har under 50 millioner kroner i verdiskaping, og over halvparten, åtte selskaper, er i intervallet mellom 50 og 500 millioner kroner. To selskap har mellom 500 millioner og 1 milliard kroner i omsetning, mens resterende tre selskaper har mellom én og fem milliarder kroner i verdiskaping. Disse tre selskapene er Caverion Norge AS, Cisco Systems Norway AS og Nexans Norway AS.

Figur 3-3: Fordeling av selskaper etter antall ansatte i 2023. Kilde: Menon Economics



De fleste eiere av infrastruktur har færre enn 25 ansatte, og 12 av selskapene har ingen ansatte overhodet. Dette er typisk selskaper som er satt opp for å forvalte eierskapet til infrastrukturen, men ikke drifte den. Ytterligere ni av eierne har mellom 21 og 250 ansatte, mens kun fire har mellom 251 og 1 000 ansatte. Telenor ASA og Telia Norge AS er eneste selskaper med mer enn 1 000 ansatte.

Blant leverandører er det kun tre selskaper har under 25 ansatte. Seks leverandører har mellom 26 og 250 ansatte, mens de resterende 6 leverandørene fordeler seg likt på kategoriene 251 til 1 000 ansatte og 1 000 til 2 500 ansatte.

Det er verdt å merke at ettersom dette er et begrenset utvalg selskap som knyttes direkte til den kritiske digitale infrastrukturen, kan mål på omsetning, verdiskaping og ansatte være noe misvisende. Dette gjelder særlig selskaper som er en del av større konsern med aktivitet i utlandet. I slike tilfeller kan ansatte eller omsetning

[4] Det innebærer at EBITDA, som er sum av driftsresultat, avskrivninger og nedskrivninger, er negativt og større i absoluttverdi enn lønnskostnader.

være registrert på andre deler av konsernet. For eksempel er 13 eiere og leverandører registrert med null ansatte i Norge i 2023. For enkelte av selskapene er dette reelt fordi de er helt nyopprettede eller fordi det ikke er drift i selskapet, men for de fleste skyldes dette at de ansatte er registrert i en annen norsk eller utenlandsk enhet.

Et alternativ ville vært å legge aktivitet fra konsernregnskap til grunn i analysene, men dette vurderes som lite hensiktsmessig da det er nettopp de identifiserte underenhetene som jobber direkte opp mot norsk digital infrastruktur. Å fokusere på underenhetene slik vi har valgt å gjøre gir dermed mer presis informasjon om de relevante aktørene, men kan på den andre siden medføre at enkelte skjevheter ettersom vi ikke får med den all relevant aktivitet for enkelte av selskapene.

3.3 Øvrige kjennetegn ved virksomhetene

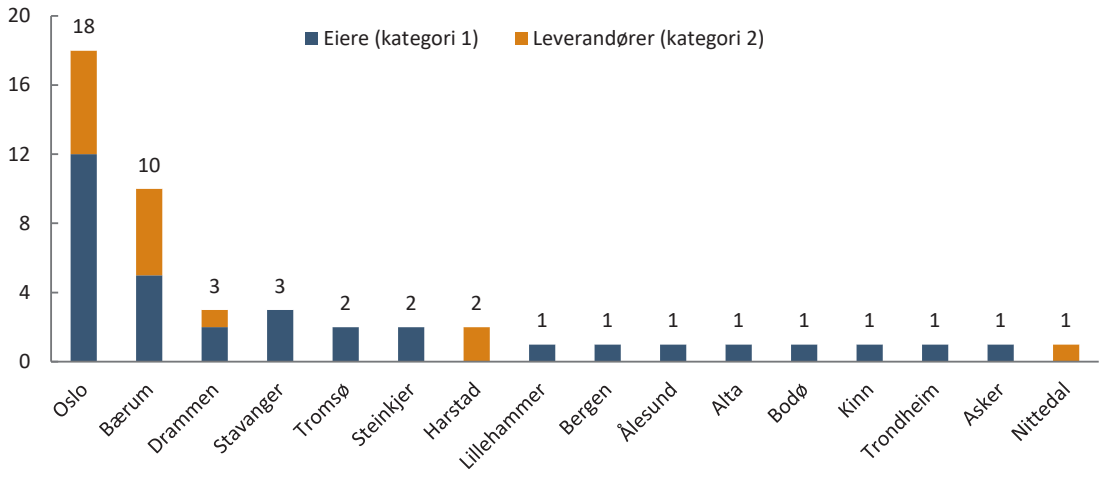
3.3.1 Selskapsform

Samtlige selskap er aksjeselskap, med unntak av Telenor ASA som er allmennaksjeselskap[5] og De-Cix Management Gmbh[6], som er et tysk selskap som tilsvarer den norske selskapsformen aksjeselskap.[7]

3.3.2 Geografisk fordeling

Alle selskapene er norskregistrerte, med unntak av De-Cix Gmbh, som er registrert i Tyskland. I figuren under viser vi hvordan de norske hovedkontorene til selskapene fordeler seg på kommuner. De fleste har hovedkontor på det sentrale Østlandet – de som er lokalisert i resten av landet består særlig av lokale infrastrukturselskaper som er eid av kommuner og fylker. Det gjelder eksempelvis Eidsiva Bredbånd AS, Eviny Digital AS og Brebåndsfylket AS.

Figur 3-4: Fordeling av selskapene etter det norske hovedkontorets lokasjon, fordelt mellom eiere av infrastruktur og leverandører. Kilde: Menon Economics



[5] *Et allmennaksjeselskap (ASA) er en norsk selskapsform som betegner et børsnotert selskap der hvem som helst kan kjøpe aksjer og bli medeier.*
[6] *Gesellschaft mit beschränkter Haftung, vanligvis forkortet GmbH, er tysk for «selskap med begrenset heftelse»*
[7] *De-Cix Management Gmbh er et norskregistrert utenlandsk foretak (NUF)*

Totalt har 29 selskaper, eller 60 prosent av selskapene, hovedkontor i Oslo, Bærum eller Drammen. Øvrige kommuner hvor to av selskapene har hovedkontor er Harstad, Stavanger, Steinkjer og Tromsø, som alle er regionale sentra. Ytterligere ni kommuner har hovedkontor for ett selskap som enten eier infrastruktur eller deres leverandører.

3.3.3 Styremedlemmers nasjonalitet

Som en del av analysen har vi kartlagt styremedlemmers nasjonalitet i både selskapene som eier og forvalter infrastrukturen og deres leverandører, samt i konsernene disse selskapene inngår i der dette er relevant. Sistnevnte gruppe gjelder først og fremst norske datterselskap som inngår i utenlandske konsern.

Styremedlemmenes nasjonalitet er kartlagt ved hjelp av både styreinformasjon som Menon besitter for norske selskap, supplert med informasjon om nasjonalitet fra Orbis og i enkelte tilfeller offentlige kilder på nett som selskapenes hjemmesider og årsrapporter.

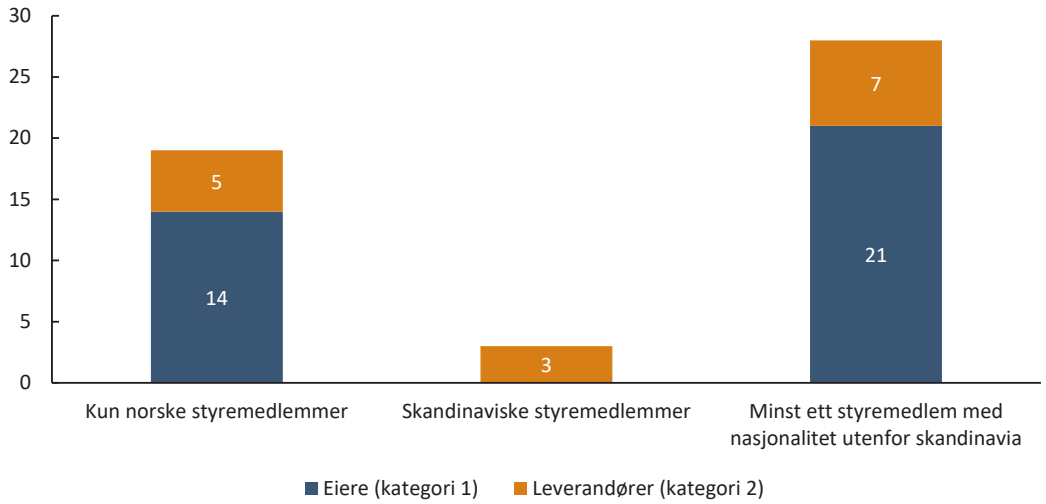
Styremedlemmer i eiere og forvaltere av infrastruktur og deres leverandører

Antall styremedlemmer varierer betydelig mellom selskapene, der ett selskap kun har ett styremedlem, til Telenor ASA som har 10 styremedlemmer. Vi presenterer derfor først statistikk der vi har kategorisert på selskapsnivå basert på styresammensetningen, før vi presenterer statistikk på antall styremedlemmer fordelt på nasjonalitet.

I figuren under har vi kategorisert selskapene etter hvorvidt de utelukkende har norske styremedlemmer, om de har skandinaviske styremedlemmer eller om de har innslag av nasjonaliteter utenfor Skandinavia i styret. 17 av selskapene har utelukkende norske styremedlemmer, mens 3 selskap har innslag av skandinaviske styremedlemmer utenom Norge. Til sammen utgjør disse to gruppene 42 prosent av selskapene. I de tilfellene det ikke har vært mulig å oppdrive sikker informasjon om nasjonalitet, har styremedlemmet blitt tildelt nasjonalitet basert på bosted, arbeidssted, fødested og/eller utdanningssted.[8]

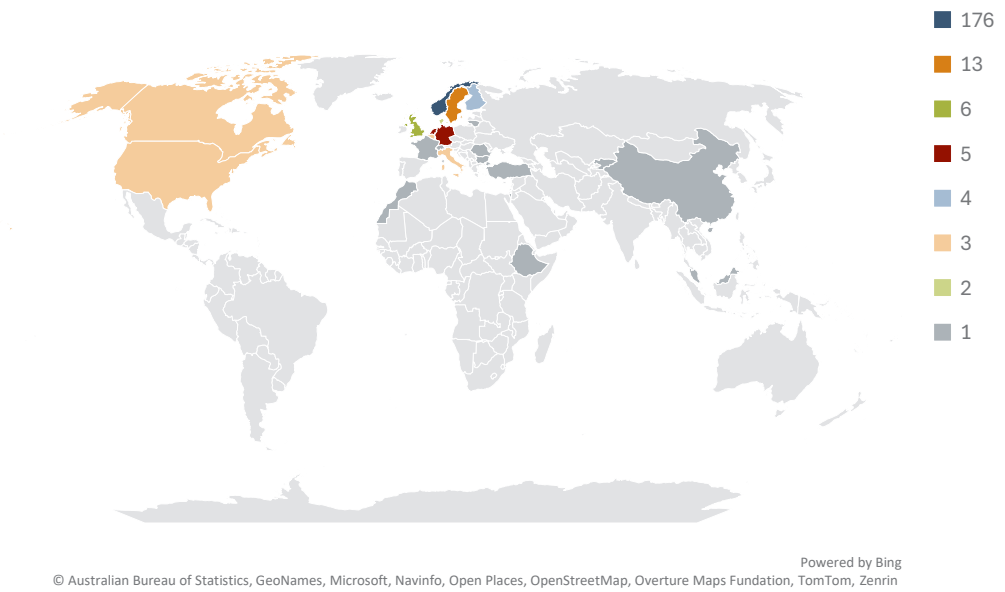
[8] *Dette gjelder kun et fåtall personer –39 av totalt 484 kartlagte styremedlemmer.*

Figur 3-5: Antall selskaper etter sammensetning av nasjonaliteter i selskapets styre. Kilde: Menon Economics og Orbis



Figuren over viser at 28 selskaper, eller 56 prosent av de kartlagte, har innslag av styremedlemmer med nasjonaliteter fra utenfor Skandinavia. Som vist i kartet under er styremedlemmer utenfor Skandinavia først og fremst fra Europa eller Nord-Amerika, med kun noen få unntak. Unntakene fra Europa og Nord-Amerika er styremedlemmer fra Etiopia, Israel, Kina, Kirgisistan, Malaysia, Marokko og Tyrkia.

Figur 3-6: Fordeling av antall styremedlemmer på stater. Kilde: Menon Economics og Orbis

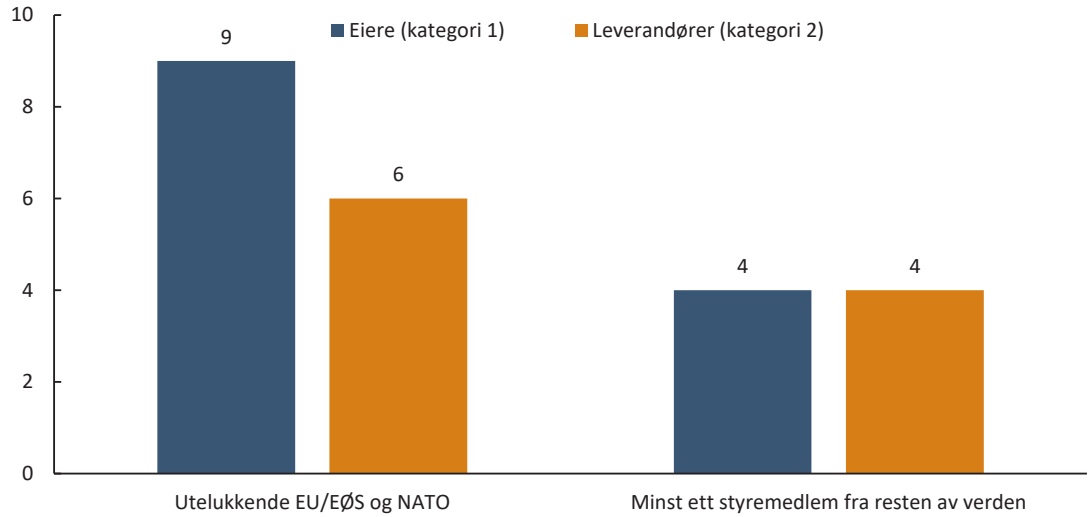


Styremedlemmer i konsern hvor eiere og forvaltere av infrastruktur og deres leverandører inngår

I tillegg til å undersøke styremedlemmene i selskapene som eier kritisk digital kommunikasjonsinfrastruktur og deres leverandører, har vi undersøkt styremedlemmene i morselskap i eierkjeden til disse selskapene.[9] Det er 23 av 50 selskap som har et morselskap hvor vi har kartlagt nasjonalitet på styremedlemmene i eierselskapet. Dette er i de fleste tilfeller øverste ledd i internasjonale konsern.

I figuren under har vi kategorisert morselskapene etter hvorvidt de utelukkende har styremedlemmer fra EU/EØS og NATO-medlemmer, eller om de har minst et styremedlem fra resten av verden.

Figur 3-7: Antall selskap etter sammensetning av nasjonaliteter i morselskapets styre. Kilde: Menon Economics og Orbis

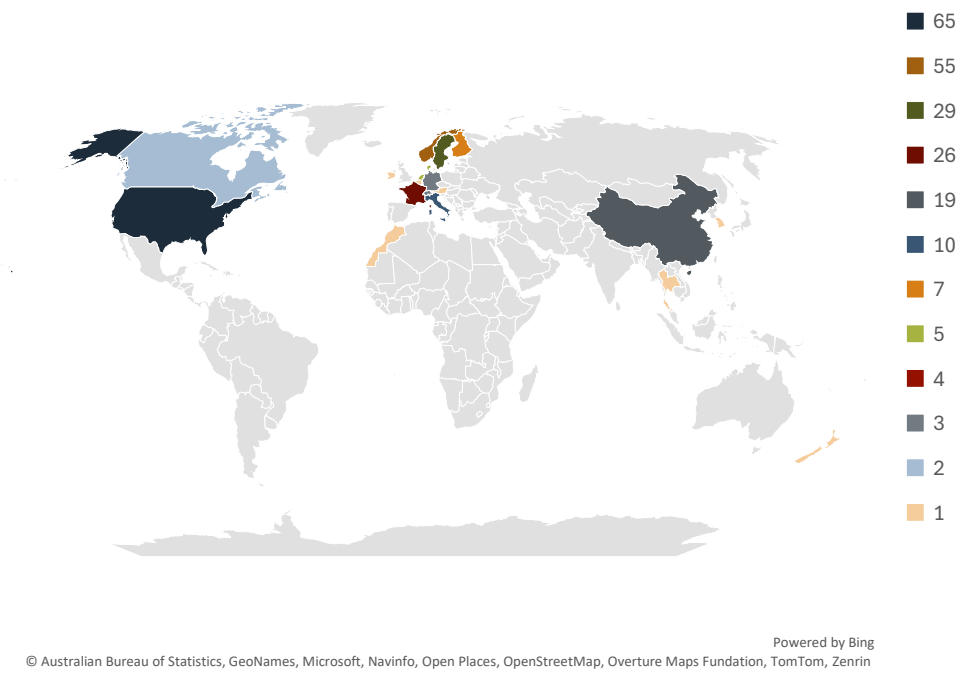


Omtrent 65 prosent av de kartlagte morselskapene har utelukkende styremedlemmer fra EU/EØS- og NATO-land. Dette gjelder flere eiere enn leverandører. Like mange eiere og leverandører har morselskap med minst ett styremedlem fra resten av verden.

Figuren under viser hvordan styremedlemmene i morselskapene fordeler seg på land. Det er flest styremedlemmer i USA og Norge, etterfulgt av Sverige, Frankrike, Kina og Storbritannia. Blant land utenfor Europa og Nord-Amerika, er Chile, Marokko, Thailand, Sør-Korea, New Zealand og Singapore representert.

[9] Vi har brukt informasjon om global ultimat eier, som er det øverste leddet i eierkjeden med kjent majoritetseierskap.

Figur 3-8: Fordeling av antall styremedlemmer i morselskap på stater. Kilde: Menon Economics og Orbis



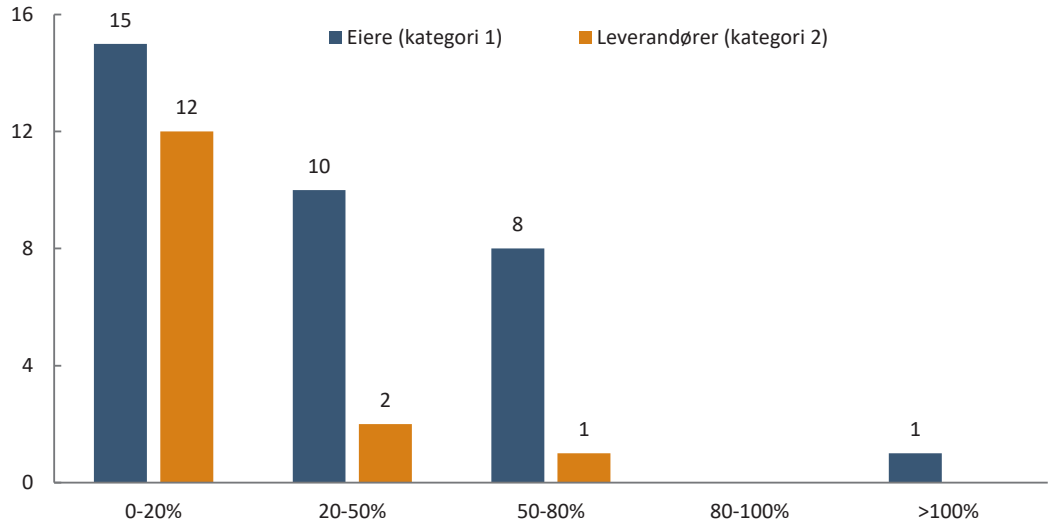
3.3.4 Gjeld og gjeldsgrad

I tillegg til eierskapsstrukturer har vi også sett på gjelden til de norske selskapene. Dette er gjort fordi gjeld har potensiell stor innvirkning på beslutningstaking, investeringsevne og risikoeksponering. For det første kan høye gjeldsgrader kan føre til økt sårbarhet ved økonomiske nedgangstider eller renteendringer, noe som kan påvirke driften av den kritiske infrastrukturen negativt. For det andre kan høy gjeld gi kreditorer en betydelig påvirkningskraft over selskapets strategi, spesielt dersom gjelden er underlagt internasjonale finansinstitusjoner. Med andre ord kan gjeld øke eksponering og risiko i forbindelse med utenlandsk eierskap. Til slutt er det et viktig poeng at kreditorer har større makt ved insolvens og konkurs, og at gjeldsstrukturen derfor er en viktig indikator på hvem som i realiteten har kontroll over selskapet. Om et selskap går konkurs er det nemlig som utgangspunkt kreditorene som overtar eierskapet til de resterende aktiva i selskapet.

Det er imidlertid begrenset offentlig informasjon om kreditorer i selskapene vi ser på her. Vi har likevel innhentet data på gjeldsgrad[10] i selskapene for å gi innsikt i gjeldssituasjonen og kontroll, samt risiko knyttet til selskapets drift og evne til å opprettholde samfunnskritiske funksjoner. Vi har beregnet gjeldsgrad på selskapsnivå, og ikke for konsernene som selskapene eventuelt inngår i. Figuren under viser hvordan selskapene fordeler seg på ulike nivåer av gjeldsgrad.

[10] *Gjeldsgraden er beregnet som langsiktig gjeld delt på eiendeler.*

Figur 3-9: Antall selskaper fordelt etter gjeldsgrad og eiere/leverandører i 2023. Kilde: Menon Economics



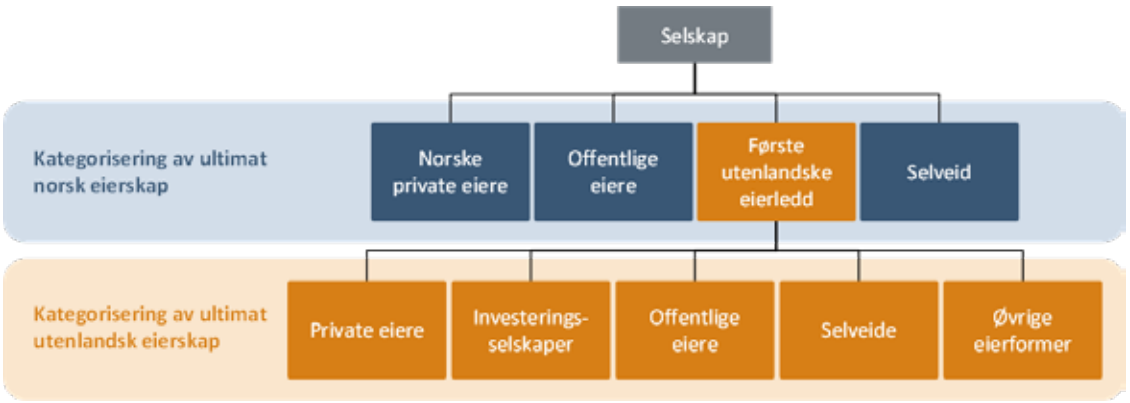
Som vi ser av figuren, har de fleste selskapene relativt lav gjeldsgrad. 43 prosent av eiere og 80 prosent av leverandører har gjeldsgrad under 20 prosent. Det er imidlertid åtte eiere og én leverandør som har relativt høy gjeldsgrad på mellom 50 og 80 prosent. I tillegg har én eier av infrastruktur en gjeldsgrad på over 100 prosent, som innebærer en negativ egenkapital. Selskapet dette gjelder er Exa Infrastructure Norge AS.

4 Eierskap i kritisk digital kommunikasjonsinfrastruktur

I dette kapittelet kartlegger vi ultimate eiere i selskaper innen kritisk digital infrastruktur, med fokus på både norske og utenlandske eiere. Utenlandsk eierskap dominerer, og er mer utbredt i kritisk digital kommunikasjon enn i norsk næringsliv generelt. Offentlig eierskap er også mer utbredt i disse selskapene. En betydelig del av eierskapet består av småaksjonærer uten vesentlig innflytelse, særlig i børsnoterte selskaper som Telenor og Telia. De ultimate eierskapene spores ofte tilbake til Norden, EU/EØS eller NATO-land, med betydelig eierskap fra land som Sverige og USA.

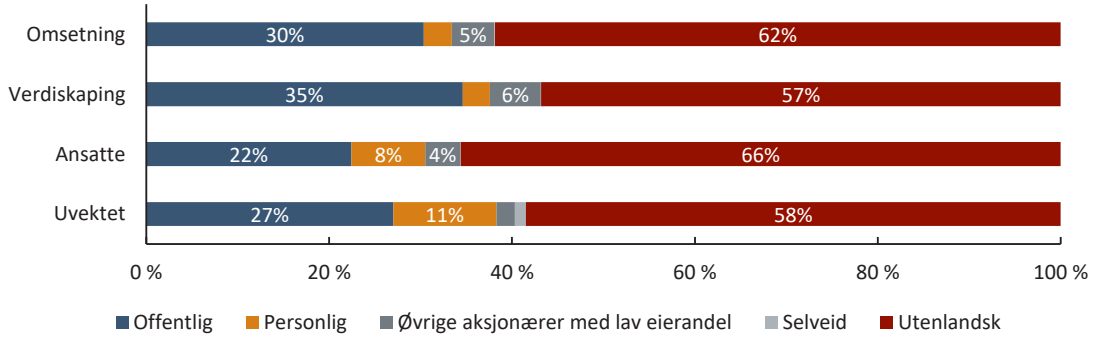
Alle selskapene som er omtalt i denne rapporten har fått kartlagt sitt *ultimate norske eierskap.* Dette inkluderer eierskap som kan spores tilbake til en ultimat norsk eier, eller til første utenlandske eierledd. I tillegg har vi gjennomført en tilnærmet fullstendig kartlegging av eierskapet i alle selskap som er definert som eier eller forvalter av kritisk digital infrastruktur, samt for utvalgte leverandører.[11] Figuren under illustrerer hvordan de ultimate eierne kategoriseres i disse to prosessene.

Figur 4-1: Illustrasjon av kategorisering av norsk og utenlandsk eierskap



I figuren under vises kategoriseringen av ultimat norsk eierskap for alle selskapene i kartleggingen.

Figur 4-2: Fordeling av eierskap for alle selskap i 2023, etter vekting. Kilde: Menon Economics



[11] *Vi har kartlagt alle effektive eierandeler over 5 prosent, samt de fleste eierandeler over 2 prosent i børsnoterte selskaper.*

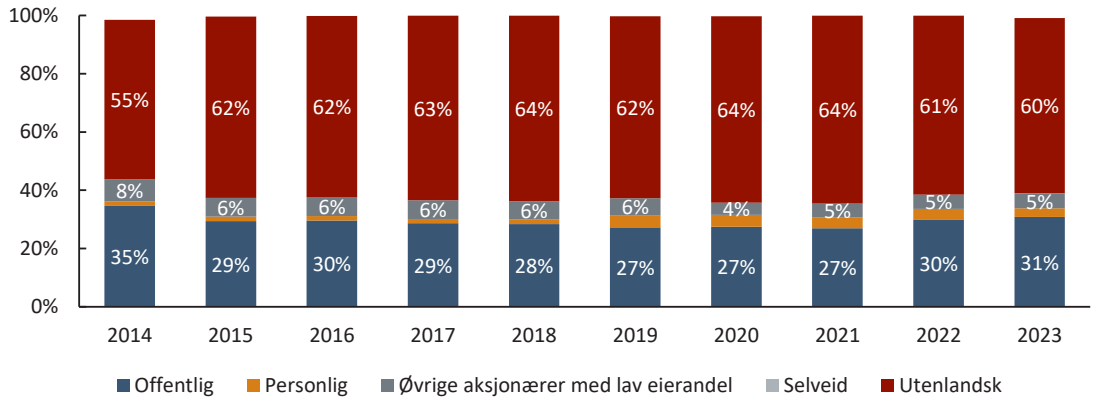
Figuren over viser at en vesentlig andel av eierskapet i selskapene utenlandsk. Den videre kategoriseringen av dette eierskapet omtales nærmere for selskapene i henholdsvis Kategori 1 og Kategori 2 i kapittel 4.1 og 4.2. Der gjennomgår vi også andre overordnede funn, før vi gir en kort beskrivelse av eierskapet i hvert selskap.[12] Ettersom færre av selskapene i kategori 2 har blitt kartlagt utover det norske ultimate eierskapet, vil omtalen her være mindre omfattende enn for kategori 1.

Når vi ser på eierskapet i kritisk digital kommunikasjonsinfrastruktur under ett (både kategori 1 og 2), så er utenlandsk eierskap svært utbredt sammenlignet med eierskapet i norsk næringsliv som helhet. I kartleggingen av eierskapet i norsk næringsliv finner Menon (2023)[13] at 36 prosent av næringslivet er eid av utenlandske eiere, mens for kritisk digital kommunikasjonsinfrastruktur er tilsvarende tall om lag 55 prosent.[14]

Tilsvarende er offentlig eierskap langt mer utbredt i kritisk digital infrastruktur, sammenlignet med eierskapet i øvrige næringsliv. Vår analyse viser at det offentlige (norske og utenlandske myndigheter) eier nesten halvparten av selskapene kartlagt her, men det offentlige eide 22 prosent av norsk næringsliv i 2021 (omfatter kun eierskapet til den norske stat)[15]. En naturlig forklaring på at offentlig eierskap er utbredt, er at det er svært kapitalkrevende å bygge ut infrastrukturen, samtidig som det er samfunnskritisk. Av samme årsaker er privat eierskap mindre utbredt for disse selskapene, sammenlignet med næringslivet som helhet.

En stor utfordring med slike eierskapskartlegginger, er at de først og fremst gir et øyeblikksbilde av hvordan eierskapet ser ut akkurat nå, og det finnes ingen garanti mot at det ikke kan gjøres vesentlige endringer i eierskapet til enkeltselskaper på kort tid. Figuren under viser hvordan fordelingen av ultimat eierskap har variert mellom 2014 og 2023.

Figur 4-3: Historisk fordeling av ultimat eierskap i alle selskapene som kartlegges, vektet etter omsetning. Kilde: Menon Economics



Som figuren viser, er det lite som endrer seg i fordelingen av ultimat eierskap på tvers av selskapene over tid. I hele perioden mellom 2014 og 2023 er majoriteten av det ultimate eierskapet i utlandet, etterfulgt av norsk offentlig eierskap. Den noe større økningen i utenlandsk eierskap mellom 2014 og 2015 skyldes primært en fusjon

[12] I underlagsmaterialet som følger med denne rapporten finner man utfyllende eierskapsinformasjon for alle kartlagte selskaper.
[13] Menon Economics (2023). Privat eierskap i Norge 2021
[14] Tallet omfattet eierskap i norsk næringsliv i 2021 og er vektet etter verdiskaping. Det forventes at andelen ikke er endret vesentlig fra 2021 til 2023.
[15] Menon Economics (2023). Privat eierskap i Norge 2021

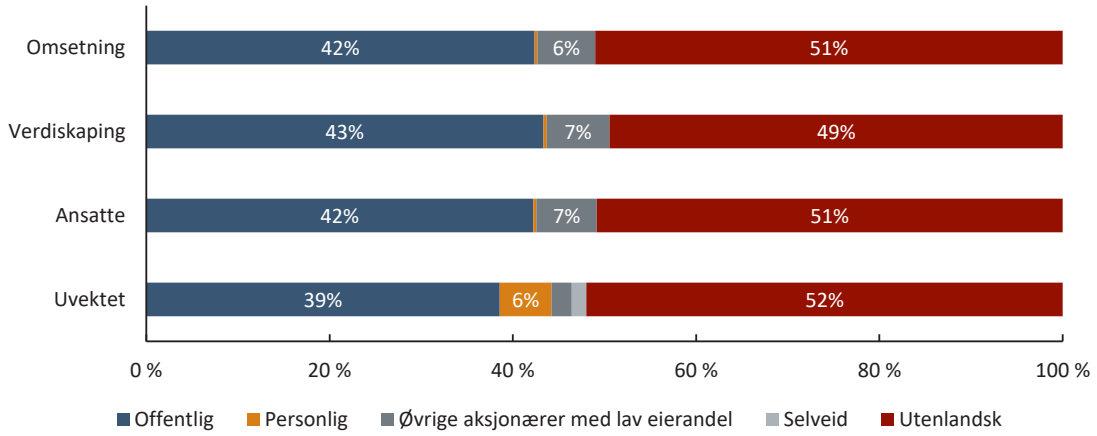
mellom Telia (tidl. NetCom) og Tele2 Norge, og dermed en vekst i registrert omsetning i selskapet. Endringen skyldes altså ikke reelle endringer i eierskap.

4.1 Eierskap i selskaper som eier eller forvalter kritisk digital kommunikasjons-infrastruktur

4.1.1 Overordnet om eierskapet

Selskapene i denne kategorien har alle gjennomgått en omfattende kartlegging for å avdekke ultimate eiere. I figuren under viser vi en overordnet fordeling av eierskapet i selskapene i kategori 1.

Figur 4-4: Fordeling av eierskap blant eiere og forvaltere (kategori 1), etter vekting. Kilde: Menon Economics



Som figuren viser, er majoriteten av selskapene eid av utenlandske eiere eller norske offentlige eiere. Omfanget av norsk personlig eierskap og øvrige småaksjonærer[16] er begrenset. En fordeling av eierskapet i hvert enkelt selskap vises i vedlegg C.

Som det fremgår av figuren over, er fordelingen av eierskap lite sensitiv for om man måler det som andel av verdiskaping, omsetning eller ansatte. Unntaket er dersom man vekter alle selskaper likt; da blir personlig eierskap større, på bekostning av de øvrige aksjonærene med lave eierandeler. Dette indikerer at personlig eierskap er mer fremtredende i mindre selskap. Videre er det de større selskapene som har større grupper av aksjonærer med små eierandeler. Dette gjelder særlig for Telenor ASA og Telia AS. Telenor er børsnotert og Telia AS er heleid av børsnoterte Telia AB, og det er en betydelig andel av begge selskapene som eies av aksjonærer med mindre enn to prosent eierandel.

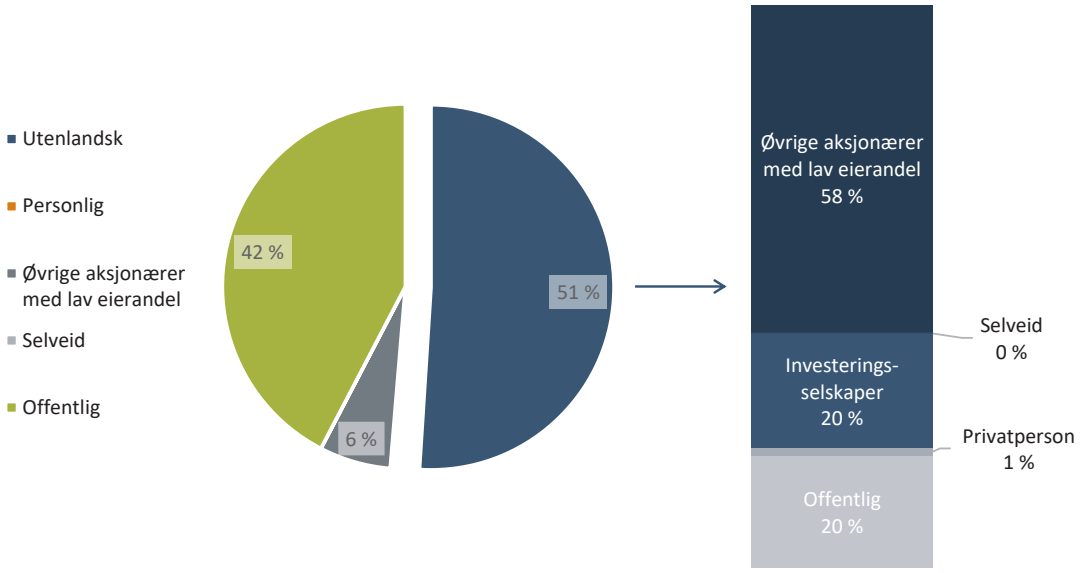
Ettersom vi har flere tilfeller av selskaper i samme konsern, vil et uvektet snitt også gi en «dobbelttelling» av de ultimate eierne i disse selskapene. Ved å vekte eierskapet etter omsetning, verdiskaping eller antall ansatte i hvert enkelt selskap unngår vi dermed denne dobbelttellingen. I de påfølgende figurene vekter vi selskapene

[16] *Når eierskapet kartlegges, tas det i hvert eierledd utgangspunkt i de 20 største aksjonærene. Øvrige aksjonærer (som dermed har < 5 % eierskap) inngår i kategorien «øvrige aksjonærer med lav eierandel».*

etter omsetning, da vi anser dette som det mest hensiktsmessige målet for kunne å sammenlikne selskapene på tvers.

Vi har videre kartlagt det utenlandske eierskapet i selskapene. Den overordnede fordelingen av dette eierskapet vises i figuren under.

Figur 4-5: Fordeling av ultimat utenlandsk eierskap blant eiere og forvaltere (kategori 1), vektet etter omsetning. Kilde: Menon Economics



Som figuren viser, består majoriteten av det utenlandske eierskapet av aksjonærer med små eierandeler. Dette kommer av at enkelte selskaper vil ha svært mange indirekte eiere med veldig små eierandeler hver og gjelder særlig de som er børsnoterte eller hvor en betydelig andel eies av et børsnotert selskap. Det samme kan også gjelde for selskap som er helt eller delvis eid av investeringsselskap eller enkeltfond, avhengig av hvordan investorene er fordelt. Ettersom disse mindre eierandelene i praksis ikke gir noen nevneverdig innflytelse på selskapene vi undersøker, har det ikke vært hensiktsmessig å kartlegge disse eierskapene videre. Til sammen utgjør likevel disse mindre eierne en betydelig andel av det samlede utenlandske eierskapet fordi flere av de største selskapene vi undersøker (slik som Telenor, Telia og Nexans) er børsnoterte eller inngår i børsnoterte konsern.

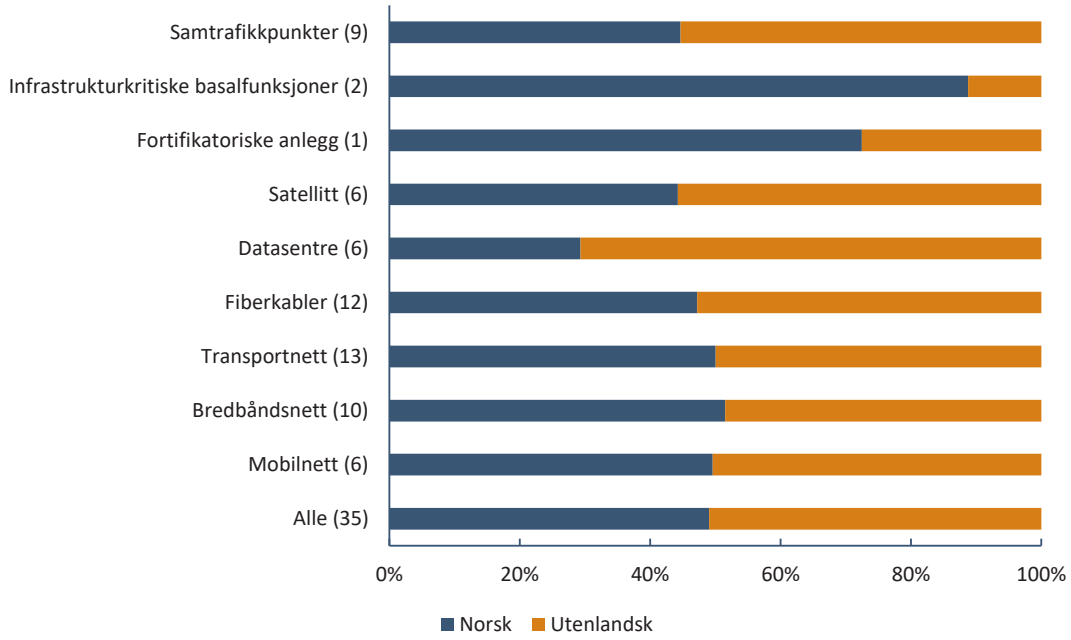
Selskapene opererer innenfor flere ulike segmenter innen kommunikasjonsinfrastruktur. Selskapene er fordelt på følgende vis (merk at hvert selskap kan være kategorisert i flere infrastrukturkategorier):

- **Samtrafikkpunkter:** Bulk Infrastructure Holding AS, De-Cix Management Gmbh, Exa Infrastructure Norge AS, GlobalConnect AS, Infrastructure Nordics 4 AS, Lyse Tele AS, Orange Business Digital Norway AS, Telenor ASA, Telia Norge AS
- **Infrastrukturkritiske basalfunksjoner:** Nasjonal Referansedatabase AS, Norid AS
- **Fortifikatoriske anlegg:** Telenor Towers Norway AS
- **Satellitt:** Inmarsat Solutions AS, Kongsberg Satellite Services AS, OneWeb Norway AS, Space Norway AS, Space Norway Satcom AS, Starlink Norway AS

- **Datasentre:** Bulk Infrastructure Holding AS, Infrastructure Nordics 4 AS, Orange Business Digital Norway AS, Eidsiva Bredbånd AS, Green Mountain AS, Lefdal Mine Datacenter AS
- **Fiberkabler:** Bulk Infrastructure Holding AS, Space Norway AS, Telenor ASA, GlobalConnect AS, Lyse Tele AS, Telia Norge AS, Arelion Norway AS, Lumen Technologies Norway AS, NTE Telekom AS, Tampnet AS, Telenor Fiber AS, Bredbåndsfylket AS
- **Transportnett:** Bulk Infrastructure Holding AS, Telenor ASA, GlobalConnect AS, Lyse Tele AS, Telia Norge AS, NTE Telekom AS, Tampnet AS, Eviny Digital AS, KystTele AS, N0r5ke Fibre AS, Stamfiber AS, Viken Fiber AS, Bredbåndsfylket AS
- **Bredbåndsnett:** Telenor ASA, GlobalConnect AS, Lyse Tele AS, Telia Norge AS, NTE Telekom AS, Eviny Digital AS, Viken Fiber AS, Eidsiva Bredbånd AS, Bredbåndsfylket AS, Ishavslink AS
- **Mobilnett:** Telenor ASA, Lyse Tele AS, Telia Norge AS, Telenor Towers Norway AS, Telia Towers Norway AS, Tårnselskapet AS

I figuren under vises andelen norsk og utenlandsk eierskap i hvert segment.

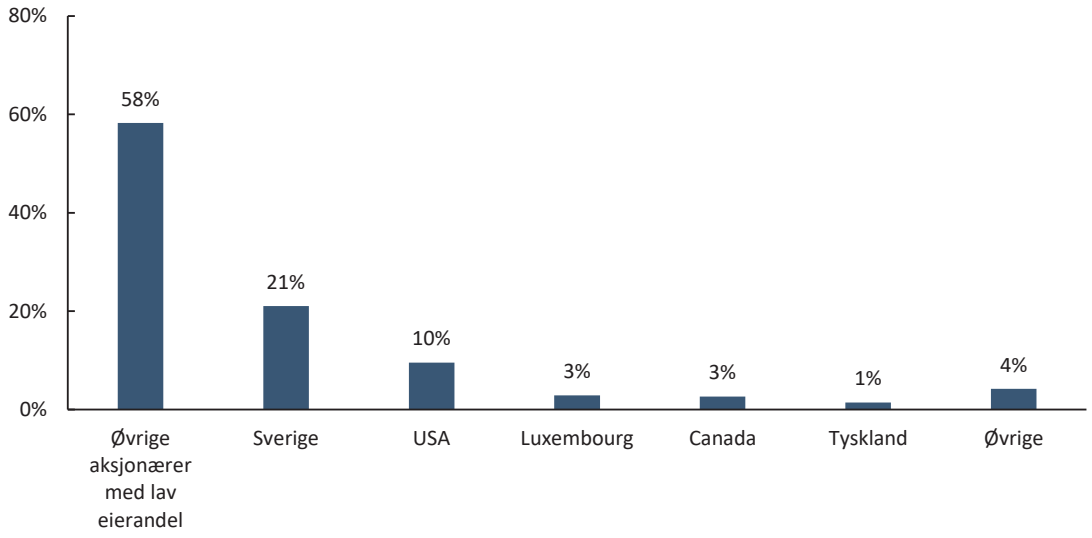
Figur 4-6: Fordeling mellom norsk og utenlandsk ultimat eierskap innenfor ulike infrastrukturkategorier, vektet etter omsetning. Antall selskaper i parentes. Kun eiere og forvaltere (kategori 1). Kilde: Menon Economics.



Som vist på figuren er fordelingen av eierskapet ganske lik på tvers av flere infrastrukturkategorier. Unntakene er datasentre, som i større grad har utenlandsk eierskap, og fortifikatoriske anlegg og infrastrukturkritiske basalfunksjoner som har større grad av norsk eierskap enn de øvrige.

I figuren under vises det utenlandske eierskapet fordelt etter hvilke land eierskapet spores tilbake til. Som nevnt, består majoriteten av det utenlandske eierskapet av aksjonærer med små eierandeler som ikke har blitt videre kartlagt. Dette medfører også at det utenlandske eierskapet i denne gruppen ikke kan knyttes til ett enkelt land.

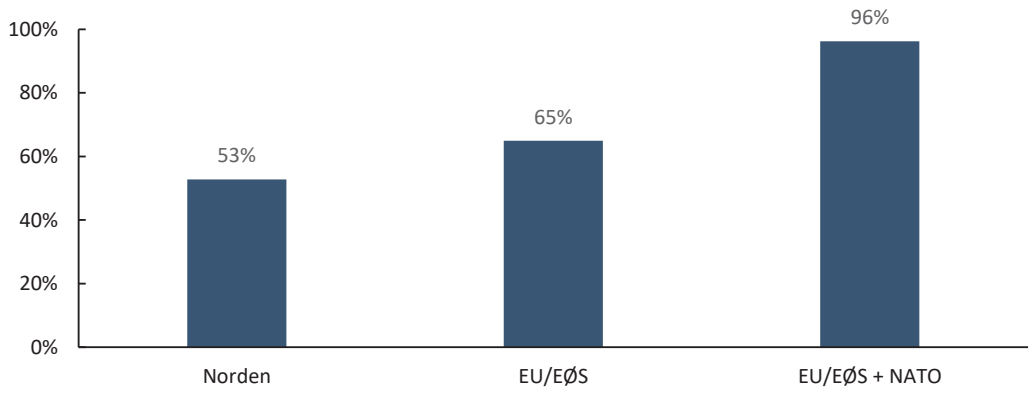
Figur 4-7: Geografisk fordeling av utenlandsk ultimat eierskap blant eiere og forvaltere (kategori 1), vektet etter omsetning. Kilde: Menon Economics



Sverige utpeker seg som det fremste eierlandet blant ultimate utenlandske eiere, etterfulgt av USA og Luxembourg. Det er likevel viktig å understreke at det kan finnes andre aktører i andre land selv om dette er der eierskapskjeden vi har kartlagt stopper. Eksempelvis er alt eierskapet registrert i Luxembourg i stor grad knyttet til fond forvaltet av EQT[17] – som igjen er eid av et bredt sett av investorer med små effektive eierandeler. I slike tilfeller har det ikke vært hensiktsmessig å gå videre bakover i eierkjeden for de fleste investorene i disse fondene, og eierkjeden stopper derfor i Luxembourg i våre data.

For å få et bedre overblikk over hvordan eierskapet fordeler seg på ulike regioner, har vi gruppert utenlandsk eierskap etter hvorvidt er en del av Norden, EU/EØS eller NATO.

Figur 4-8: Regionvis fordeling av kjent ultimat utenlandsk eierskap blant eiere og forvaltere (kategori 1), vektet etter omsetning. Kilde: Menon Economics



[17] *EQT er en av Europas største fondsforvaltere som primært investerer i unoterte selskap (private equity)*

Majoriteten av det utenlandske eierskapet ligger i Norden. Til sammen ligger noe mer av eierskapet i EU/EØS, og tilnærmet alt ultimat eierskap kan spores tilbake til et NATO-land. Det er kun en mindre andel på fire prosent av den samlede omsetningen i selskapene som eies utenfor disse landene. Blant disse er eierskap fra Israel størst, med én prosent effektivt eierskap i selskapene i kategori 1.

4.1.2 Eierskapsinformasjon på selskapsnivå

De aller fleste selskapene vi har gjennomgått har transparente eierforhold der eierskap kan spores direkte tilbake til kjent utenlandsk offentlig eller privat eierskap i EU/EØS- og NATO-land, eller børsnoterte selskaper der eierskapet er spredt på svært mange, mindre aksjonærer. I denne kategorien finnes også en rekke store og velkjente investeringsselskap.

Enkelte selskap har mer komplekse eierstrukturer som gjør eierforholdene vanskeligere å avdekke. Dette gjelder særlig eierskap som spores tilbake til land der det ikke lenger er mulig å hente ut eierskapsdata, eller til investeringsselskap uten kjente investorer.

I tabellen under følger en kort omtale av eierskapet i hvert av selskapene i kategori 1. Selskap der vi har identifisert særlig utfordrende eller potensielt problematiske eierskap diskuteres videre i kapittel 5.

Tabell 4-1: Kort beskrivelse av ultimat eierskap blant eiere og forvaltere (kategori 1)

Selskap	Beskrivelse av eierskap
Arelion Norway AS	Heleid av den svenske staten
Bredbåndsfylket AS	Majoritetseid av Troms og Finnmark fylkeskommune. Resterende 20 % eies av kommuner i Troms.
Bulk Infrastructure Holding AS	Eierskapet er hovedsakelig fordelt mellom styreleder Peter Nærbø og investeringsselskapet BGO. Utover dette finner vi flere mindre aksjonærer, inkludert John Fredriksen og ansatte.
De-Cix Management Gmbh	Heleid av *Eco – Association of the Internet industry,* en tysk paraplyorganisasjon for internett- og digitaliseringsindustri
Eidsiva Bredbånd AS	Heleid av norske kommuner og fylkeskommuner, med Oslo kommune og Innlandet fylkeskommune som største aksjonærer.
Eviny Digital AS	Tilnærmet heleid av Statkraft og norske kommuner.
Exa Infrastructure Norge AS	Heleid av Cube Aggregator, registrert på Cayman Islands. Manglende sikre datakilder gjør det videre eierskapet utfordrende å avdekke, men annen omtale av Cube Aggregator tilsier at dette kontrolleres av I Squared Capital, som igjen eies av Gautam Bhandari (USA) og Sadek M. Wahba (USA/Storbritannia), samt flere mindre aksjonærer.
GlobalConnect AS	Heleid av ulike EQT-fond, som kan spores tilbake til svært mange mindre aksjonærer
Green Mountain AS	Heleid av Azrieli Group, som igjen er majoritetseid av den israelske Azrieli-familien.
Infrastructure Nordics 4 AS	Ultimat eierskap spores tilbake til investeringsselskapene Iconiq Capital og IPI Partners.
Inmarsat Solutions AS	Eies av Viasat. Største ultimate eiere er Blackrock og The Baupost Group (investeringsselskap), men ingen har mer enn 11 prosent i ultimat eierskap.
Ishavslink AS	Største ultimate eiere er samvirkelagene Infranord SA og Alta Kraftlag SA. Utover dette er eierskapet i all hovedsak hos norske kommuner.
Kongsberg Satellite Services AS	Majoritetseid av nærings- og fiskeridepartementet. Utelukkende småaksjonærer med < 3 prosent ultimat eierskap utover dette.
KystTele AS	Heleid av Kjell Ivar Hansen Røsnes gjennom Nord-Invest AS
Lefdal Mine Datacenter AS	Majoritetseid (2/3) av Ameriprise Financial Inc., som igjen spores til mindre eierandeler hos investeringsfond fra Vanguard og BlackRock, samt en rekke småaksjonærer med < 3 prosent eierskap. Den resterende tredjedelen eies av tyske stiftelser.
Lumen Technologies Norway AS	Lumen Technologies Norway AS inngikk i konsernet til amerikanske Lumen Technologies Inc. Inntil Colt Technology Services kjøpte opp Lumen EMEA i november 2023, som omfattet den norske virksomheten til konsernet

Lyse Tele AS	Heleid av norske kommuner
N0r5ke Fibre AS	Ultimate eiere er primært av Anders Vik, Bjørn Vik og Urs von Rothenthurm Beeler (Sveits). I tillegg er det en rekke småaksjonærer, hovedsakelig norske privatpersoner.
Nasjonal Referansedatabase AS	Største ultimate eiere er Nærings- og fiskeridepartementet og svenske myndigheter. Det øvrige eierskapet fordeles mellom norske kommuner, EQT-fond, norske privatpersoner og øvrige småaksjonærer.[18]
Norid AS	Heleid av Digitaliserings- og forvaltningsdepartementet
NTE Telekom AS	Heleid av norske kommuner.
OneWeb Norway AS	Største indirekte eiere er franske og britiske myndigheter, Dhanjii og Aakash Kerai (UK) gjennom Bharti Enterprises Ltd., og et investeringsfond fra japanske Softbank.
Orange Business Digital Norway AS	Eneste vesentlige indirekte eier er franske myndigheter. Kun småaksjonærer med under 2 prosent eierskap utover dette.
Space Norway AS	Heleid av Nærings- og fiskeridepartementet
Space Norway Satcom AS	Heleid av Nærings- og fiskeridepartementet. Var inntil nylig en del av Telenor-konsernet som Telenor Satellite, men har nå fått nytt navn og blitt et heleid datterselskap av Space Norway AS.
Stamfiber AS	Primært eid av Statnett og norske kommuner. Utover dette er det noe eierskap hos EQT-fond gjennom GlobalConnect, samt svært mange småaksjonærer, primært bestående av norske privatpersoner.
Starlink Norway AS	Majoritetseid av The Elon Musk Trust. Utover dette ligger det ultimate eierskapet hos en rekke investeringsfond, men fordelingen mellom disse er svært usikker.
Tampnet AS	Hovedsakelig eid gjennom EQT-fond, som spores tilbake til en rekke småaksjonærer. I tillegg til dette eier danske myndigheter en betydelig andel gjennom Arbejdsmarkedets Tillægspension. En tilsvarende andel eies av 3I Infrastructure PLC.
Telenor ASA	Majoritetseid av Nærings- og fiskeridepartementet. Utover dette er de største ultimate eierskapene i ulike norske og internasjonale investeringsselskap, men ingen har mer enn fem prosent eierskap.
Telenor Fiber AS	Eies 70 prosent av Telenor ASA, som gir Nærings- og fiskeridepartementet et ultimat eierskap på rett under 40 prosent. De resterende 30 prosentene eies av et konsortium som ledes av investeringsselskapet KKR med Oslo Pensjonsforsikring som medinvestor.[19]
Telenor Towers Norway AS	Heleid av Telenor ASA, og dermed majoritetseid av Nærings- og fiskeridepartementet.
Telia Norge AS	Største ultimate eier er svenske myndigheter. Utover dette er de største ultimate eierskapene i en rekke investeringsselskap, men ingen har mer enn fire prosent eierskap.
Telia Towers Norway AS	Eies 51 prosent av Telia Company AB, som gir svenske myndigheter en ultimat eierandel på 21 prosent. De resterende 49 prosentene fordeles mellom investeringsselskapene Brookfield (Canada) og Alecta (Sverige)
Tårnselskapet AS	En del av Lyse-konsernet. Tilnærmet heleid av norske kommuner.
Viken Fiber AS	Heleid av norske kommuner og Statkraft.

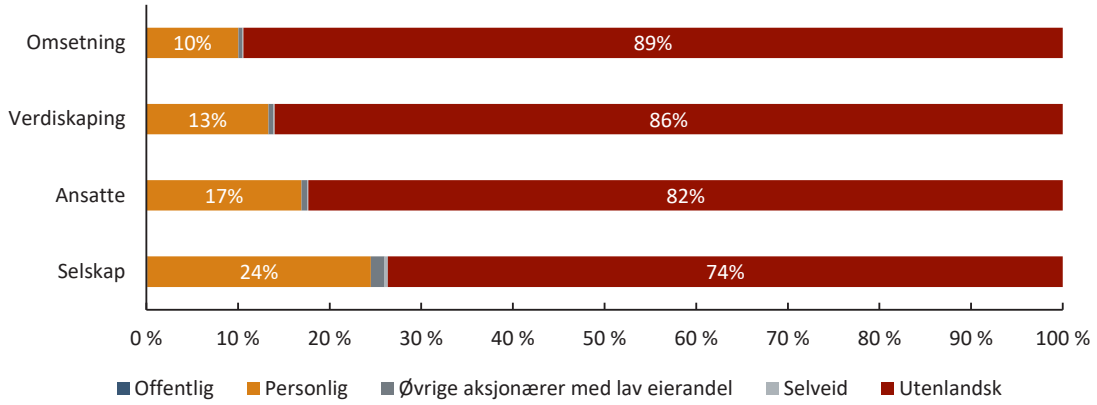
4.2 Eierskap i leverandører til kritisk digital infrastruktur

Som tidligere beskrevet, har ni av femten leverandører gjennomgått en tilsvarende kartlegging av utenlandsk eierskap som selskapene i kategori 1. De resterende seks har kun fått kartlagt sitt norske ultimate eierskap. Selskapene er derfor delt inn i henholdsvis kategori 2A (fullstendig kartlegging) og kategori 2B (begrenset kartlegging). Selskapene i kategori 2A er i gjennomsnitt større enn i kategori 2B, og står for om lag 90 prosent av de ansatte, 85 prosent av omsetningen og 80 prosent av verdiskapingen for hele kategori 2.

[18] Selskapet eies direkte av flere andre tilbydere, nærmere bestemt Telenor Mobile Holding AS, Telenor Networks Holding AS, GlobalConnect AS, Lyse Tele AS, Phonero Distribusjon AS og Unifon AS.
[19] Telenor ASA. (2024). Telenor Årsrapport 2023. Tilgjengelig her.

I figuren under viser vi en overordnet fordeling av eierskapet i alle selskapene i kategori 2. En fordeling av eierskapet i hvert enkelt selskap vises i vedlegg D.

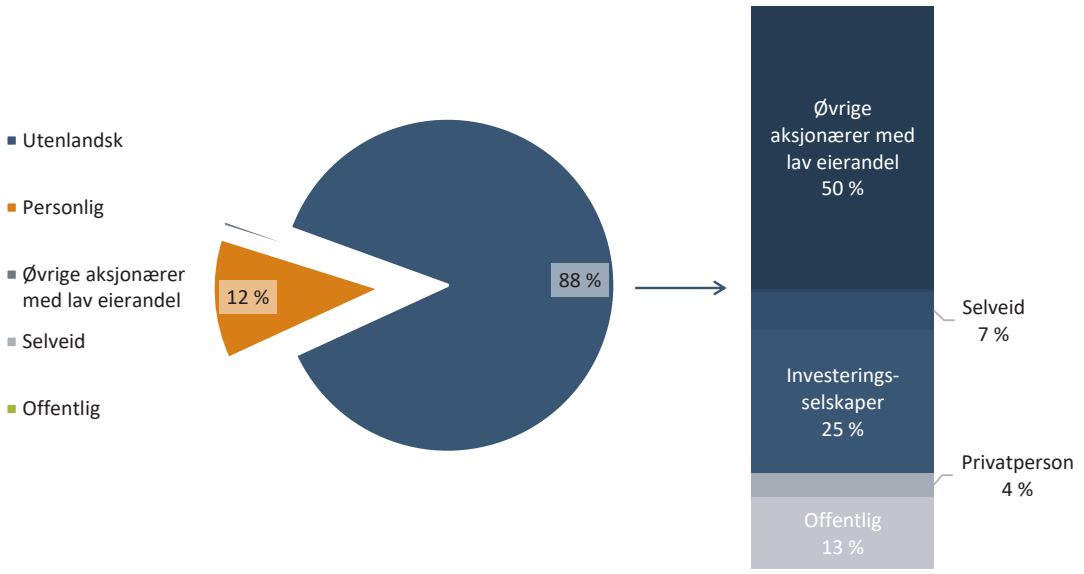
Figur 4-9: Fordeling av eierskap blant leverandører (kategori 2), etter vekting. Kilde: Menon Economics



Som figuren viser, har leverandørene betydelig mindre offentlig eierskap enn eiere og forvaltere, og heller en større andel personlig og utenlandsk eierskap. Fordelingen av eierskap varierer noe mer etter hvordan selskapene vektes mot hverandre – som også er naturlig når denne kategorien omfatter et mindre antall selskaper. Én ting som er verdt å merke seg, er at fordelingen av eierkapstyper blant selskapene i kategori 2A er noenlunde lik den samlede fordelingen for kategori 2, mens samtlige av leverandørene i kategori 2B utelukkende er eid av utenlandske aktører.

For selskapene i kategori 2A har vi også gjennomført en videre kartlegging av det utenlandske eierskapet. Den overordnede fordelingen av dette eierskapet vises i figuren under.

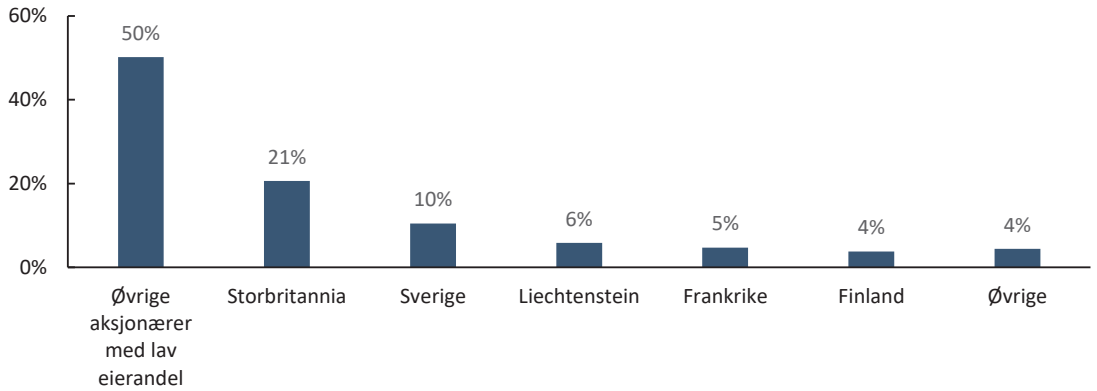
Figur 4-10: Fordeling av utenlandsk ultimat eierskap hos leverandører med fullstendig kartlegging (kategori 2A), vektet etter omsetning. Kilde: Menon Economics



Tilsvarende som for kategori 1, ser vi at det utenlandske eierskapet primært fordeler seg mellom aksjonærer med små eierandeler, investeringsselskap og offentlige eiere. Samtidig ser vi en større andel eierskap hos privatpersoner og selveide aktører[20] (primært stiftelser), og mindre eierskap hos offentlige aktører og aksjonærer med lav eierandel. Det er verdt å merke at denne eierskapsfordelingen baserer seg på et svært begrenset utvalg selskaper – kun fem av selskapene i kategori 2A spores tilbake til utenlandsk eierskap. Dermed vil denne fordelingen kunne endres betydelig ved endringer i eierskapet til enkeltselskaper.

Vi har videre sett på hvordan det utenlandske ultimate eierskapet fordeler seg på ulike land, vist i figuren under.

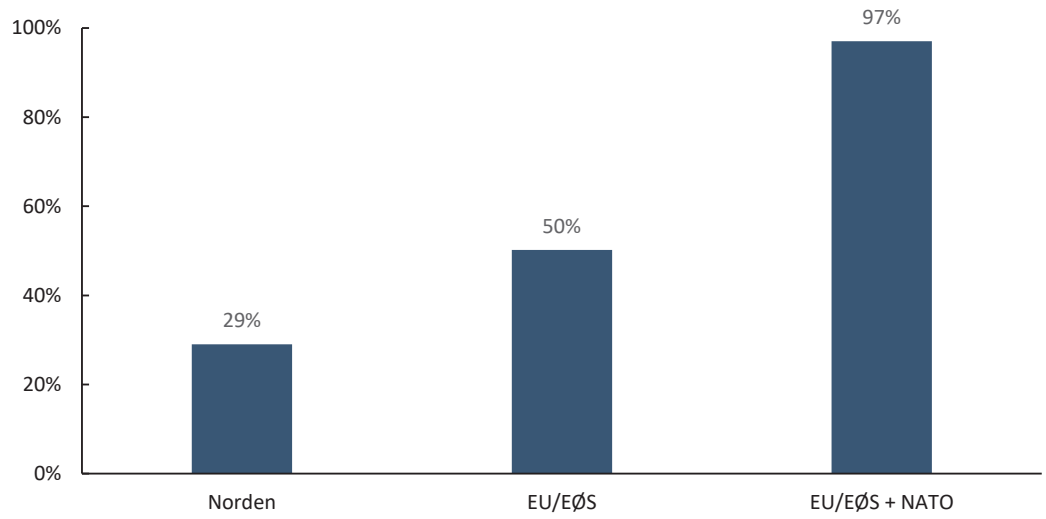
Figur 4-11: Geografisk fordeling av utenlandsk ultimat eierskap blant leverandører i kategori 2A, vektet etter omsetning. Kilde: Menon Economics



[20] *Selveide aktører inkluderer stiftelser, samvirkeforetak og organisasjoner hvor ingen fysiske personer har eierrådighet over den enheten.*

De utenlandske ultimate eierne i kategori 2A spores primært tilbake til Storbritannia og Sverige. Samtidig må også disse resultatene behandles med forsiktighet, da eierskapet i enkelte land kun baseres på én enkelt ultimat eier. Eksempelvis er alt eierskapet i Liechtenstein knyttet til en stiftelse som indirekte eier ti prosent av Nexans Norway, som er den største aktøren i kategori 2A. Det er dermed mer interessant å gruppere eierskapet etter ulike regioner, slik som i figuren under.

Figur 4-12: Regionvis fordeling av kjent utenlandsk eierskap blant leverandører i kategori 2A, vektet etter omsetning. Kilde: Menon Economics



Det er en mindre andel av det utenlandske eierskapet i kategori 2-selskapene kan knyttes til Norden og EU/EØS enn for selskapene i kategori 1. Dette skyldes i hovedsak den høye andelen av eierskapet som kan knyttes til Storbritannia. Samtidig kan mesteparten av eierskapet, på samme måte som for kategori 1, knyttes til et NATO-land, og kun tre prosent av eierskapet knyttes til land utenfor NATO og EU/EØS. Blant disse landene er eierskap fra Chile størst, hvor 1,3 prosent av det ultimate eierskapet i selskapene kan spores til.

4.2.1 Eierskap per selskap

I tabellen under følger en kort omtale av eierskapet i hvert av selskapene i kategori 2.

Tabell 4-2: Kort beskrivelse av ultimat eierskap blant leverandører (kategori 2)

Selskap	Beskrivelse av eierskap
Kategori 2A (fullstendig kartlegging)	
Caverion Norge AS	Eies av et investeringsfond forvaltet av Triton. Svenske myndigheter har en betydelig eierandel i ett av disse fondene, som medfører at disse er største ultimate eier.
Eltel Networks AS	Børsnotert konsern med svært mange aksjonærer med små eierandeler.
Netel AS	Eies av Netel Holding, som er børsnotert. Nær halvparten av det ultimate eierskapet spores til investeringsfond fra IK Partners. Øvrige eiere består primært av andre investeringsfond og aksjonærer med små eierandeler.
Nexans Norway AS	Konsernet er børsnotert, og mesteparten av det ultimate eierskapet fordeles derfor på aksjonærer med små eierandeler. Det chilenske

	konglomeratet Quiñenco innehar allikevel en betydelig eierandel på rundt 17%.
OneCo Networks Oslo	Majoritetseid av Møller-familien. Alle ultimate eiere er norske privatpersoner.
Prysmian Group Norge AS	Konsernet er børsnotert, og mesteparten av det ultimate eierskapet fordeles derfor på aksjonærer med små eierandeler.
Seaworks AS og Seaworks Management AS	Heleid av Helene og Martin Hokland
Site Service AS	Majoritetseid av investeringsselskap med mange, små investorer bak
Kategori 2B (begrenset kartlegging)	
Cisco Systems Norway AS	Del av amerikansk konsern
Ericsson AS	Del av svensk konsern
Huawei Technologies Norway AS	Del av kinesisk konsern
Juniper Networks Norway AS	Del av amerikansk konsern
Nokia Solutions and Networks Norge AS	Del av finsk konsern
Palo Alto Networks (Norway) AS	Del av amerikansk konsern

5 Vurderinger knyttet til utenlandsk eierskap

Oppsummert har vi ikke avdekket eierforhold som fremstår som problematiske i vår omfattende kartlegging av selskap som eier og forvalter kritisk digital kommunikasjonsinfrastruktur og deres leverandører. Unntaket er Huawei som vi opplever det er bevissthet rundt og kjennskap til fra tidligere, og der norske myndigheter allerede har tatt grep for å minimere denne risikoen.

I dette prosjektet har vi gjennomført omfattende kartlegginger av eierskapet i 50 selskaper, som enten eier og forvalter kritisk digital infrastruktur eller er leverandører til disse. Et sentralt funn er at mange av selskapene som eier og forvalter kritisk digital infrastruktur i Norge er deleid eller heleid av utenlandske aksjonærer. Det samme gjelder leverandørene. Vi har lykkes med å kartlegge store deler av eierskapet til de aktuelle selskapene og finner ingen direkte problematiske eierskapsforhold.

Eierskapet til denne infrastrukturen og viktige leverandører er en viktig del av risikovurderingen når det kommer til mulige sårbarheter i kritisk kommunikasjonsinfrastruktur. Det er samtidig ikke en tilstrekkelig kartlegging av risikoen. I en helhetlig vurdering av risikobildet må man spørre seg om det er andre muligheter til å utøve kontroll over infrastrukturen på, utover eierskapet. I en slik vurdering er leverandører av hardware som kritiske komponenter, softwareleverandører og sabotasjekapasitet viktige faktorer. Spesialiserte tjenesteleverandører kan ha små, men kritiske leveranser av viktige komponenter som inngår i en stor forsyningskjede. Dette fragmenterer aktørbildet og gjør risikovurderinger til en kompleks øvelse.

5.1 Ingen tydelig risiko ved det enkelte eierforholdet til kartlagte selskaper

Når vi har vurdert eventuell risiko knyttet til hvert enkelt eierforhold har vi vektlagt to ulike elementer; innflytelse (eierandel) og risikoprofil på eieren. Hvor vanskelig det er å innhente eierskapsinformasjon på selskapet bør også anses som en risikofaktor – både fordi det gir usikkerhet knyttet til hvem som eier selskapet, men også fordi vanskeligheten ved å innhente informasjon ofte er korrelert med risikoprofilen på eieren.

Det er generelt få tilfeller hvor vi enten ikke har lykkes med å nøste eierskapet tilbake til en ultimat eier eller hvor eieren fremstår som et åpenbart risikoelement. Vi har i prosjektet hatt særlig fokus på å avdekke ultimate eiere av norsk digital infrastruktur i stater som kan utgjøre en risiko for Norge og norsk infrastruktur. I praksis finner vi i liten grad eierforhold som anses som direkte problematisk med tanke på bindinger til fremmede makter eller statsborgerskap i stater som vurderes som en etterretningstrussel.

En viktig nyanse er at vi kategoriserer investeringsselskap som en type ultimat eier. Dette omfatter i all vesentlig hovedsak er forvaltningsselskaper hvor de som eier investeringsselskapet forvalter midler på vegne av investorer. Det er med andre ord ikke (bare) forvalterne av kapitalen som eier kapitalen. Vi har derfor i enkelte tilfeller kartlagt de *største* eierne av investeringsselskapet (forvaltningsselskapet), mens vi i andre tilfeller har kartlagt de største innskyterne av kapital som forvaltes av investeringsselskapet. Vanligvis har innskyterne av kapitalen (såkalte «limited partners») lite innflytelse på forvaltningen av kapitalen.[21] I begge tilfeller har vi identifisert og undersøkt eierne, enten de står bak en vesentlig andel av kapitalen eller de eier en vesentlig andel av investeringsselskapet.

[21] *Unntaket vil være tilfeller hvor hjørnesteinsinvestorer står bak majoriteten av kapitalen som investeringsselskapet forvalter, men dette er uvanlig.*

Det er identifisert et begrenset antall utenlandske privatpersoner med en eierandel i en størrelsesorden som gjør det interessant å undersøke privatpersonene. For samtlige utenlandske private eiere med mer enn 10 prosent eierandel har vi har gjort omfattende sjekker av hvem eieren er og om de har kontroverser knyttet til seg og/eller kjente bindinger til regimer som utgjør en risiko. Vi har ikke avdekket slike kontroverser eller kjente bindinger.

5.2 Identifiserte risikoelementer som man bør være bevisst på

Til tross for at det ikke er identifisert alvorlig risiko ved eierskapet til de kartlagte selskapene er det likevel noen elementer knyttet til enkelte selskap og eierforhold som er naturlig å adressere i en risikovurdering. Det er særlig tre forhold vi ønsker å belyse med disse eksemplene:

- Selskaper eid fra udemokratiske land
- Eierskap og makt konsentrert på enkeltpersoner som er politisk markerte
- Eierskap gjennom lavskatteland (definert som jurisdiksjon med gunstig skatteregime).

Huawei Technologies Norway AS er eid av Huawei Technologies Co., Ltd., som er en global leverandør av teknologi og løsninger til kommunikasjonsinfrastruktur med en kompleks posisjon i det globale markedet og i Norge. Formelt sett er Huawei et ansatteid selskap i sin helhet, men dette har ikke hindret bekymringer rundt dets tilknytninger til kinesiske myndigheter, spesielt med tanke på selskapets sivilmilitære funksjoner.[22] I tillegg har grunnleggeren av Huawei bakgrunn som general fra det kinesiske forsvaret, noe som ytterligere forsterker inntrykket av nære bånd til det kinesiske styre generelt og forsvaret spesifikt. Etterretningslovgivningen i Kina innebærer dessuten at selskaper til enhver tid kan bli pålagt å dele informasjon med myndighetene, noe som innebærer en betydelig sikkerhetsrisiko, ifølge både USA, Japan og Australia.[23] Dette har resultert i at Huawei ofte har blitt ansett som en problematisk leverandør i flere vestlige land, inklusiv Norge. Samlet sett er Huawei ansett som en sikkerhetsrisiko som leverandør til kritisk digital infrastruktur.

Et annet tilfelle med eierskap som er verdt å fremheve er **Starlink Norway AS**, som er majoritetseid av Elon Musk Trust. Dette er det fremste tilfellet av de undersøkte eierforholdene på at en utenlandsk privatperson sitter med majoritetseierskap og kontroll av en eier av digital kommunikasjonsinfrastruktur. Starlinks rolle i Ukraina har vært både kontroversiell og essensiell. Tjenesten har vært viktig for Ukrainas kommunikasjon under krisen, og har blant annet vært brukt til flere forsvarsformål. Samtidig har det også vært diskusjoner rundt Starlinks påvirkning og potensielle begrensninger i bruk. Spørsmålet om hvorvidt russiske styrker kan eller har brukt Starlink er også relevant i sikkerhetssammenheng.[24]

Det er reelle bekymringer rundt konsentrasjonen av makt over kritisk infrastruktur i hender på enkeltpersoner, spesielt når disse personene, som Elon Musk, er politisk markerte. Elon Musk donerte eksempelvis 75 millioner dollar til en gruppe som jobber for Donald Trump sin presidentkampanje over en periode på tre måneder høsten 2024.[25] Slike eksempler reiser spørsmål om personlige interesser kan påvirke beslutningsprosesser knyttet til sikkerhet og bruk. Samtidig er det viktig å understreke at dette tilfellet ikke fremstår som en direkte trussel mot norsk kritisk infrastruktur, men det understreker behovet for årvåkenhet overfor eierskap og kontroll over teknologi som er sentral i den globale digitale infrastrukturen.

[22] *Huawei. (u.d.). We Are An Independent Company. Tilgjengelig her.*
[23] *CNBC. (2019). Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice. Tilgjengelig her.*
[24] *Washington Post. (2024). Russia's illicit Starlink terminals help power its advance in Ukraine. Tilgjengelig her.*
[25] *The Guardian. (2024). Elon Musk gave $75m to his pro-Trump group in three months. Tilgjengelig her.*

Vi har identifisert et tilfelle med eierskap gjennom lavskatteland. **Exa Infrastructure Norge AS** er eid av to investeringsselskap, og deres eierskap går i sin helhet gjennom lavskattejurisdiskjonen på Caymanøyene. Eierskapet er organisert gjennom en rekke holdingselskaper registrert i Storbritannia. Bakover i eierkjeden til Exa Infrastructure Norge AS, ender finnes selskapet Cube Telecom Europe Aggregator LLC, som er registrert på Caymanøyene. Dette selskapet er igjen heleid av investeringsselskapet «I Squared Capital». Dette selskapet eies igjen av grunnleggerne Sadek M. Wahba og Gautam Bhandari (USA), sammen med en rekke andre aksjonærer, inkludert ansatte i selskapet.[26]

Generelt er det mulige risikoelementer forbundet med bruken av lavskatteland som Caymanøyene. Eierskap gjennom lavskatteland kan være motivert av flere forhold. Dette inkluderer både skattemessige hensyn, ønske om diskresjon og hemmelighold, og i noen tilfeller ønske om å enkelt kunne gjennomføre internasjonale investeringer. Særlig sistnevnte er sjeldent diskutert, men er nokså vanlig blant mange aktører, som ønsker å forenkle kapitalbevegelser og bidra til å tiltrekke seg kapital fra medinvestorer, særlig i Nord-Amerika. Eksempelvis har Norfund benyttet slike jurisdiksjoner for å tilrettelegge for investeringer, selv om dette kan medføre økt omdømmerisiko. I en gjennomgang av Norads investeringer gjennom tredjeland[27], peker PwC på flere praktiske forhold som har ført til at man investerer gjennom tredjeland/lavskatteland.[28]

I et scenario hvor selskap som eier kritisk infrastruktur er eid gjennom lavskatteland, uten transparens lenger bak i eierkjeden, kan man ikke utelukke at dette gjøres ut ifra et ønske om å skjule hvem som kontrollerer infrastrukturen. Det er viktig å påpeke at vi ikke har avdekket slike tilfeller her, og at det ikke fremstår som den mest vanlige motivasjonen bak investeringer gjennom lavskatteland.

[26] Basert på selskapets offentlige uttalelser. Selskapet avdekker ikke nøyaktige eierandeler for sine aksjonærer.
[27] PwC valgte å ikke benytte begrepet skatteparadis fordi begrepet oppleves som lite presist og det ikke finnes en omforent definisjon som entydig klargjør hvilke land som faller inn under.
[28] PwC. (2021). Analyse av Norfunds investeringer gjennom tredjeland. Tilgjengelig her.

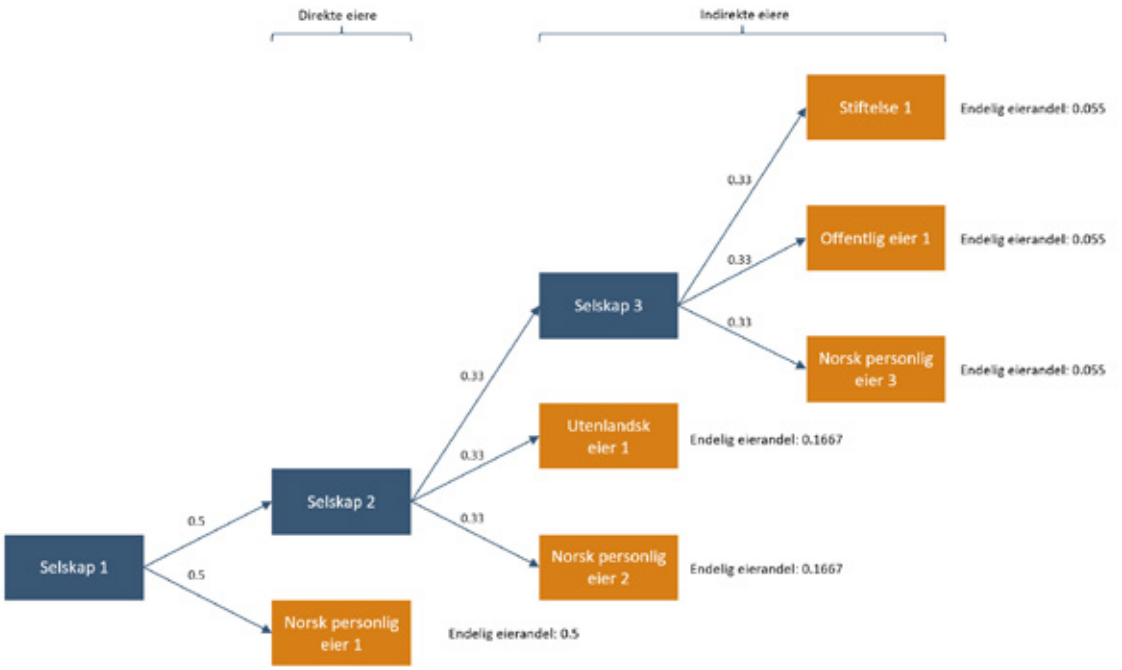
Vedlegg

Vedlegg A: Metode for identifisering av ultimate eiere

Metode for identifisering av ultimate eiere

I bearbeidingen av eierskapsdataene begrenser vi datasettet til å gjelde de 20 største eierne per foretak. For de fleste foretak vil dette utgjøre tilnærmet 100 prosent av eierskapet. Eierskapet rulles bakover i flere ledd, slik at vi til slutt ender opp med de ultimate eierne. Dette er viktig fordi mye av næringslivet eies gjennom flere ledd. Eksempelvis betyr dette at dersom selskap A er et heleid datterselskap av selskap B, hvor selskap B er eid 100 prosent av en enkeltperson, så vil også selskap A defineres som 100 prosent privat eid. Vi fokuserer dermed på den ultimate eieren ved å kartlegge hele eierskapsstrukturen i norsk næringsliv. Ettersom eierskapsstrukturer ofte er lange og komplekse, blir denne typen kartlegging en omfattende oppgave. Figuren nedenfor illustrerer hvordan vi for et tenkt selskap identifiserer de ultimate eierne i selskapet.

Figur V-1: Illustrasjon av hvordan eierskapsdatabasen definerer ultimat eier. Oransje bokser indikerer ultimat eier



Et problem i identifiseringen av ultimat eier kan oppstå ved krysseierskap, altså der to selskap direkte eller indirekte sitter med eierandeler i hverandre. Dette kan potensielt skape en uendelig rekke med indirekte eierskap. Problemet marginaliseres ved at vi regner eierskapsstrukturen bakover i 25 ledd, slik at eierandelen av krysseierskapet i det 25. ledd blir tilnærmet null.

Om beregningen av eierskapets bidrag til verdiskaping og sysselsetting

Når vi kombinerer foretaksdata med eierskapsinformasjon vekter vi eierskapets bidrag til sysselsetting og verdiskaping i foretaket i henhold til eierens eierandel. Eksempelvis, dersom et foretak eies 70 prosent av norske

personer og 30 prosent av en utenlandsk eier, så fordeler vi 70 prosent av foretakets sysselsetting og verdiskaping til det norske private eierskapet.

I tilfeller hvor selskapet holder aksjer i eget selskap, er dette kontrollert for ved at disse eierskapspostene er fordelt utover de ultimate eierne i henhold til deres eierbrøk. For eksempel; hvis 10 prosent av aksjene er eid av selskapet selv, mens de øvrige 90 prosentene er eid av hhv. en norsk privat eier (45 prosent) og en utenlandske eier (45 prosent) så vil begge disse eierpostene oppjusteres til 50 prosent.

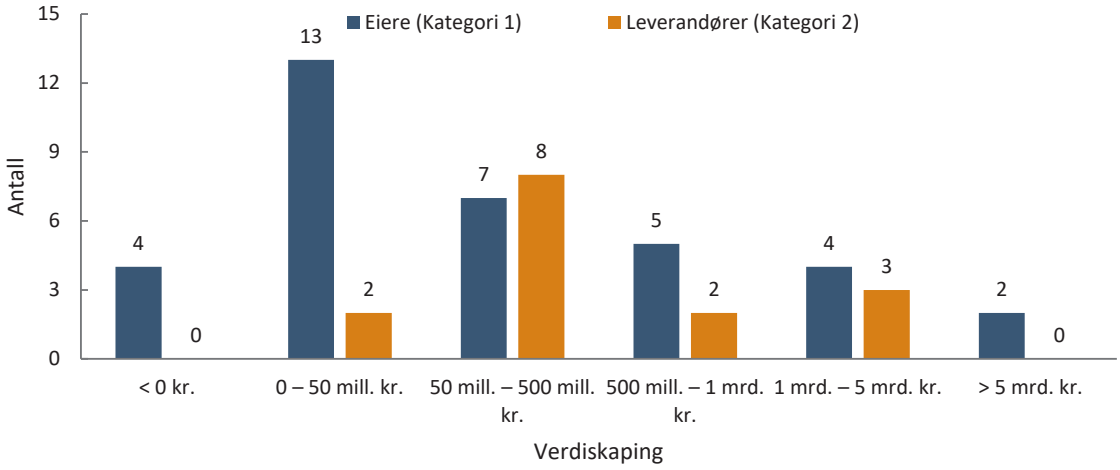
Om personlig eierskap

personlig eierskap og familieeierskap blir ofte omtalt om hverandre. Det finnes ikke noen standard definisjon av begrepet familieeierskap. Bøhren & Berzins[29] operasjonaliserer begrepet familieeierskap som foretak som er kontrollert av et eller flere familiemedlemmer i felleskap. I denne rapporten opererer vi med en definisjon av personlig eierskap som omfatter både:

- «Familieeide bedrifter», der flere fra familien eier sammen
- Enkeltpersoners bedrifter, der det kun er én eier (det er absolutt flest av disse)
- Bedrifter med flere private eiere som ikke er i slekt

Vedlegg B: Figurer

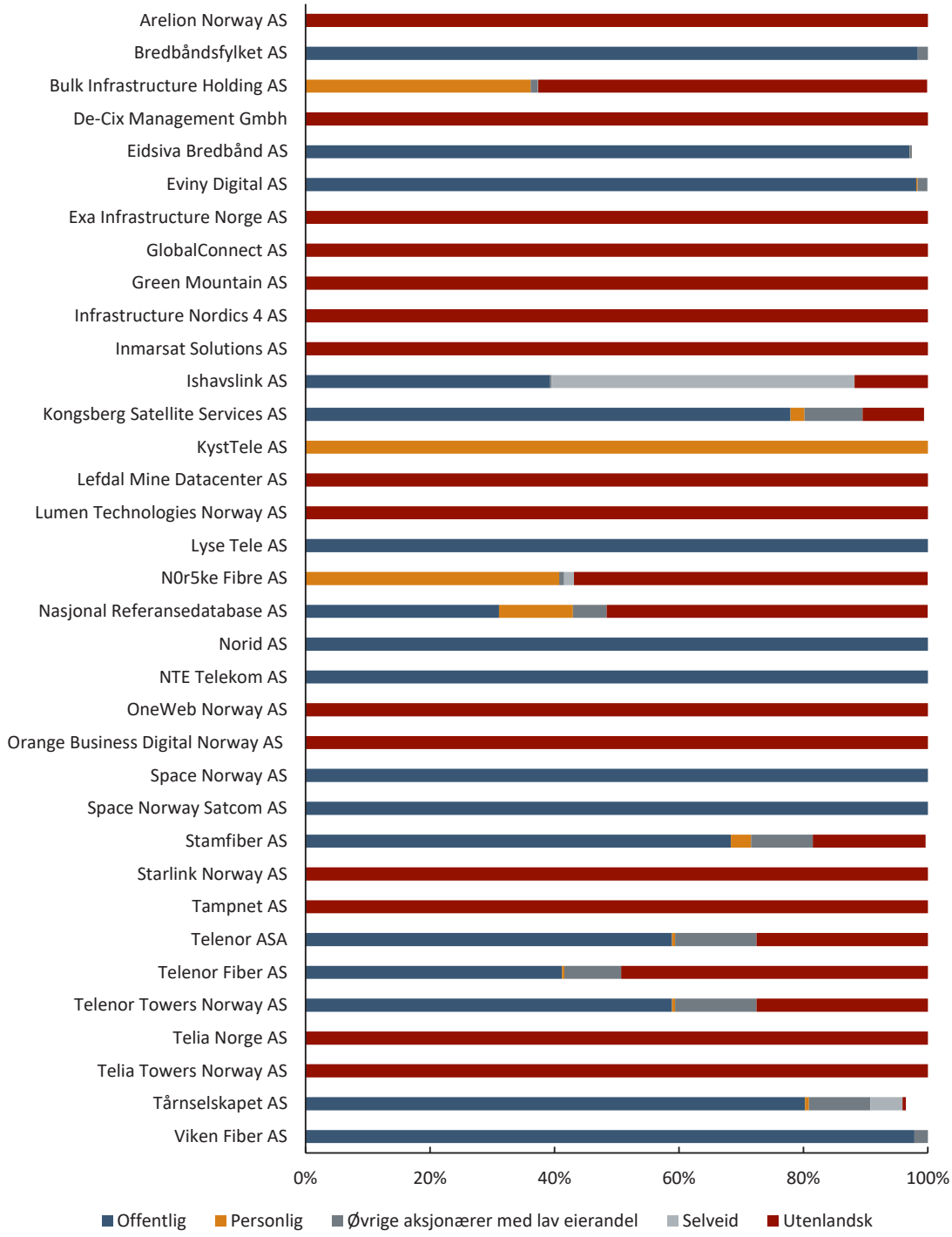
Figur V-2: Fordeling av selskaper etter størrelse på verdiskaping i 2023. Kilde: Menon Economics



[29] *Bøhren, Ø. & Berzins, J. (2013). Norske familiebedrifter – omfang, eierstyring og lønnsomhet. Tilgjengelig her.*

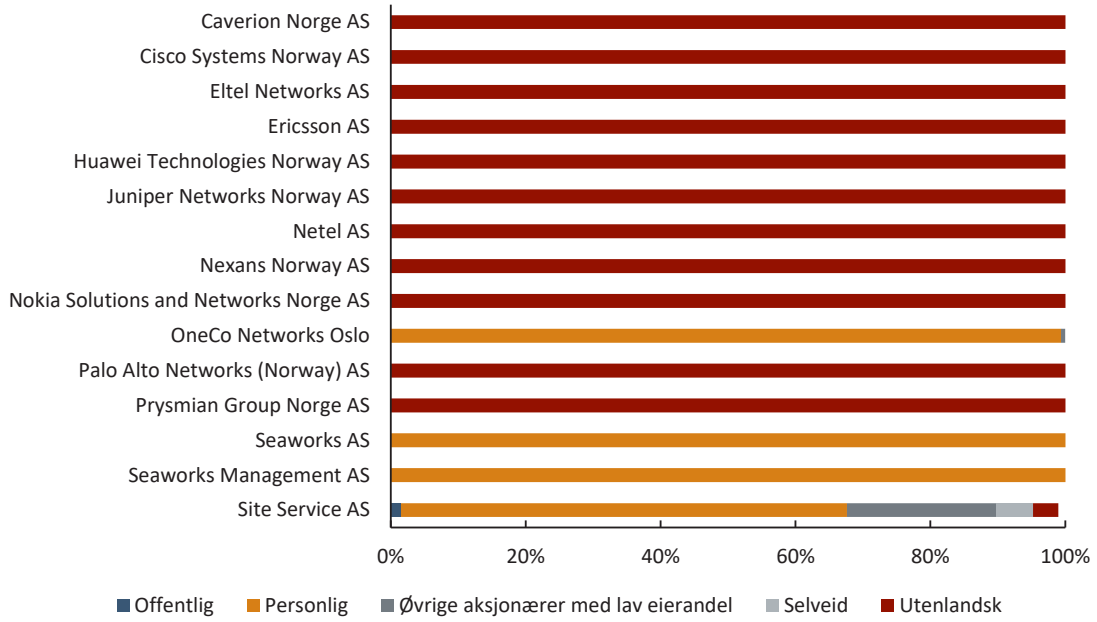
Vedlegg C: Fordeling av eierskapstyper per selskap (kategori 1)

Figur V-3: Fordeling av eiertyper per selskap for eiere og forvaltere av infrastruktur (kategori 1). Kilde: Menon Economics



Vedlegg D: Fordeling av eierskapstyper per selskap (Kategori 2)

Figur V-4: Fordeling av eiertyper per selskap for eiere og forvaltere av infrastruktur (kategori 1). Kilde: Menon Economics



Vedlegg E: Selskaper fordelt på eierskapsform

Tabellen under fordeler de ulike selskapene som undersøkes etter største eierform.[30] For selskapene som inngår i konsern fordeles selskapene etter hvordan konsernet kategoriseres.

Tabell V-1: Oversikt over eierform i selskapene som kartlegges

Eierform	Kategori 1	Kategori 2A	Kategori 2B
Børsnotert	Inmarsat Solutions AS Lumen Technologies Norway AS OneWeb Norway AS Orange Business Digital Norway AS Telia Norge AS Telia Towers Norway AS	Eltel Networks AS Netel AS Nexans Norway AS Prysmian Group Norge AS	Cisco Systems Norway AS Ericsson AS Juniper Networks Norway AS Nokia Solutions and Networks Norge AS Palo Alto Networks (Norway) AS
Majoritetseid av investeringsselskap	Bulk Infrastructure Holding AS Exa Infrastructure Norge AS GlobalConnect AS Green Mountain AS Infrastructure Nordics 4 AS Lefdal Mine Datacenter AS Starlink Norway AS	Caverion Norge AS Site Service AS	Huawei Technologies Norway AS
Majoritetseid av offentlig aktør	Arelion Norway AS Bredbåndsfylket AS Eidsiva Bredbånd AS Eviny Digital AS Kongsberg Satellite Services AS Lyse Tele AS Norid AS NTE Telekom AS Space Norway AS Space Norway Satcom AS Stamfiber AS Telenor ASA Viken Fiber AS		
Majoritetseid av privatperson	KystTele AS	OneCo Networks Oslo Seaworks AS Seaworks Management AS	
Selveid	De-Cix Management Gmbh		
Annet spredt eierskap	Ishavslink AS N0r5ke Fibre AS Nasjonal Referansedatabase AS Tampnet AS Telenor Fiber AS		

[30] *Selskap som er majoritetseide kan fremdeles være børsnoterte (som eksempelvis Telenor ASA). Her er det kun selskaper som ikke har en tydelig majoritetseier som er definert som børsnoterte.*

Menon Economics analyserer økonomiske problemstillinger og gir råd til bedrifter, organisasjoner og myndigheter. Vi er et medarbeidereiet konsulentselskap som opererer i grenseflatene mellom økonomi, politikk og marked. Menon kombinerer samfunns- og bedriftsøkonomisk kompetanse innenfor fagfelt som samfunnsøkonomisk lønnsomhet, verdsetting, nærings- og konkurranseøkonomi, strategi, finans og organisasjonsdesign. Vi benytter forskningsbaserte metoder i våre analyser og jobber tett med ledende akademiske miljøer innenfor de fleste fagfelt. Alle offentlige rapporter fra Menon er tilgjengelige på vår hjemmeside www.menon.no.

+47 909 90 102 | post@menon.no | Sørkedalsveien 10 B, 0369 Oslo | menon.no

Vedlegg 4

Juridisk utredning foretatt av professor Christoffer Conrad Eriksen, Universitetet i Oslo

Professor Christoffer Conrad Eriksen
Institutt for offentlig rett
Det juridiske fakultet
Universitetet i Oslo

Oslo 22. november 2024

UTREDNING AV RETTSLIGE RAMMER FOR KONTROLL MED KRITISK DIGITAL INFRASTRUKTUR

Innholdsfortegnelse:

1

1. Bakgrunn

I juni 2024 inngikk jeg avtale om et utredningsoppdrag med Digitaliserings- og forvaltningsdepartementet på vegne av et ekspertutvalg regjeringen har satt ned for å gi konkrete forslag til hvordan staten kan ivareta nasjonal kontroll med kritisk digital kommunikasjonsinfrastruktur, som mobil- og bredbåndsnett («ekomsikkerhetsutvalget»).

Formålet med oppdraget er å «*utrede ulike muligheter eller forutsetninger for myndighetsutøvelse overfor utenlandske selskaper når formålet er å ivareta nasjonal kontroll med kritisk digital infrastruktur som disse enten eier eller kontrollerer i Norge*».

Det er avtalt at utredningen skal leveres som en tekst som kan inngå som et vedlegg eller et kapittel i ekomsikkerhetsutvalgets rapport.

I oppdragsavtalen ble bakgrunnen for oppdraget beskrevet slik:

> «I januar 2024 satte regjeringen ned et eget ekspertutvalg for å vurdere hvordan staten kan ivareta nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur. Bakteppet for oppnevnelsen kan sammenfattes med utviklingen i den sikkerhetspolitiske situasjonen i Europa og verden ellers, at kommunikasjonsnettene våre bærer stadig viktigere samfunnsverdier, samtidig med at man har sett eksempler på salg av eierandeler eller deler av viktig kommunikasjonsinfrastruktur.
>
> Disse forholdene har aktualisert behovet for å avklare om myndighetene har tilgang til nødvendige virkemidler for å oppnå tilstrekkelig nasjonal kontroll over kritisk digital infrastruktur. Dette gjelder både eierskap, regulering eller også avtalerettslige virkemidler for de som eier infrastrukturen.
>
> Det er særlig problemsstillinger som oppstår ved eierskapstransaksjoner utvalget skal se nærmere på, men utvalgets arbeid er delt inn i tre delmål:
>
> 1) Identifisere kritisk infrastruktur på et overordnet nivå (til eget formål)
> 2) Status for nasjonal kontroll og dagens virkemidler
> 3) Vurdere tiltak for styrket nasjonal kontroll
>
> Eksempler på virkemidler myndighetene har for å ivareta nasjonal kontroll over digital infrastruktur er regulering og nasjonalt eierskap. Investeringer og eierskifte kan medføre at en ny utenlandsk eier får tilgang til eller betydelig innflytelse i et norsk foretak, noe som kan utgjøre en risiko for nasjonale sikkerhetsinteresser. Det finnes flere regelverk som gir eller kan gi myndighetene mulighet til å gripe inn i utenlandske investeringer i norske foretak. Sikkerhetsloven har som formål å ivareta nasjonale sikkerhetsinteresser, og hjemler dagens ordning for investeringskontroll. I lovens § 10-3 kan det settes vilkår for gjennomføringen av et erverv dersom ervervet kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Myndighetens mulighet til å kunne pålegge vilkår som reduserer risikoen ved et eierskifte er dermed et viktig virkemiddel for å ivareta nasjonal kontroll av kritisk digital infrastruktur.»

I den nærmere beskrivelsen av oppdraget fremgår det at utredningen skal omfatte forutsetninger for myndighetsutøvelse på generelt grunnlag og med tanke på noen bestemte

spørsmål. Slik jeg forstår oppdragsavtalens konkrete spørsmål skal utredningen omfatte en vurdering av hvilke deler av et utenlandsk konsern eller en kompleks eierstruktur som bør pålegges vilkår vedrørende sikkerheten til kritisk infrastruktur i Norge, for at vilkårene skal anses for å være bindende og kunne håndheves. Videre skal denne vurderingen av hvem vilkår skal pålegges også belyse hvilken betydning det har at utenlandske morselskaper, gjennom norske datterselskaper, eier fysisk infrastruktur i Norge eller tilbyr ekom- eller datasentertjenester i Norge til norske brukere. Endelig forstår jeg også oppdragsavtalen slik at utredningen også skal omfatte en vurdering av om det kan være hensiktsmessig at myndigheter inngår avtaler med utenlandske selskaper om at de skal etterleve vilkår, som et alternativ til at selskapene pålegges vilkår i kraft av myndighetsutøvelse.

Selv om oppdraget omfatter flere konkrete spørsmål er det det likevel angitt i avtalen at «kjernen i oppdraget» er å utrede hvilke forutsetninger som må til for at norske myndigheter kan pålegge og faktisk følge opp risikoreduserende vilkår overfor utenlandske selskaper som eier eller kontrollerer kritisk digital infrastruktur i Norge. I oppdragsbeskrivelsen er det videre presisert at det kan være aktuelt at norske myndigheter stiller både strukturelle og adferdsbaserte vilkår for å ivareta sikkerhetsinteresser.

I det følgende redegjør jeg nærmere for hvordan jeg har tolket oppdraget (punkt 2), før jeg gir en oversikt over de spørsmål jeg har utredet (punkt 3).

2. Tolkning av oppdraget

Oppdragsavtalen ber om en utredning av «muligheter eller forutsetninger for myndighetsutøvelse overfor utenlandske selskaper». Med myndighetsutøvelse forstår jeg i denne sammenheng den rettslige kompetanse (myndighet) og frihet som den norske staten har etter norsk intern rett og folkeretten til å pålegge utenlandske virksomheter vilkår og å håndheve disse vilkårene overfor de utenlandske selskapene.

Med uttrykket «vilkår» forstår jeg plikter som selskaper og andre private parter må oppfylle for at deres virksomhet skal anses som lovlige. I lys av bakgrunnen for oppdraget legger jeg til grunn at utredningen bør konsentreres om kompetansen til å pålegge vilkår med hjemmel i sikkerhetsloven.

Som jeg kommer tilbake til, er det en forutsetning for å kunne pålegge vilkår overfor utenlandske selskaper at vilkårene er lovlige etter norsk intern rett. Hvilke vilkår sikkerhetsloven gir hjemmel for å pålegge etter intern norsk rett reiser spørsmål om overordnete rettsnormers betydning for tolkningen av lovens bestemmelser. Noen sider ved dette spørsmålet har vært utredet i lovens forarbeider, andre sider har ikke vært utredet. I denne utredningen har det derfor vært nødvendig i å gå forholdsvis grundig inn i de rammene overordnede rettsnormer setter for tolkningen av sikkerhetsloven.

Med overordnede rettsnormer mener jeg rettsnormer som kan utledes av henholdsvis Grunnloven, Den europeiske menneskerettighetskonvensjon (EMK) og EØS-avtalen. Etter norsk rett er det klart at Grunnloven er overordnet den ordinære lovgivningen i den forstand at den ikke kan anvendes slik at den fører til resultater som er i strid med Grunnloven. Ved konflikt mellom lov og Grunnlov skal domstolene bygge sin avgjørelse på den regel som

følger av grunnloven, ikke på lovbestemmelsen.[1] Når det gjelder EMK og EØS-avtalen er dette i utgangspunktet avtaler mellom Norge og andre stater som kun er folkerettslige forpliktende for Norge, og ikke overordnet lovgivningen. Stortinget har likevel vedtatt at begge avtaler skal gjelde som norsk lov, og at de skal ha forrang foran annen lovgivning ved konflikt, jf. menneskerettsloven §§ 2 og 3 og EØS-loven §§ 1 og 2. I den forstand er både EMK og EØS-avtalen overordnet annen norsk lovgivning, herunder også sikkerhetsloven.

Forutsatt at det er hjemmel etter intern norsk rett, kan norske myndigheter pålegge virksomheter ulike typer av vilkår. I samsvar med oppdragsavtalen skiller jeg her mellom strukturelle og adferdsbaserte vilkår.

Med strukturelle vilkår forstår jeg vilkår som angår virksomhetenes struktur. For eksempel vil det være et strukturelt vilkår dersom en virksomhet pålegges en plikt til å sørge for at en sensitiv eiendel eller eiendom blir ekskludert fra et oppkjøp. Jeg legger til grunn at slike vilkår kan være aktuelt der hvor en investor ønsker å kjøpe seg inn i en virksomhet og deler av denne virksomheten driver produksjon inn mot en forhåndsdefinert sensitiv sektor. Et strukturelt vilkår vil kunne sikre at investoren ikke får tilgang til eller kontroll over de verdiene som regelverket skal beskytte.

Videre legger jeg til grunn at adferdsbaserte vilkår, ikke handler om virksomhetenes struktur, men om pålegg av plikter innenfor eksisterende virksomhetsstrukturer. Et eksempel kan være at en ny minoritetseier ikke skal få styreplass eller tilgang til sensitiv informasjon i et selskap, eller at stemmeretten for visse eiere oppheves. Vilkår kan også innrettes slik at de begrenser eierens mulighet til å få innsikt i foretakets virksomhet på visse områder, for eksempel i utviklingen av kritisk teknologi eller sårbarheter i tjenesteproduksjon og infrastrukturen selv.

Jeg går ellers ut ifra at vilkår kan ta høyde for fremtidige hendelser, for eksempel å sikre varsling til norske myndigheter i tide til å kunne gripe inn ved eventuelle fremtidige sikkerhetstruende eierskifter eller å legge enkelte begrensninger på fremtidige videresalg av eierandeler.

Jeg legger videre til grunn at utredningen skal omfatte adgangen til å pålegge vilkår overfor virksomheter som eier eller kontrollerer digital infrastruktur som har avgjørende eller vesentlig betydning for grunnleggende nasjonale funksjoner eller som har avgjørende betydning for nasjonale sikkerhetsinteresser, uten å kunne knyttes direkte til en grunnleggende nasjonal funksjon, jf. Sik kerhetsloven § 1-3. Det betyr at disse virksomhetene kan være omfattet av sikkerhetsloven. Der infrastrukturen har avgjørende betydning for grunnleggende nasjonale funksjoner, er det klart at departementet er forpliktet til å vedta at virksomhetene skal være omfattet av sikkerhetsloven jf. § 1-3 første ledd. Er det tale om infrastruktur som har vesentlig betydning for grunnleggende nasjonale funksjoner, er det opp til departementets skjønn om det skal treffes vedtak om at sikkerhetsloven gjelder for virksomhetene jf. § 1-3 andre ledd.

[1] Se Rt 1976. s. 1

3. Oversikt

I det følgende presenterer jeg først en sammenfatning av vurderingene i denne utredningen (punkt 4).

Videre redegjør jeg for hvilke rettslig grunnlag myndighetene må ha for å avtale eller pålegge private parter vilkår (punkt 5).

Jeg vurderer deretter om sikkerhetslovens hjemler gir tilstrekkelig rettslig grunnlag for å pålegge risikoreduserende tiltak overfor virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge (punkt 6), og myndighetenes adgang til å håndheve slike vilkår (punkt 7).

Endelig redegjør jeg for de folkerettslige rammer for norske myndigheters adgang både til å pålegge og håndheve vilkår overfor utenlandske virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge (punkt 8).

4. Sammenfatning

Oversikt over forutsetninger

Det er klart at norske myndigheter kan stille og følge opp risikoreduserende vilkår overfor virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge.

Forutsetningene for at slike vilkår kan håndheves er (i) at det er et lovlig rettsgrunnlag for å oppstille vilkårene, (ii) at vilkårene ikke går lenger enn det rettsgrunnlaget tillater, og (iii) at virksomhetene kan presses til å oppfylle vilkårene med tvangstiltak.

Overfor utenlandske virksomheter er det i tillegg en forutsetning (iv) at de aktuelle vilkårene enten (a) bygger på avtale eller (b) bygger på myndighetsutøvelse innenfor rammene av norsk jurisdiksjon, og i begge tilfeller, (v) at norske myndigheter har enten (a) jurisdiksjon til å gjennomføre håndhevelsestiltakene eller (b) at det foreligger en folkerettslig avtale som gir grunnlag for å gjennomføre håndhevelsestiltak i en annen stat.

Rettsgrunnlaget må være lovlig (i)

Norske myndigheter kan i kraft av sin partsautonomi inngå avtale om kjøp av digital infrastruktur eller tjenester relatert til slik infrastruktur, og i slike avtaler sette vilkår i den grad leverandøren samtykker.

Videre har Kongen i statsråd en generell kompetanse (myndighet) til å fastsette vilkår etter sikkerhetsloven § 2-5. Kongen i statsråd har også kompetanse til å fastsette vilkår ved anskaffelser etter lovens § 9-4 og ved erverv etter § 10-3. En forutsetning for at disse hjemlene kan anvendes som grunnlag for å pålegge virksomheter plikter, er at hjemlene er tilstrekkelig presise, og i samsvar med de krav Grunnloven, EMK og EØS-retten stiller.

Det er klart at vilkårene for anvendelse av lovens § 2-5 er forholdsvis upresise, samtidig som det bare er lovens formål som setter rammer for hvilke vedtak som kan fattes etter bestemmelsen. Det gjør det i praksis krevende for domstoler å kontrollere lovligheten av vedtakene, i strid med Grunnlovens og EMKs forutsetninger om at rettsstaten skal sikre både forutberegnelighet og en effektiv domstolskontroll. Fordi sikkerhetsloven § 2-5 også kan anvendes for å gripe inn mot og stille vilkår til investeringer i norske virksomheter, kan bestemmelsen også hemme interessen i, eller gjøre det mindre attraktivt å investere i norske selskaper, i strid med EØS-rettens regler om etableringsrett og kapitalfrihet. Det kan derfor reises spørsmål om bestemmelsen går utover de krav til lovhjemlers presisjon som følger av Grunnloven, EMK og EØS-retten. Slik jeg ser er det likevel gode argumenter for at sikkerhetsloven § 2-5 ikke går utover de presisjonskrav som følger av Grunnloven, EMK og EØS-retten, gitt at bestemmelsen tolkes i samsvar med forarbeidenes forutsetning om at den kun skal anvendes som en «sikkerhetsventil». Jeg antar derfor at Kongen i statsråd kan anvende bestemmelsen for å pålegge virksomheter vilkår, uten stor risiko for at slike vilkår blir ansett for å være ugyldige fordi hjemmelen er for upresis.

Vilkårene for anvendelse av sikkerhetsloven § 10-3 er tilsvarende upresise, som vilkårene for anvendelse av § 2-5. Fordi § 10-3 i motsetning til § 2-5 kun gir kompetanse til å stanse eller stille vilkår for erverv, kan bestemmelsen neppe anses for å være i strid med Grunnlovens eller EMKs presisjonskrav. Derimot er det nokså klart at bestemmelsen og den mekanismen for investeringskontroll bestemmelsen er en del av, er en restriksjon på etableringsretten og kapitalfriheten som er beskyttet av EØS-avtalen og EØS-loven. På grunn av mangelen på presisjon i denne kontrollmekanismen er det gode argumenter som tilsier at denne restriksjonen går lenger enn det EØS-retten tillater. Det innebærer at det er betydelig risiko for at vilkår fastsatt med hjemmel i lovens § 10-3 kan anses som ugyldige i den grad de er rettet mot virksomheter i EØS. Tilsvarende er det er betydelig risiko for at vedtak om stans av erverv fastsatt med hjemmel i lovens § 10-3 kan anses som ugyldige i den grad vedtak er rettet mot virksomheter i EØS. Konsekvensen av ugyldighet er at vilkårene og stansingsvedtak ikke kan håndheves og at de som utsettes for slike vilkår blir ofre for ulovlig myndighetsutøvelse.

Vilkår må ha tilstrekkelig hjemmel (ii)

I den grad sikkerhetsloven § 2-5 og § 10-3 anses for å være tilstrekkelig presise lovhjemler, må bestemmelsene også antas å gi tilstrekkelig hjemmel for å pålegge virksomheter både strukturelle og adferdsbaserte vilkår. Forutsetningen er at vilkårene ligger innenfor sikkerhetslovens formål og ikke er uforholdsmessig tyngende. Det er klart at sikkerhetslovens formål favner vidt og at både § 2-5 og § 10-3 derfor gir Kongen i statsråd tilstrekkelig hjemmel blant annet for å stille vilkår om at en sensitiv eiendel eller eiendom blir ekskludert fra et oppkjøp eller at en ny minoritetseier ikke skal få styreplass eller tilgang til sensitiv informasjon i et selskap.

Plikter og unnlatelser som kan håndheves ved tvang (iii)

For å håndheve vilkår med tvang, må manglende etterlevelse av krav kunne møtes med sanksjoner eller begjæres fullbyrdet etter tvangsfullbyrdelseslovens regler. Vedtak etter sikkerhetsloven § 2-5 og § 10-3 er begge straffesanksjonert jf. sikkerhetsloven § 11-4 fjerde ledd. For øvrig kan tvangsfullbyrdelse av et krav bare gjennomføres når det foreligger et

alminnelig eller et særlig tvangsgrunnlag for kravet, og dette tvangsgrunnlaget er tvangskraftig jf. tvangsfullbyrdelsesloven § 4-1.

De mest aktuelle alminnelige tvangsgrunnlag for myndighetens adgang til å håndheve vilkår overfor utenlandske virksomheter er dommer eller kjennelser avsagt av norsk domstoler, voldgiftsdommer, og avgjørelser av utenlandske domstoler. For øvrig er de vedtak Kongen i statsråd treffer etter sikkerhetsloven § 2-5, § 9-4 og § 10-3 særlige tvangsgrunnlag for tvangstiltak etter tvangsfullbyrdelsesloven kapittel 13.

Tvangsfullbyrdelse kan gå ut på ulike tvangshandlinger. Jeg antar at tvangsgjennomføring av strukturelle eller adferdsbaserte vilkår først og fremst vil gjelde krav som går ut på annet enn betaling av penger. Etter tvangsfullbyrdelsesloven kapittel 13 kan andre krav enn penger blant annet gjennomføres ved utlevering av løsøre og verdipapir jf. § 13-8, fravikelse av fast eiendom jf. § 13-11, sikkerhetsstillelse jf. § 13-3, andre handleplikter som påleggelse av mulkt jf. § 13-14, og unnlatelses- og tåleplikter jf. § 13-6.

Statens avtalefrihet rekker lenger enn statens jurisdiksjon (iv. a)

Staten har avtalefrihet og kan i utgangspunktet inngå avtaler med enhver privat part, også utenlandske virksomheter om forhold staten ikke har jurisdiksjon over. Når staten inngår avtaler med virksomheter om forhold som ligger utenfor norsk jurisdiksjon, kan staten heller ikke utøve offentlig myndighet ved avtaleinngåelsen. Såfremt staten uten utøvelse av offentlig myndighet oppnår enighet med utenlandske virksomheter om vilkår for deres eierskap eller kontroll over kritisk digital infrastruktur i Norge, kan vilkårene både gjelde strukturelle og adferdsbaserte forhold.

Fordi avtaler ikke binder andre enn avtalepartene, vil for eksempel en avtale med et datterselskap i et norsk eller utenlandsk konsern i utgangspunktet ikke være bindende for alle andre selskaper i konsernet, med mindre disse også er parter i avtalen. For å binde et utenlandsk morselskap til bestemte vilkår, er det derfor i utgangspunktet ikke tilstrekkelig å inngå avtale med norske datterselskaper, selv om det er norske datterselskaper som eier fysisk infrastruktur i Norge eller tilbyr ekom- eller datasentertjenester i Norge til norske brukere.

Statens jurisdiksjon til å fastsette vilkår med virkning for utenlandske virksomheter (iv. b)

Norske myndigheter har jurisdiksjon til å fastsette vilkår gjennom myndighetsutøvelse, også overfor utenlandske virksomheter. Det virksomhetene gjør i Norge har norske myndighetene allerede jurisdiksjon over i kraft territorialhøyheten. Jeg antar derfor at norske myndigheter i kraft av sin suverenitet over norsk territorium kan stille vilkår om at en ny utenlandsk eier i norsk selskap, ikke skal ha tilgang til informasjon om hvor digital infrastruktur er lokalisert.

Norske myndigheter har også jurisdiksjon til å regulere, og pålegge vilkår overfor det virksomheter gjør i utlandet, såfremt det er tale om handlinger som først blir fullført i Norge. Vilkår kan derfor pålegges utenlandsk selskap såfremt vilkårene angår handlinger som først blir fullført i Norge. Konkret innebærer dette at norske myndigheter kan pålegge utenlandske selskap vilkår som gjelder handlinger som først blir fullført i Norge, uavhengig av om det utenlandske selskapet selv eier infrastruktur eller tilbyr ekom- eller

datasentertjenester i Norge, eller om det har kontroll over infrastrukturen og tjenestene gjennom norske datterselskaper.

I tillegg antar jeg at norske myndigheter har jurisdiksjon over handlinger som foretas av utenlandske virksomheter som har direkte, vesentlige og forutsigbare virkninger i Norge jf. den folkerettslige effektdoktrinen. Det innebærer at norske myndigheter har jurisdiksjon til å fastsette vilkår overfor utenlandske virksomheter i den grad det er tale om vilkår for handlinger som har direkte, vesentlige og forutsigbare virkninger i Norge. Det kan for eksempel gi grunnlag for å stille vilkår til en utenlandsks virksomhets håndtering av informasjon om digital infrastruktur i Norge, i den grad visse måter å håndtere informasjonen på har direkte, vesentlige og forutsigbare skadevirkninger i Norge. Effektdoktrinen kan også gi adgang for norske myndigheter til å stille vilkår til utenlandske virksomheter som ikke eier infrastruktur i Norge, men som tilbyr tjenester som anvendes i riket, forutsatt at vilkårene gjelder forhold som har direkte, vesentlige og forutsigbare virkninger i Norge.

Utenlandske eiere eller morselskap kan derfor pålegges vilkår som angår forhold som har direkte, vesentlige og forutsigbare virkninger i Norge, for eksempel dersom vilkårene angår styringen av norske selskaper som eier fysisk infrastruktur i Norge eller tilbyr ekom- eller datasentertjenester i Norge til norske brukere.

Jeg gjør likevel oppmerksom på at norske myndigheter ikke har eksklusiv jurisdiksjon over utenlandske aktører, slik at disse også kan være underlagt andre plikter som kan stå i motsetning til de vilkår norske myndigheter pålegger. Det avgjørende for effekten av vilkårene vil derfor ikke nødvendigvis bero på om vilkårene er bindende i en rettslig forstand, men på muligheten for å håndheve vilkårene med tvang (se nedenfor).

Håndhevelsesjurisdiksjon (v. a)

Enten vilkår er fastsatt ved avtale eller ved utøvelse av offentlig myndighet, kan de kun håndheves av norske myndigheter ved tvang, såfremt tvangstiltakene kan gjennomføres i Norge uten å krenke andre staters suverenitet. Norske myndigheter har ikke adgang til å gjennomføre tvangstiltak utenfor Norge uten at aksept fra den staten der tvangstiltakene skjer.

Det kan være krevende å identifisere hvor et tvangstiltak blir gjennomført. Høyesterett har i en straffesak antatt at det er tillatt for norske myndigheter å hente ut digital informasjon fra lagringssteder i utlandet, forutsatt at uthenting skjer fra en terminal i Norge, og uten at det utenlandske lagringsstedet blir påvirket av en eventuell uthenting av informasjon. Jeg antar at tilsvarende gjelder der staten har en privatrettslig avtale med en utenlandsk virksomhet, som har et vilkår som gir staten rett til å hente digital informasjon lagret i utlandet.

Folkerettslige håndhevelseskonvensjoner for avtalte vilkår (v. b)

Utover forholdsvis omfattende nordiske samarbeidsavtaler, er det flere europeiske og internasjonale avtaler om grensekryssende samarbeid om tvangsjurisdiksjon. Blant annet gir regelverket om den europeiske arrestordre et grunnlag for at den norske påtalemyndighetens beslutninger får virkning i andre europeiske land. Andre sentrale internasjonale avtaler som åpner for at norsk myndighetsutøvelse kan få virkning i andre

land er, er *Convention on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters* («Lugano-konvensjonen» og *The Convention on the Recognition and Enforcement of Foreign Arbitral Awards* («New York-konvensjonen). Ingen av disse konvensjonene gjelder imidlertid vilkår fastsatt i kraft av offentlig myndighetsutøvelse, det vil si plikter som norske myndigheter ensidig pålegger private parter. Videre gjelder Lugano-konvensjonen ikke for voldgiftssaker. Derimot gjelder New York konvensjonen kun for voldgiftssaker. Regelverket om den europeiske arrestsordren gjelder bare straffesaker, og faller utenfor denne utredningens tematikk.

Etter Lugano-konvensjonen kan en part i kontraktsforhold begjære gjennomføring av tvangstiltak i de statene og organisasjonene som har sluttet seg til konvensjonen, det vil si EU, Danmark, Norge, Island og Sveits. Forutsetningen for at tvangstiltak kan begjæres gjennomført etter konvensjonen er at det foreligger en dom eller kjennelse i Norge for kravet.

En part kan også begjære gjennomføring av tvangstiltak etter New York-konvensjonen. Forutsetningen er da at det må foreligge en voldgiftsavgjørelse. Er denne forutsetningen oppfylt kan imidlertid tvangstiltak begjæres gjennomført i konvensjonens 172 medlemsland, inklusive USA, Kina, India og Brasil.

Hvorvidt norske myndigheter kan begjære håndhevelsestiltak gjennomført på grunnlag av en privatrettslig avtale etter Lugano-konvensjonen eller New York-konvensjonen vil bero på en konkret vurdering av den enkelte avtale. For Lugano-konvensjonens del vil et vesentlig moment være om myndighetenes rettigheter etter avtalen går utover rettigheter enhver privat borger kunne hatt. Etter New York-konvensjonen vil det være vesentlig om det er forhold som tilsier at avtalen ikke kan avgjøres av voldgift, jf. konvensjonen artikkel II nr. 1.

5. Adgangen til å pålegge vilkår

5.1 Oversikt

Det å stille som vilkår at virksomheter skal ha bestemte strukturer eller handle på bestemte måter innebærer at virksomhetene pålegges plikter. Etter norsk rett kan ingen private rettssubjekter pålegges plikter uten et rettsgrunnlag. Plikter kan blant annet etableres gjennom avtale og myndighetsutøvelse.

I det følgende redegjør jeg nærmere for adgangen til å stille vilkår gjennom avtale og myndighetsutøvelse.

5.2 Avtaler

Enhver kan ved avtale forplikte seg til å gjøre eller unnlate noe. Det gjelder også for private parter i deres relasjoner med staten. Staten kan derfor blant annet inngå avtale om kjøp av digital infrastruktur (fysisk anskaffelse), eller avtale bruk av slik infrastruktur (anskaffelse av tjenester). I slike avtaler kan det tas inn vilkår som innebærer at virksomheter som leverer infrastruktur eller tjenester forplikter seg til ha bestemte organisasjonsstrukturer, å handle på bestemte måter, eller unnlate å foreta visse handlinger.

Staten kan som eier også inngå avtaler som stiller vilkår for noens bruk av statens eiendom eller eiendeler. I den grad staten er eier av fast eiendom, der digital infrastruktur er plassert, eller staten eier selve den digitale infrastrukturen, kan staten i utgangspunktet kreve at den som skal inngå avtale om bruk av infrastrukturen oppfyller vilkår, herunder at virksomheter som bruker infrastrukturen skal ha bestemte strukturer eller handle på bestemte måter.

Det er klart at avtaleforhold mellom staten og private parter både er regulert av kontraktsrettens og den offentlige rettens regler. I utgangspunktet gjelder kontraktsrettens regler om når bindende avtale er inngått, hva som er riktig ytelse, og krav ved mangelfull eller forsinket ytelse også for avtaler mellom staten og private. I tillegg gjelder forvaltningsloven all forvaltningsvirksomhet, og de alminnelige reglene i lovens kapittel II og III får kommer derfor også til anvendelse når det inngås avtaler med private parter. Hvorvidt forvaltningslovens regler om enkeltvedtak (kapittel IV) også gjelder beror på en temmelig sammensatt vurdering, hvor det sentrale er om avtalen er inngått under utøvelse av offentlig myndighet. Forvaltningslovutvalget har oppsummert de sentrale momentene for denne vurderingen slik:

> «I vurderingen tas det hensyn til hvilket samfunnsområde avtalen er gjort på, hva formålet med avtalen er, om det dreier seg om fordeling av et knapphetsgode, og hvilken motytelse den private parten må svare. Jo mer balansert avtalen er med hensyn til fordelingen av rettigheter og plikter, desto mindre offentligrettslig preg har den. På den annen side vil avtaler på områder hvor det offentlige skal dekke grunnleggende behov for innbyggerne, som på helse-, omsorgs- og utdanningssektoren, ofte bli regnet som myndighetsutøving.»[2]

Når staten inngår rent kommersielle avtaler skal det ikke anses som utøvelse av offentlig myndighet. Jeg legger her til grunn at i den grad det er aktuelt å inngå avtaler om at virksomheter som eier eller kontrollerer kritisk digital infrastruktur forplikter seg til ha bestemte organisasjonsstrukturer eller å handlinger eller unnlatelser, vil det være tale om kommersielle avtaler. Er det tale om å bruke offentlig myndighet til å pålegge private parter vilkår må reglene om myndighetsutøvelse overholdes (se nedenfor). Jeg legger for ordens skyld til at statens kommersielle avtaler med private kan være underlagt andre offentligrettslige regler enn forvaltningslovens kapittel II og III, avhengig av hva kontrakten går ut på. Blant annet følger det av Grunnloven § 75 at det er opp til Stortinget å bevilge penger til de avtalene staten inngå, og gjelder avtalen en offentlig anskaffelse kommer anskaffelsesreglene til anvendelse jf lov om offentlige anskaffelser.

I tilfeller der selskap som eier kritisk digital infrastruktur i Norge, enten inngår i en konsernstruktur eller i en annen kompleks eierstruktur, må det vurderes om det er tilstrekkelig å inngå avtale med selskapet eller om det også bør inngås avtale med andre deler av konsernet eller eierne. Dette fordi det er en viss mulighet for at konsernet, eller andre eiere, kan omgå de vilkår som kun hviler på det selskapet som eier infrastruktur i Norge, gjennom restruktureringer eller andre selskapsrettslige disposisjoner.

[2] Se NOU 2019: 5, s. 436-436.

Det er en risiko for omgåelse av avtalte vilkår fordi det også i konsernforhold er slik at det kun er det selskapet som har inngått en avtale som er bundet av denne. Hovedregelen er at et konsernselskap ikke er ansvarlig for å oppfylle et annet konsernselskaps forpliktelser. Selv om det i konsernforhold kan være noe lavere terskel for at et selskaps avtale med utenforstående, skal være bindende for andre selskaper i konsernet,[3] er det ingen automatikk i at en avtale med et selskap blir bindende for andre selskap innenfor samme konsern. For å redusere risikoen for at avtalte vilkår blir omgått gjennom restruktureringer eller andre selskapsrettslige disposisjoner, bør eventuelle avtaler om vilkår ikke bare inngås med selskap som eier eller kontrollerer kritisk digital infrastruktur i Norge, men også med det konsernet selskapet eventuelt inngår i eller andre eiere som står bak selskapet.

5.3 Kravet til rettsgrunnlag for myndighetsutøvelse

5.3.1 Rettslige utgangspunkter – legalitetsprinsippet og vilkårslæren

Staten kan pålegge private parter plikter gjennom utøvelse av offentlig myndighet. Når pliktene går ut på at virksomheter skal ha bestemte strukturer eller handle på bestemte måter, og dette ikke kan forankres i avtale eller eierrådighet, er det nødvendig med hjemmel i lov.

Grunnloven § 113 gir et formelt uttrykk for kravet om lovhjemmel for inngrep. Bestemmelsen lyder: «Myndighetenes inngrep overfor den enkelte må ha grunnlag i lov.»

Høyesterett har tolket bestemmelsen som uttrykk for et «grunnleggende prinsipp at myndighetshandlinger og myndighetsbeslutninger skal være forankret i folkeflertallets vilje», og at det betyr at «[d]en utøvende makt … ikke [kan] gå lenger i sin maktbruk overfor borgerne enn det fullmaktene fra lovgiver gir uttrykk for».[4]

Når forvaltningen pålegger plikter overfor private parter vil det være en form for maktbruk som krever forankring i Stortinget. Er pliktene av et visst omfang vil de anses som «inngrep», som etter ordlyden i Grunnloven § 113 krever «grunnlag i lov».

Selv om Grunnloven § 113 etter ordlyden kun omhandler inngrep mot «den enkelte» er det klart bestemmelsen også gjelder inngrep overfor andre private rettssubjekter, som aksjeselskaper og andre foretak.[5] Det innebærer at vilkår som stilles til selskaper og andre virksomheter må ha hjemmel i lov, dersom vilkårene er å anses som «inngrep».

Krever myndighetene at sensitive eiendeler eller eiendom ekskluderes fra et oppkjøp, eller at virksomheten vedtar bestemmelser som hindrer nye eiere i å utøve stemmerett, delta i virksomhetens styre, eller få tilgang til sensitiv informasjon skal det anses som «inngrep» etter § 113, og krever derfor i utgangspunkt «grunnlag i lov». Det å pålegge slike plikter kan

[3] Se HR-2017-1932-A avsnitt 102
[4] HR-2018-1907-A, avsnitt 49
[5] Se for illustrasjon HR-2018-1907-A, der Høyesterett vurderte Grunnloven § 113 i en sak hvor et aksjeselskap var part.

etter omstendighetene også anses som inngrep i både markeds- og menneskerettigheter beskyttet av EMK og EØS.

Har lovgivningen forutsatt at visse handlinger krever tillatelse fra forvaltningen, og forvaltningen i tillegg er gitt en viss frihet til å velge om tillatelse skal gis, er det antatt at dette gir et tilstrekkelig lovgrunnlag for å stille vilkår for tillatelsen. Synspunktet og det sentrale innholdet i denne såkalte vilkårslæren er at når forvaltningen kan gjøre det mer, nekte tillatelse, kan forvaltningen også gjøre det mindre, stille vilkår for en tillatelse. Forutsetningen er imidlertid at vilkår har en saklig sammenheng med tillatelsen, og ikke er uforholdsmessig tyngende. I tillegg er det, som jeg kommer tilbake til nedenfor i forbindelse med EØS-retten, en forutsetning at rammene for forvaltningens frihet til å velge om det skal gis tillatelse ikke er for upresise.

Det medfører at i de tilfeller lovgivningen krever godkjenning for visse erverv av eierandeler i selskaper, og forvaltningen er gitt frihet til å vurdere om godkjennelse skal gis, kan det i utgangspunktet stilles vilkår for ervervet.

For øvrig må lovgivningen tolkes for å ta stilling til om forvaltningen kan pålegge private plikter, og i tilfelle hva slags plikter.

Dersom det er tale om å pålegge plikter på selskaper som eier ellet kontrollerer kritisk digital infrastruktur i Norge, må det vurderes om det er tilstrekkelig å kun treffe vedtak rettet mot det aktuelle selskapet. I tilfeller der selskapet inngår i en konsernstruktur eller i en annen kompleks eierstruktur, er det mulig at vilkår ikke vil ha nødvendig effekt om det ikke også treffes vedtak rettet mot andre deler av konsernet eller eierne, så fremt lovgivning gir hjemmel til det. Dette fordi det er en viss mulighet for at et konsern eller andre eiere kan omgå de vilkår som kun hviler på det selskapet som eier kritisk digital infrastruktur i Norge, gjennom restruktureringer eller andre selskapsrettslige disposisjoner.

For å redusere risikoen for at vilkår blir omgått gjennom restruktureringer eller andre selskapsrettslige disposisjoner, bør altså eventuelle vilkår ikke bare pålegges selskap som eier eller kontrollerer kritisk digital infrastruktur i Norge, men etter omstendighetene, også med det konsernet selskapet eventuelt inngår i eller andre eiere som står bak selskapet, så fremt lovgivningen gir nødvendig hjemmel, og det ligger innenfor det norske myndigheter kan vedta i kraft av deres jurisdiksjon.

Det er klart at Grunnloven, EMK, og EØS-avtalen stiller krav til tolkning av norsk lovgivning som gir hjemmel til å foreta inngrep. Før jeg går nærmere inn på tolkningen av de konkrete lovhjemlene for å stille vilkår i sikkerhetsloven skal jeg derfor redegjøre for de overordnede krav Grunnloven, EMK, og EØS-avtalen stiller for at lovbestemmelser kan gi forvaltningen kompetanse til å pålegge private plikter.

5.2.2 Grunnlovens hjemmelskrav

Oversikt

Lovkravet i Grunnloven § 113 stiller ikke bare krav om at inngrep må ha hjemmel i lov, men krever også at hjemmelen må være tilstrekkelig for forvaltningens inngrep.[6]

I det følgende redegjør jeg kort for hvilke krav til hjemmel som må stilles til de inngrep, som kan bli aktuelt å gjennomføre overfor virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge.

Deretter redegjør jeg for om hjemmelskravet går så langt at dette, tolket i lys Grunnloven, stiller noen minstekrav til presisjonen i inngrepshjemler.

Krav til hjemmel for strukturelle og adferdsbaserte vilkår

Høyesterett har formulert det slik at vurderingen av om en lovhjemmel gir tilstrekkelig hjemmel for et inngrep vil bero på en konkret vurdering. I avgjørelsen inntatt i Rt 1995 s. 530 (Fjordlaks) uttrykte førstvoterende dette slik:

> «Jeg antar, med bakgrunn i teori og rettspraksis, at kravet til lovhjemmel må nyanseres blant annet ut fra hvilket område en befinner seg på, arten av inngrepet, hvordan det rammer og hvor tyngende det er overfor den som rammes. Også andre rettskildefaktorer enn loven selv må etter omstendighetene trekkes inn.»

Flere har hevdet at jo sterkere inngrep jo klarere krav til hjemmelens klarhet. [7] Det tilsier at er nødvendig med klar lovhjemmel for tyngende inngrep som for eksempel pålegg om at en aktør skal selge deler av sin virksomhet. Som Tobiassen har vist i en nylig undersøkelse av Høyesterettspraksis må dette utgangspunktet likevel modifiseres.[8] Legalitetsprinsippet kan være en skranke i de tilfeller det er tale om svært generell og upresis ordlyd, og inngrepet går betydelig lenger enn forarbeidene gir dekning for. Legalitetsprinsippet kan også være en skranke i de tilfeller inngrepets tyngende karakter ikke står i rimelig forhold til de grunnene som kan anføres for at lovhjemmelen skal være tilstrekkelig.[9]

Den siste av disse to ovennevnte skrankene er i realiteten uttrykk for en helhetsvurdering hvor det skal svært mye til for at Høyesterett kommer til at en lovbestemmelse ikke gir hjemmel. Høyesteretts anvendelse av den første av de nevnte skrankene gir derimot en viss veiledning om hvor vid en lovbestemmelse kan være før den ikke lenger kan anses som hjemmel for inngripende vedtak. [10]

Jeg antar derfor at for å stille konkrete vilkår til en virksomhet, er det i utgangspunktet tilstrekkelig at lovens ordlyd kan tolkes som en kompetanse til å pålegge virksomheten plikter for å drive lovlig. Det er ikke nødvendig at loven spesifiserer hvilke plikter som kan pålegges

[6] For en utførlig gjennomgåelse med referanser til tidligere teori, se Nicolai Skjerdal, *Kvalitative hjemmelskrav*, 1998.
[7] Erik Boe, *Innføring i juss: Statsrett og forvaltningsrett*, 1993, s. 663.
[8] Se Tomas Midttun Tobiassen, *Når myndighetene griper inn, En studie av legalitetsprinsippet i Høyesteretts praksis*, 2019.
[9] Tomas Midttun Tobiassen, *Når myndighetene griper inn, En studie av legalitetsprinsippet i Høyesteretts praksis*, 2019, s. 123.
[10] Se for eksempel Rt. 2004 s. 1603.

virksomhetene, gitt at de plikter som virksomheten blir pålagt ligger innenfor lovens formål. For at myndighetene skal ha kompetanse til å pålegge virksomheter plikt til å handle på bestemte måter, er det derfor i utgangspunktet tilstrekkelig at lovbestemmelsen gir myndighetene kompetanse til å gripe inn i virksomhetenes frihet, det er ikke nødvendig at lovbestemmelsene angir at myndighetene kan gripe inn med nærmere angitte vilkår. Er det tale om å pålegge en virksomhet å endre en allerede lovlig struktur, kan det innebære krav om oppsplitting av en virksomhet, som går lenger enn pålegg om hva virksomheten kan og ikke kan gjøre i kraft av den strukturen virksomheten har. Det tilser at inngrepshjemler ikke uten videre gir adgang til å pålegge strukturelle tiltak, uten at det har holdepunkter i formålet med loven, ordlyden eller forarbeider.

Når lovgivningen gir forvaltningen frihet til å vurdere om tillatelser skal gis, følger det som nevnt ovenfor av vilkårslæren at myndighetene også har frihet til å stille vilkår for tillatelsen. Forvaltningen har i slike tilfeller også frihet til å velge hvilke vilkår som skal stilles, så lenge vilkårene har saklig sammenheng med tillatelsen, ikke er uforholdsmessig tyngende og for øvrig ligger innenfor lovens formål. Er disse vilkårene oppfylt kan det både pålegges adferdsregulerende og strukturelle vilkår. Tilsvarende gjelder der loven gir forvaltningen frihet til å vurdere om tillatelser skal gis, og uttrykkelig sier at det kan stilles «vilkår» for tillatelsen.

Videre står norske myndigheter relativt fritt til å velge hvilke vilkår som skal pålegges virksomheter som eier eller kontroller kritisk digital infrastruktur, selv om lovhjemmelen for å pålegge vilkår er generelt utformet, forutsatt at vilkårene ikke er uforholdsmessig tyngende eller går betydelig lenger enn det forarbeidene gir dekning for.

Minstekrav til utforming av inngrepshjemler

Et ytterligere spørsmål er om Grunnloven stiller krav til presisjon i inngrepshjemler. Hensynene bak Grunnloven § 113, domstolenes plikt til kontrollere lovligheten av forvaltningens vedtak etter § 89, og rettsstatsformålet i Grunnloven § 2 tilsier at inngrepshjemler ikke bør være for upresise.

Når det gjelder § 113 har Høyesterett oppsummert de sentrale hensyn bak bestemmelsen i Rt. 2014 s. 1105 (Acta):

> «Lovkravet fremmer forutberegnelighet og legger til rette for at den enkelte kan treffe rasjonelle valg. Det motvirker vilkårlighet og usaklig forskjellsbehandling, jf. også Grunnloven § 98 første ledd som slår fast at «[a]lle er like for loven». Lovkravet støtter Stortingets lovgiverfunksjon etter Grunnloven § 75 [bokstav] a og den demokratiske ideen som ligger bak ordningen med at lovgivningskompetansen er hos en folkevalgt nasjonalforsamling: Den utøvende makt kan ikke gå lenger i sin maktbruk overfor borgerne enn det fullmaktene fra lovgiver gir grunnlag for.»[11]

[11] Rt. 2014 s. 1105 (Acta), avsnitt 26. Dommen avsagt under dissens 4-1. Førstvoterendes uttalelser om hensynene bak legalitetsprinsippet fikk støtte av flertallet og har senere blitt gjentatt i flere avgjørelser, blant annet HR-2016-1286-A og HR-2018-1907-A.

I den grad lovgivningen gir forvaltningen betydelig frihet til selv å velge når det skal gripes inn overfor den enkelte og hva inngrepet skal gå ut på, vil muligheten til å forutberegne sin rettsstilling gjennom lovgivningen bli svekket, og inngrepene vil også få en svakere demokratisk forankring. Det tilsier at lovgivningens inngrepshjemler bør angi både betingelsen som må være oppfylt for at forvaltningen kan gripe inn, og rammer for hva inngrepet kan gå ut på.

Det har også vært hevdet at Grunnloven setter grenser for hvor vid adgang forvaltningen skal ha til selv å velge i hvilke tilfeller det skal treffes enkeltvedtak og hva slik vedtak skal gå ut på. Castberg sier det slik:

> «Jo videre spillerum en lov gir forvaltningsorganene skjønn i deres myndighetsutøvelse, desto mindre blir den reelle verdi av myndighetenes forankring i lov. Det er utvilsomt en grense for hva grunnloven her tillater. En lov som helt generelt ville bemyndige politiet til å verne om det offentliges interesser ved inngrep overfor borgerne, ville være grunnlovsstridig.»[12]

Videre fremholder Castberg at provisorisk anordning av 31. august 1936 er et eksempel på en kompetansetildeleing som i prinsippet var for vidtgående.[13] Ordlyden var:

> «Når en utlending, hvis ophold eller virksomhet her i riket finnes å være i strid med statens interesser, ikke vil eller ikke kan forlate landet, kan Justisdepartementet beslutte at han skal være undergitt sådanne innskrenkninger med hensyn til bevegelsesfrihet og samkvem med andre som departementet bestemmer.»

Castberg mente riktignok at kompetansetildelingen kunne være innenfor Grunnlovens grenser, fordi det var mulig at Grunnloven stilte strengere krav til inngrep mot norske borgere enn inngrep mot utlendinger. Overfor norske borgere var Castberg imidlertid ikke i tvil. En så vidtgående kompetansetildeling «ville ha vært i strid ned det legalitetsprinsipp som vår forfatning bygger på».

Det har likevel ikke vært noen enighet om hvor Grunnlovens grenser for kompetansetildeling går, og ingen lov har så langt blitt satt til side fordi den går utover disse grensene. Den nevnte provisoriske anordningen fra 1936 har heller ikke av alle vært ansett som et typetilfelle på en for vidtgående kompetansetildeling. Torkel Opsahl omtaler den samme anordningen i Delegasjon av Stortingets lovgivningsmyndighet, og kommenterer at den neppe var i strid med noen lov.[14]

Andenæs har derimot i sin fremstilling av Norges statsforfatning uttalt seg i samme retning som Castberg:

> «Legalitetsprinsippet regnes for et prinsipp av grunnlovs rang, og det må være en grense for hvor langt lovgivningen kan gå i å utvanne hjemmelskravet.»

[12] Castberg 1964, s. 14
[13] Se Castberg 1964, s. 14.
[14] Opsahl, s. 325.

Videre er det antatt at kjernen i domstolens konstitusjonelle adgang til å kontrollere forvaltningen, som siden 2020 har kommet til uttrykk i Grunnloven § 89, er at lovgivningen ikke kan «legge en avgjørelse til et forvaltningsorgan på en slik måte at domstolene ikke har rett til å prøve om et vedtak skyldes maktmisbruk fra vedkommende forvaltningsorgans side».[15] Den «maktmisbruk» det er forutsatt at domstolene alltid kan kontrollere er forvaltningens «overskridelse av grensen for vedkommende myndighet eller fullmakt (ultra vires), anvendelse av myndigheten til et annet formål enn det loven har fastsatt (détournement de pouvoir) og krenkelse av likhetsgrunnsetningen».[16] Det er åpenbart at domstolens kontroll av om forvaltningen har overskredet grensene for sin myndighet blir nærmest illusorisk, dersom de grensene loven angir for forvaltningens myndighet er så upresise at det i praksis ikke kan kontrolleres om forvaltningen er utenfor eller innenfor grensene. Som nærmere utdypet nedenfor har det likevel blitt akseptert at lovgivningen kan begrense domstolskontrollen på et avgrenset område, med mindre begrensningene går så langt at større grupper av tvister på sentrale rettsområder blir unndratt kontroll.[17]

Kravene til legalitet og domstolskontroll er også sentrale deler av rettsstaten, som det har vært antatt at Grunnloven har beskyttet, og som siden 2012 har vært nedfelt i Grunnloven § 2. Selv om det er vanskelig å utlede noe konkret innhold fra forarbeidene til Grunnloven § 2, er ikke uttrykket «rettsstaten» kun et honnørord. Slik dommer i Høyesterett, Ingvald Falch, har utlagt kjernen i begrepet, er særlig to kjennetegn sentrale ved rettsstaten: «rettsbinding sikret av uavhengige domstoler».[18] Rettsbindingen består i at offentlige myndigheter er bundet av retten, som er noe annet enn at uavhengige domstoler kontrollerer om rettsbindingen etterleves. Videre fremholder Falch også andre sentrale kjennetegn ved rettsstaten, blant annet at «rettsreglene, i alle fall som utgangspunkt, [må] være gjort kjent på *forhånd*, det vil si før borgerne foretar de handlinger hvis lovlighet skal bedømmes.»[19] Det vil klart nok svekke rettsstaten dersom lovbestemmelser ikke setter vilkår for i hvilke tilfeller forvaltningen kan gripe inn i, og heller ingen annen konkret regulering av hva inngrepene kan gå ut på. Slike bestemmelser reduserer den rettslige bindingen av, og muligheten for å føre rettslig kontroll med, forvaltningen. Dessuten vil slike lovbestemmelser føre til at private parters mulighet til å forutsi sin rettsstilling også blir redusert.

Selv om det konstitusjonelle vernet av legalitetsprinsippet, domstolskontrollen med forvaltningen og rettsstaten svekkes av upresise lovbestemmelser som gir et

[15] Forvaltningskomiteens innstilling (1958) s. 369. Formålet med grunnlovsfestingen av domstolenes legalitetskontroll med forvaltningen i 2020 var ikke å endre rettstilstanden, men å grunnlovfeste «den etablerte ordningen» med domstolskontroll av forvaltningen, se Innst.258 S (2019–2020) s. 1. Forvaltningskomiteens uttalelser i 1958 om domstolskontrollens konstitusjonelle kjerne er derfor fortsatt relevant, også for tolkningen av Grunnloven § 89, slik den lyder i dag.
[16] Forvaltningskomiteens innstilling (1958) s. 369.
[17] Se Rt. 2012, s. 519, avsnitt 81, Johs. Andenæs, *Statsforfatningen i Norge*, 8. utgave 1998, s. 287 og den mer utførlige drøftelsen i Olav Haugen Moen*, Forvaltningsskjønn og domstolskontroll*, 2019, s. 125-130.
[18] Ingvald Flach, «Rettstatens betydning», *Lov og rett* 2021, s.43-57, på s. 48.
[19] Falch 2021, s. 49.

forvaltningsorgan stort spillerom, er det i løpet av de siste hundre år likevel vedtatt flere slike bestemmelser, enten i lov, eller i provisorisk anordning.[20]

Høyesterett har i likhet med Stortinget heller ikke tolket Grunnloven slik at legalitetsprinsippet, domstolskontrollen med forvaltningen og rettsstaten setter strenge krav til hvordan lovgivningen skal utformes. Høyesterett har akseptert at lovgivningen legger forholdsvis omfattende begrensninger på domstolskontrollen med forvaltningen. I forbindelse med etableringen av Gjenopptakelseskommisjonen ble straffeprosessloven endret i 2001, slik at alle gjenopptakelsessaker ble flyttet fra domstolene til det nye forvaltningsorganet (Gjenopptakelseskommisjonen). Spørsmålet om loven hindret domstolene fra å kontrollene kommisjonen kom opp i dommen i Rt 2012 s. 519. Saken gjaldt gyldigheten av en beslutning truffet av kommisjonen, og Høyesterett i storkammer kom til at loven måtte tolkes slik at domstolene kunne prøve kommisjonens generelle lovtolkning og etterlevelse av grunnleggende saksbehandlingsregler, men at domstolene ikke kunne overprøve kommisjonens konkrete rettsanvendelse, blant annet fordi loven ga anvisning på til dels «meget skjønnsmessige vurderinger.»[21] En slik begrensning i domstolskontrollen ble ansett for å være forenlig med det konstitusjonelle vernet av domstolenes kontroll med forvaltningen. Det bærende synspunktet så ut til være at det er tilstrekkelig for å oppfylle Grunnlovens krav at forvaltningsvedtak kan bringes inn «for domstolene for prøving, og [at] «domstolene har et visst minimum av overprøvingskompetanse».

Det må etter avgjørelsen være klart at det ikke er i strid med det konstitusjonelle vernet av domstolenes kontroll med forvaltningen, om kontrollen beskjæres «på et avgrenset område».

Det kan likevel reises spørsmål om det er forenelig med den formelle forankringen rettsstaten og legalitetsprinsippet nå har fått i Grunnloven §§ 2 og 113, å vedta lovhjemler som gir myndighetene kompetanse og frihet til å pålegge private plikter, som ikke har presise vilkår for i hvilke tilfeller det kan treffes enkeltvedtak, eller noen konkrete rammer for hva enkeltvedtakene helt konkret kan gå utpå. Det er for så vidt klart at selv slik lovgivning ikke vil gi forvaltningen frihet til å treffe enkeltvedtak med et innhold som er strid med Grunnlovens menneskerettigheter eller andre overordnete rettsnormer. Likevel er det ikke gitt at lovhjemler som ikke setter ytterligere rammer for i hvilke tilfeller forvaltningen kan gripe inn overfor den enkelte og hva inngrepene kan gå utpå, går for langt i å utfordre kjernen i den hensyn som Høyesterett har lagt til grunn at legalitetsprinsippet og rettsstaten skal ivareta.[22] På bakgrunn av rettskildematerialet er det neppe mulig å gi et generelt svar på spørsmålet.

Oppsummert må det bero på en sammensatt vurdering om lovgivningen går for langt i å utfordre legalitetsprinsippets og rettsstatens kjerne, når det ikke settes presise betingelser

[20] Noen eksempler er provisorisk anordning av 31. august 1936 (nå opphevet) om tiltak overfor utlendinger, provisoriske anordning av 8. mai 1945 om prisregulering mv. (nå opphevet), prisloven av 1953 § 23 (nå opphevet), lov av 1953 om oppfinnelser av betydning for rikets forsvar § 6, og forurensningsloven § 40 andre ledd.
[21] Rt 2012 s. 519, avsnitt 76.
[22] se Rt. 2014 s. 1105, avsnitt 26, HR-2020-2472-P (Klimadommen), avsnitt 123, og HR-2021-417-P (Acer), avsnitt 80.

for i hvilke tilfeller forvaltningen kan gripe inn overfor den enkelte og heller ikke rammer for hva inngrepene kan gå utpå. Relevante momenter i denne vurderingen må blant annet bero på hva slags forvaltningsområdet det gjelder, om de aktuelle lovbestemmelsene i realiteten omfatter hele eller deler av det aktuelle forvaltningsområdet, og hvorvidt lovens formål setter snevre eller vide rammer for hvilke inngrep forvaltningen kan foreta.

5.2.3 EMKs hjemmelskrav

EMK rettighetsbeskyttelse innebærer krav om at inngrep i rettigheter må kunne kontrolleres og bygge på tilstrekkelig presis hjemmel. Kravet til domstolskontroll og presise hjemler henger sammen.

EMK artikkel 6 krever blant annet at enhver skal ha rett til en rettferdig og offentlig rettergang, for å få avgjort sine borgerlige rettigheter og plikter. Den europeiske menneskerettighetsdomstolen (EMD) har tolket bestemmelsen slik at den krever at domstolene kan foreta reell kontroll av om forvaltningens avgjørelser er lovlige. En illustrasjon av dette er EMDs avgjørelse i Obermeier mot Østerrike. Saken gjaldt suspensjon av en delvis ufør arbeidstaker, som etter loven måtte godkjennes av et særskilt forvaltningsorgan. Et sentralt spørsmål i saken var om nasjonale domstoler hadde foretatt en tilstrekkelig kontroll med det særskilte forvaltningsorganets vurdering av om suspensjonen burde godkjennes. I den forbindelse uttalte EMD:

> "In this respect it must be taken into account that the relevant legislation does not contain any substantial and precise provisions for the decisions to be taken by the Disabled Persons Board or the Provincial Governor. From this silence of the law, the Austrian Administrative Court has itself inferred that the Administrative Court can only determine whether the discretion enjoyed by the administrative authorities has been used in a manner compatible with the object and purpose of the law. This means, in the final result, that the decision taken by the administrative authorities, which declares the dismissal of a disabled person to be socially justified, remains in the majority of cases, including the present one, without any effective review exercised by the courts."[23]

EMDs vurdering var altså at EMKs krav til en rettferdig rettergang ikke var oppfylt når lovens bestemmelser ikke ga domstolene anledning til å prøve annet enn om organet hadde gått utover lovens formål. Det tilsier at det vil være i strid med EMK-artikkel 6 om en lovhjemmel er slik utformet at domstolene ikke kan kontrollere annet enn om norske myndigheter har gått utenfor lovens formål. Det er i så fall et strengere krav til lovhjemlers presisjon enn det som følger av Grunnloven.

Basert på EMDs praksis kan det reises spørsmål om det er i strid med EMK artikkel 6 å anvende lovhjemler som angir så upresise kriterier for vurderinger av om forvaltningens beslutninger er lovlige, at domstolene i realiteten kun kan kontrollere om forvaltningen har gått utenfor lovens formål. Det vil nok likevel være å trekke avgjørelsen i Obermeier mot

[23] Se Obermeier mot Østerrike 28. juni 1990, avsnitt 70.

Østerrike for langt at det alltid vil være i strid med EMK-artikkel 6 om en lovhjemmel er utformet på den måten at domstolene i realiteten ikke kan kontrollere annet enn om norske myndigheter har gått utenfor lovens formål. Så lenge loven angir kriterier for å vurdere lovligheten av myndighetenes beslutninger, vil det ikke nødvendigvis være i strid med EMK artikkel 6 at kriteriene er upresist utformet, så lenge nasjonale domstoler kan prøve om kriteriene er tolket riktig.[24] Dersom domstolene i tillegg kan prøve om en avgjørelse bygger på riktig faktum, om saksbehandlingsregler er fulgt, vil det også gi ytterligere holdepunkter for at kravet til rettferdig rettergang er overholdt. Videre vil kravene til presis utforming av lovgivningen antageligvis heller ikke være så strenge når det gjelder forvaltningen av nasjonal sikkerhet, hvor statene må ha nokså stor frihet til å utøve skjønn ved vurdering av hvilke tiltak som er best egnet for å ivareta sikkerheten.

Videre er det etter EMK klart at inngrep krever lovhjemmel, legitimt formål og en begrunnelse for hvorfor inngrepet er et nødvendig og forholdsmessig tiltak i et demokratisk samfunn. På den bakgrunn har EMD blant annet presisert hva som kan ansees som tilstrekkelig hjemmel.

Vilkår som pålegges virksomheter som eier eller kontrollerer kritisk digital infrastruktur kan blant annet tenkes å gripe inn i flere EMK-rettigheter. Som illustrasjon antar jeg for eksempel at visse strukturelle vilkår som påbud om salg av deler av virksomhet eller eiendom etter omstendighetene kan være inngrep i EMK tilleggsprotokoll 1 artikkel 1 (EMK P1-1). Bestemmelsen lyder slik:

> «Enhver fysisk eller juridisk person har rett til å få nyte sin eiendom i fred. Ingen skal bli fratatt sin eiendom unntatt i det offentliges interesse og på de betingelser som er hjemlet ved lov og ved folkerettens alminnelige prinsipper.»

EMK P1-1 er inkorporert som norsk lov jf. Menneskerettsloven av 1999 § 2. Ved motstrid går EMK P1-1 foran annen formell lov, jf. Menneskerettsloven § 3 jf. § 2. Det er på det rene at inngrep i eiendomsretten, for eksempel krav om at noen avstår deler av sin virksomhet krever hjemmel, og at det stilles krav til hjemmelens kvalitet.[25]

Det grunnleggende avgjørelsen om hva som skal anses som tilstrekkelig hjemmel for inngrep i rettigheter vernet av EMK er Sunday Times mot Storbritannia, som riktignok ikke gjaldt inngrep i eiendomsretten, men inngrep i ytringsfriheten.[26] Den delen av avgjørelsen som gjelder lovkravet er likevel utformet helt generelt og er også gjentatt i senere avgjørelse, og har av den grunn betydning for hvilke krav som skal stilles til hjemmelen for inngrep i blant annet eiendomsretten. Det EMD sier om lovkravet er:

> «In the Court's opinion, the following are two of the requirements that flow from the expression 'prescribed by law'. First, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as a ' law ' unless it is formulated with sufficient precision to enable the citizen to regulate his

[24] Se i denne retning Zumbotel mot Østerrike, 21. september 1993, avsnitt 32 og 33.
[25] Se for eksempel Carbonara og Ventura mot Italia, 30. mai 2000, avsnitt 64.
[26] Se Sunday Times mot Storbritannia 26. april 1979.

> conduct: he must be able – if need with appropriate advice – to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. Those consequences need not be foreseeable with absolute certainty: experience shows this to be unattainable. Again, whilst certainty is highly desirable, it may bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice.»[27]

Av de to delene av lovkravet som EMD her tar opp her, er det det andre som er en relevant skranke mot for vide lovhjemler. EMDs poeng ser ut til å være at kravet om rettsgrunnlag for inngrep i rettighetene forutsetter at normene er så presise at borgerne på forhånd kan vite under hvilke vilkår inngrep i rettighetene kan skje, og hva slags inngrep det vil være tale om. Slik kan man i rimelig grad forutse hva som blir de rettslige konsekvensene av ens handlinger.

Når det gjelder inngrep i eiendomsretten etter EMK P1-1 har EMD uttrykt dette slik i Carbonara og Ventura mot Italia: «the requirement of lawfulness means that rules of domestic law must be sufficiently accessible, precise and foreseeable»[28]

EMDs krav til presisjon i rettsgrunnlaget er imidlertid ikke nødvendigvis et krav om presisjon i lovtekst. Kravene kan oppfylles også av andre rettskildefaktorer, såfremt de er offentlige og tilgjengelige for allmennheten. Eksempelvis kan forvaltningsinstrukser og andre direktiver som ikke er rettslig bindende, få betydning ved vurderingen av om rettsgrunnlaget er tilstrekkelig presist.[29] EMD har blant annet uttrykt dette slik:

> «the Court considers that although those directives did not themselves have the force of law, they may to the admittedly limited extent to which those concerned were made sufficiently aware of their contents - be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the Rules»[30]

Det er altså ikke nødvendigvis et krav om at presist rettsgrunnlag må være nedfelt i lovtekst, en generell lov som lest i lyst av offentlig tilgjengelig forarbeider som presiserer hjemmelen vil kunne oppfylle presisjonskravet.

5.2.4 EØS-avtalens hjemmelskrav

Oversikt

EØS-rettens regler om de fire friheter stiller også krav til tolkning av hjemler for inngrep. Dels kan ikke lovgivningen tolkes slik at det den gir forvaltningen kompetanse til å pålegge vilkår som er uforholdsmessige inngrep i EØS-avtalens rettigheter. Dels stiller EØS-avtalen minstekrav til hvordan lovgivningen skal utformes for at den skal gi forvaltningen hjemmel til å pålegge private parter plikter. Gir en lovbestemmelse en for vid og upresis hjemmel for forvaltningen, vil det å ha bestemmelsene i seg selv kunne anses som en uforholdsmessig restriksjon på retten til fri bevegelse av varer, personer, tjenester og kapital på tvers av

[27] Se Sunday Times mot Storbritannia 26. april 1979, avsnitt 49.
[28] Se Carbonara og Ventura mot Italia, 30. mai 2000, avsnitt 64.
[29] Se Silver m.fl. mot Storbritannia 25. mars 1983, avsnitt 86-88.
[30] Se Silver m.fl. mot Storbritannia 25. mars 1983, avsnitt 88.

landegrensene, og derfor være i strid med EØS-avtalens forpliktelser. I det følgende redegjør jeg nærmere for de EØS-reglene som setter rammer for hvor vide og upresise forvaltningens lovhjemler kan være.

Først presenterer jeg helt kort hovedtrekk ved EU-domstolens vurderinger av lovhjemlers presisjon og betydning av disse vurderingene for EØS-avtalen og regler om investeringskontroll. Deretter redegjør jeg nærmere for betydning av lovgivningens rammer for forvaltningsskjønn, ved EU- og EFTA-domstolens vurderinger av om regler om investeringskontroll er lovlige restriksjoner. Videre behandler jeg EUs forordning om screening av investeringer (investeringsscreening),[31] og betydning av disse reglene for tolkningen av EØS-avtalens regler. Avslutningsvis sammenfatter jeg EØS-rettens krav til investeringskontroll og adgangen til å gjøre unntak fra disse kravene.

Hovedtrekk ved EU-domstolens vurdering av lovhjemlers presisjon mv.

Når lovgivningen ikke angir presise betingelser for vurderinger av om forvaltningen skal treffe avgjørelser, overlates i realiteten slike vurderinger til forvaltningens eget skjønn. Og uten presise kriterier for skjønnsutøvelsen er det vanskelig å forutsi hvordan forvaltningens skjønn vil bli utøvd. Fordi det kan virke dempende på transaksjoner i et marked, om aktørene ikke på forhånd kan vite om transaksjoner vil bli ansett lovlige, kan upresis lovgivning som gir forvaltningen stor frihet til å utøve skjønn, føre til mindre aktiviteter på markedene. Blant annet på den bakgrunn har EU-domstolen i flere saker lagt til grunn at det å gjøre retten til fri bevegelighet betinget av forvaltningens skjønn, i seg kan utgjøre en restriksjon på den rett EU-traktatene gir til fri bevegelighet på tvers av landegrenser.[32] I en eldre foreleggelsessak, som gjaldt fri bevegelse av varer, uttalte EU-domstolen i 1983 helt generelt at «Freedom of movement is a right whose enjoyment may not be dependent upon a discretionary power or on a concession granted by the national authorities.»[33]

Bakgrunnen for uttalelsen er at det vil virke begrensende på økonomisk virksomhet i EUs indre marked om aktørene ikke på forhånd kan vite om grensekryssende transaksjoner er lovlige, men må avvente hvordan myndighetene utøver skjønn.[34]

For øvrig er EU domstolens uttalelse om at retten til fri bevegelighet ikke kan være betinget av forvaltningsskjønn helt generell og kan derfor ikke uten videre tas til inntekt for en allmenn regel. Snarere er det tale om et uttrykk for et utgangspunkt for vurderinger av om det å gi forvaltningen skjønn er forenelig med retten til fri bevegelighet. Som et slikt utgangspunkt illustrerer uttalelsen imidlertid at enhver nasjonal regel, også regler om investeringskontroll, kan anses som en restriksjon, dersom retten til å utøve fri bevegelighet er betinget av forvaltningsskjønn. Som jeg kommer tilbake til nedenfor er det imidlertid klart at i den grad forvaltningsskjønn i seg selv anses som en restriksjon på retten til fri

[31] Se Europaparlaments- og rådsforordning (EU) 2019/452 av 19. mars 2019 om et regelsett for kontroll av utenlandske direkteinvesteringer i unionen.
[32] Se Christoffer C. Eriksen, *The European Constitution, Welfare States and Democracy: The four freedoms vs. national administrative discretion*, 2011.
[33] Se sak 124/81 avsnitt 10.
[34] Eriksen 2011

bevegelighet, kan skjønnet rettferdiggjøres dersom det kan begrunnes i EU-rettens unntaksregler.

Fordi EU-domstolens avgjørelser om tolkning av grunnfrihetene før 1992 er bindende for tolkningen av EØS-avtalen, må den nevnte uttalelsen også legges til grunn ved tolkning av EØS-rettens regler om fri bevegelighet. Det innebærer i hvert fall som et utgangspunkt at retten til fri bevegelighet heller ikke i EØS kan være betinget av skjønn, men at skjønnet må kunne rettferdiggjøres dersom det anses som en restriksjon.

Etter EU-domstolens praksis er det klart at nasjonale ordninger som kan utgjøre en hindring for eller begrensning av erverv av aksjer og avholde investorer fra andre medlemsstater i å investere i slike virksomheter, skal anses for å utgjøre «restriksjoner» etter TEUV artikkel 63, som beskytter kapitalfriheten.[35] Er ervervet av en slik art at erververen får en innflytelse på virksomheten som gjør at vedkommende kan treffe avgjørelse om dets drift, vil ervervet være beskyttet av etableringsretten etter TEUV artikkel 49.[36] I utgangspunktet vil nasjonale ordninger anses som «restriksjoner» etter denne bestemmelsen, når de kan hemme utøvelsen av etableringsretten eller gjøre utøvelsen av etableringsretten mindre attraktiv.[37] Tilsvarende gjelder ved tolkning av EØS-avtalens artikkel 31 og 40.[38]

Det er klart at regler som krever at myndighetene godkjenner investeringer i en virksomhet, vil gjøre det mindre attraktivt å foreta investeringer. Slike godkjenningsregler er derfor ansett som «restriksjoner» på etableringsretten og kapitalfriheten, både av EU-domstolen og av EFTA-domstolen.[39] Og som nærmere utdypet nedenfor har begge domstolene i flere saker kommet til at slike restriksjoner ikke kan forsvares som forholdsmessige restriksjoner, dersom godkjenningsordningen gir myndighetene et skjønn som ikke er avgrenset av presise og tilgjengelige kriterier.

I EU domstolens praksis er det imidlertid ikke bare krav om godkjenning av investeringer som er ansett som restriksjoner. I tillegg har EU-domstolen kommet til at det også kan anses som restriksjoner å ha regler som gir myndigheter kompetanse til å stanse eller pålegge aktører plikter, etter at de har gjennomført investeringer eller transaksjoner.[40] Et fellestrekk i noen av de forholdsvis få sakene hvor EU-domstolen har ansett slike regler for å være restriksjoner på fri bevegelighet er at de aktuelle reglene gir myndighetenes kompetanse til å utøve skjønn som ikke er avgrenset av presise kriterier.[41] Ett eksempel er EU-domstolens avgjørelse i en traktatbruddsak mot Frankrike, C-483/99.

Et av spørsmålene i saken gjaldt om den franske finansministerens myndighet til å stanse enhver beslutning om å overføre eller pantsette verdiene av utenlandske datterselskap i et

[35] Se for eksempel C-543/08, avsnitt 47.
[36] Se for eksempel C-251/98, avsnitt 22.
[37] Se for eksempel C-55/84, avsnitt 37.
[38] Se blant annet E-9/11, avsnitt 82.
[39] Se for illustrasjon EU-domstolens sak C-483/99, se særlig avsnittene 37, 41, 42 og 56, og EFTA-domstolens sak E-9/11, særlig avsnitt 79-82.
[40] Eriksen 2011
[41] Se blant annet C-483/99, avsnitt 52 og 53 og C-318/10, avsnitt 27 og 28.

fransk oljeselskap (Société Nationale Elf-Aquitaine). Om kompetansen til å stanse slike transaksjoner uttalte EU-domstolen:

> «Even though what is involved here is not a system of prior authorisation but a system of opposition ex post facto, it is common ground that the exercise of that right is likewise not qualified by any condition limiting the wide discretion of the minister concerned regarding controls on the identity of the holders of the assets of the subsidiary companies. It follows that the system clearly goes beyond what is necessary in order to attain the objective pleaded by the French Government, namely the prevention of disruption of a minimum supply of petroleum products in the event of a real threat. Moreover, the French legislative provisions in issue do not reflect any such limitation.
>
> Since the structure of the system established does not include any precise, objective criteria, the legislation in issue goes beyond what is necessary in order to attain the objective indicated.»[42]

På det grunnlag konkluderte EU-domstolen blant annet med at det var i strid med reglene om fri bevegelighet av kapital å ha en bestemmelse i kraft som tildeler den franske staten en aksje i Elf-Aquitaine, som gir staten:

> «the right to oppose any decision to transfer or use as security … the majority of the capital of four subsidiaries of [Elf-Aquitaine]».

Selv om EU-domstolens ikke sier det direkte, forutsetter konklusjon at reglene om etterfølgende kontroll også anses som «restriksjoner» på kapitalfriheten.

Skjønn og investeringskontroll

Det er klart at avgrensningen av myndighetenes skjønn er et sentralt element i EU-domstolens vurderinger av om regler om investeringskontroll er lovlige restriksjoner regler om etableringsrett og kapitalfrihet. Forutsetningen er at restriksjonene er begrunnet i henholdsvis TEUV artikkel 52 eventuelt EØS-avtalen artikkel 33, eller almene hensyn, dersom det er tale om nasjonalitetsnøytrale restriksjoner.

Statenes anvendelse av de nevnte unntaksreglene er underlagt en forholdsvis streng domstolskontroll, også når det gjelder sikkerhetshensyn. Illustrerende er tolkningen av reglene om fri bevegelse av kapital. Her har EU-domstolen i en sak om franske regler for kontroll av utenlandske investeringer lagt til grunn at de hensyn medlemsstatene angir som begrunnelse for å anvende unntaksreglene må kunne overprøves av EUs institusjoner, og kun aksepteres dersom det er reelle grunner til å påberope de aktuelle hensynene:

> «It should be observed, first, that while Member States are still, in principle, free to determine the requirements of public policy and public security in the light of their national needs, those grounds must, in the Community context and, in particular, as

[42] Se C-483/99, avsnitt 52 og 53.

> derogations from the fundamental principle of free movement of capital, be interpreted strictly, so that their scope cannot be determined unilaterally by each Member State without any control by the Community institutions. Thus, public policy and public security may be relied on only if there is a genuine and sufficiently serious threat to a fundamental interest of society. Moreover, those derogations must not be misapplied so as, in fact, to serve purely economic ends.»[43]

For at unntaksreglene skal kunne påberopes av statene, må restriksjonene ikke bare være begrunnet i lovlige hensyn, i tillegg må restriksjonene være egnete og nødvendige virkemidler for å ivareta disse hensynene. Ved denne vurderingen har EU-domstolen i en rekke saker kommet til at det er uforholdsmessig, og etter hvert også i strid med prinsippet om rettssikkerhet (legal certainty) at medlemsstatene har lovbestemmer som gir nasjonale forvaltning for vid skjønnsmyndighet til å godkjenne meldinger om oppkjøp eller andre forhold.

EU-domstolens praksis er fulgt opp av EFTAs EØS-institusjoner. Blant annet har EFTAs overvåkningsorgan (ESA) fremholdt at norsk lovgivning har gitt forvaltningen et så vidt skjønn at retten til fri bevegelighet har blitt uforholdsmessig begrenset. Illustrerende er ESAs «letter of formal notice» angående lov av 1994 om erverv av næringsvirksomhet. I ESAs pressemelding, som oppsummerte brevet, het det:

> «It is the Authority's view that a system requiring an administrative authorisation involves a certain degree of discretion, creates legal uncertainty for investors and is, consequently, liable to hinder or make less attractive the exercise of the freedom of establishment and the free movement of capital. As the rules have not been justified they must be regarded contrary to the EEA Agreement.»[44]

Den norske regjeringen protesterte mot ESAs vurdering, men foreslo likevel å oppheve hele loven. Stortinget sluttet seg til forslaget og loven om erverv av næringsvirksomhet ble opphevet i 2002.[45]

Videre har EFTA-domstolen også lagt til grunn at legal certainty setter grenser for hvor vide skjønn lovgivningen kan gi. I sak E-9/11 som gjaldt regler om eierkontroll i den tidligere børsloven, uttalte EFTA-domstolen:

> «In a case where the acquisition of shareholdings and the exercise of voting rights above a certain threshold are based on exceptions to main rules that provide for an outright ban, legal certainty calls for those exceptions to be sufficiently clear and precise.»[46]

I samme sak la EFTA-domstolen også til grunn de krav EU-domstolen har anvendt i tilsvarende saker ved prøving av om skjønnet er uforholdsmessig:

[43] Se sak C-54/99, avsnitt 17 (referanser utelatt).
[44] Se ESA PR(00)06.
[45] Jf Lov om oppheving av lov om erverv av næringsverksemd, ikraft fra 1. juli 2002.
[46] Se sak E-9/11, avsnitt 99.

> «In this regard, the Court recalls that, while the principle of legal certainty does not preclude the conferral of discretionary powers on the competent authorities, a system of prior administrative approval must be based, as a general rule, on objective, non-discriminatory criteria which are known in advance to the undertakings concerned. All persons affected by a restrictive measure of that type must have a legal remedy available to them».[47]

EUs regler om screening av investeringer

Ved tolkning av EØS-reglene om kravene til presisjon i lovgivning om eierskapskontroll for sikkerhetsformål har det en viss betydning at det i EU, som ledd i EUs handelspolitikk er vedtatt en forordning om investeringsscreening med hjemmel i TEUV artikkel 207.[48] EUs felles handelspolitikk er ikke EØS-relevant, og forordningen er derfor ikke tatt inn i EØS-avtalen. Forordningen om investeringsscreening har likevel betydning for tolkningen av EØS-avtalens bestemmelser, da EØS-avtalens bestemmelser om fri etableringsrett og kapitalflyt i EØS-avtalens artikkel 31 og 40 setter grenser for hvordan det kan utøves kontroll med investeringer i EØS. En sak er at investorer utenfra EØS-området kan få tilgang til EUs indre marked via Norge og EØS-avtalen, dersom Norge ikke praktiserer like streng screening som EU.[49] En annen sak, som har direkte rettslig betydning for tolkning av EØS-avtalens bestemmelser om etableringsrett og kapitalflyt er at disse skal tolkes i samsvar med de tilsvarende bestemmelsene i TFEU, henholdsvis artikkel 49 og 63.[50]

EU-kommisjonen har videre vurdert forordningen om invetseringsscreening etter TFEU artikkel 63, fordi denne i motsetning til EØS-avtalen artikkel 40, både gjelder kapitalbevegelser mellom medlemsland og mellom medlemsland og tredjeland. Etter EU-kommisjonens vurdering er forordningen en restriksjon på fri kapitalbevegelse, men likevel lovlig fordi den er utformet i samsvar med unntaksreglene og alminnelige EU-rettslige prinsipper:

> «Investment screening mechanisms may represent a restriction on the free movement of capital which, however, may be justified when necessary and proportionate for the achievement of the objectives defined in the Treaty, including on public security and public policy grounds (Article 65 TFEU) or for overriding reasons in the general interest, as defined by the Court of Justice of the European Union.
>
> As clarified in the case law of the Court of Justice, whereas Member States enjoy discretion in determining public policy and public security requirements in the light of their national needs, those public interests cannot be determined unilaterally by the Member States without any control by the institutions of the EU and must be interpreted strictly: they may be relied on only if there is a genuine and sufficiently

[47] Se sak E-9/11, avsnitt 100.
[48] Se mer utførlig om dette i NOU 2023: 28, punkt 8.3 og Charlotte Hafstad, ««Weaponization» av eierskap og norske eierskapskontrollregler»», *Lov og rett* 2023, s. 303-324.
[49] Hafstad 2023.
[50] Se C-452/01 Ospelt

> serious threat to a fundamental interest of society. […] Furthermore, investment screening mechanisms should comply with the general principles of EU law, in particular the principles of proportionality and legal certainty. These principles require that the procedure and the criteria for the investment screening are defined in a non-discriminatory and sufficiently precise manner. Potential investors must be able to know such mechanisms in advance and to seek judicial review.
>
> The proposed Regulation is consistent with these requirements. It confirms that Member States may screen foreign direct investments on grounds of security or public order and sets out basic procedural requirements for Member State's screening mechanisms, such as transparency, non-discrimination between different third countries and judicial review.»[51]

Etter EØS-avtalen artikkel 40 kan det heller ikke etablere restriksjoner på kapitalflyt med mindre de kan begrunnes som nødvendige og forholdsmessige tiltak for å ivareta lovlige hensyn, som for eksempel sikkerhetshensyn. Det innebærer at regler for screening som er restriksjoner på kapitalflyt ikke bare må være begrunnet i sikkerhetshensyn, for å være lovlige etter EØS-avtalen og EØS-loven. I tillegg må slike screening regler – og praksis – være forholdsmessige, det vil si ikke gå lenger enn det som er nødvendig for å begrense kapitalflyten i EØS. For å etablere regler for investeringskontroll som er i samsvar med forpliktelsene etter EØS-avtalen artikkel 40 kan derfor den nevnte forordningen om investeringsscreening tjene som en mal for norske myndigheter.[52] For tolkningen av EØS-avtalen bestemmelser om kapitalflyt er det uansett nødvendig å gå noe nærmere inn på forordningens innhold.

Før jeg går nærmere inn på innholdet i forordningen om investeringsscreening gjør jeg oppmerksom på EU-kommisjonen ikke har vurdert forordningen etter reglene om etableringsrett, fordi disse reglene kun gjelder mellom EUs medlemsland og ikke mellom EUs medlemsland og tredjeland. I EØS-området er det imidlertid klart at også regler om investeringskontroll må utformes i samsvar med reglene om fri etableringsrett i EØS-avtalen artikkel 31. I utgangspunktet vil en investering være beskyttet av etableringsfriheten dersom investor fra EØS får kontroll i et norsk selskap, mens kapitalfriheten beskytter investeringer som ikke leder til slik kontroll. Det innebærer at i den grad norske myndigheters etablerer regler for eierskapskontroll som er restriksjoner på etableringsretten, kan ikke disse restriksjonene være uforholdsmessige.

Forordningen om investeringsscreening angir virkeområde gjennom definisjoner av sentrale begreper som screening og utenlandske direkte investeringer. Med «screening» sikter forordningen til prosedyrer som gjør det mulig å vurdere, undersøke, tillate, betinge, forby eller avvikle utenlandske direkte investeringer.[53] Utenlandske direkte investeringer er definert som enhver investering foretatt av en utenlandsk investor med det formål å etablere

[51] Se EU-kommisjonens Explanatory Memorandum, COM(2017) 487 final.
[52] Se også Hafstad 2023, s. 306.
[53] Forordning 2019/452, artikkel 2 nr. 3.

eller opprettholde varige og direkte forbindelse mellom den utenlandske investoren og den som kapitalen stilles til rådighet for (investeringsobjektet).[54] Forutsetningen er at investeringen blir gjort med tanke på utøvelse av økonomisk aktivitet i en medlemsstat. Den vide definisjonen omfatter også investeringer som gjør det mulig med effektiv deltakelse i ledelsen av eller kontrollen med en virksomhet som utøver økonomisk aktivitet.

Videre regulerer forordningen medlemsstatenes mekanismer for screening av de aktuelle investeringene, og stiller krav til hvordan slike mekanismer skal utformes. Forordningen stiller ikke krav om at medlemsstatene skal gjennomføre screening, men stiller krav til de medlemsstatene som har eller skal innføre screening av hensyn til sikkerheten eller den offentlige orden.[55] Blant annet stiller forordnings artikkel 3 nr. 2 følgende krav:

> «Rules and procedures related to screening mechanisms, including relevant timeframes, shall be transparent and not discriminate between third countries. In particular, Member States shall set out the circumstances triggering the screening, the grounds for screening and the applicable detailed procedural rules.»

Formålet med kravet til transparens er å sikre at investorene, Kommisjonen og de øvrige medlemsland kan få innblikk i hvordan investeringer vil kunne bli screenet.[56]

Kommisjonen foreslo i januar 2024 en ny forordning om investeringsscreening.[57] Forslaget, om det blir vedtatt, vil blant annet innebære et krav om at medlemsstatene skal etablere en screening mekanisme jf artikkel 3 nr. 1. Minimumskravene til innholdet i slike mekanismer bygger videre på forordning 2019/452, men presiser blant annet kravene til utformingen av disse mekanismene. Det heter i forslagets artikkel 4 nr. 1 at:

> «Rules and procedures related to screening mechanisms, and measures taken pursuant to such rules and procedures, shall comply with Union law, be transparent and shall not discriminate between third countries or between the Member States in which the foreign investor's subsidiary in the Union is established»

En endring fra forordning 2019/452 er uttrykket «shall comply with Union law». Det er ikke et nytt krav, men snarere en presisering som også sier noe om rettstilstanden per i dag. I fortalen er uttrykket begrunnet slik:

> «(12) Screening foreign investments should be carried out in accordance with this Regulation, taking into account all factual information available and adhering to the principle of proportionality and other principles enshrined in the Treaties. Moreover, the screening of foreign investments which are carried out through subsidiaries of the foreign investor established in the Union should in all cases comply with the

[54] Forordning 2019/452, artikkel 2 nr 1.
[55] Forordning 2019/452, artikkel 3 nr 1.
[56] Forordning 2019/452, fortale, avsnitt 15.
[57] Se COM(2024) 23 final

requirements stemming from Union law, and in particular with the Treaty provisions on freedom of establishment and free movement of capital, as interpreted in the case law of the Court of Justice of the European Union, consistently with the objective of preserving an open and inclusive internal market. Any restrictions to the freedom of establishment and free movement of capital in the Union, including the screening and measures arising from screening, such as mitigating measures and prohibitions should be based on a genuine and sufficiently serious threat to a fundamental interest of society, and should be appropriate and necessary as set out in the case law of the Court of Justice. At the same time, when assessing the justification and proportionality of a restriction, the specificities of investments within the Union operated through a subsidiary of a foreign investor may be taken into account when assessing any restrictions on freedom of establishment or to the free movement of capital, including where appropriate in any Commission opinion adopted pursuant to this Regulation. This should be done taking into account the integration of Member State schemes into a Union-wide cooperation mechanism.»

Samlet sett tilsier gjeldende praksis fra EU og EFTA-domstolen, forordningen om invetseringsscreening, forslaget til ny forordning, og Kommisjonens begrunnelser og forklaringer av dette regelverket, at screeningmekanismer må bygge på de prinsipper som rettspraksis har utviklet i saker om eierskapskontroll, for å være i samsvar med primærrettens krav om etableringsrett og kapitalflyt. Det innebærer at i den grad reglene er restriksjoner på grunnfrihetene, er det ikke tilstrekkelig at reglene er begrunnet i sikkerhetshensyn etter EØS-avtalen 33 eller andre lovlige allmenne hensyn. Utformingen av reglene må i tillegg både være forholdsmessige, og overholde prinsippet om rettssikkerhet (legal certainty). Det betyr blant annet at reglene må være ikke-diskriminerende, og tilstrekkelig presise til at potensielle investorer kjenner til mekanismene på forhånd, og har tilgang til domstolkontroll. Uten å oppfylle disse kravene vil screening mekanismer neppe være i samsvar med gjeldende forordnings krav om at regler og prosedyrer for screening mekanismer må være transparente, jf. forordning 2019/452 artikkel 3 nr. 2.

Etter min vurdering kan det kun gjøres unntak for de nevnte EØS-rettslige kravene til utforming av regler om investeringskontroll dersom de kan begrunnes i EØS-avtalen artikkel 123. Etter denne bestemmelsen er ikke EØS-retten til hinder for enkelte nærmere angitte tiltak. Det er tale om tiltak som blant annet «angår produksjon av eller handel med våpen, ammunisjon og krigsmateriell eller andre varer som er uunnværlige for forsvarsformål, eller forskning, utvikling eller produksjon som er uunnværlig for forsvarsformål». Og tiltak som den enkelte stat anser som «vesentlig for sin sikkerhet i tilfelle av alvorlig indre uro som truer den offentlige orden, i krigstid eller ved alvorlig internasjonal spenning som innebærer en fare for krig, eller for å oppfylle forpliktelser den har påtatt seg med sikte på å opprettholde fred og internasjonal sikkerhet».

Det er imidlertid antatt at terskelen for å anvende EØS-avtalen artikkel 123 er høy, og tiltak som begrunnes i bestemmelsen må uansett ikke gå lenger enn det som er nødvendig for å ivareta formålet. Jeg går nærmere inn på bestemmelsen nedenfor, ved vurderingen av om

EØS-avtalens krav er ivaretatt ved utformingen av sikkerhetslovens hjemler for å stille vilkår til virksomheter som eier eller kontrollerer kritisk digital infrastruktur.

6. Hjemmelsgrunnlag

6.1 Innledning- sikkerhetslovens hjemler

I norsk lovgivning har det vært en rekke bestemmelser som har gitt myndighetene kompetanse til å pålegge virksomheter plikter i forbindelse med ulike tillatelsesordninger. For muligheten til å pålegge risikoreduserende vilkår for virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge, er det i dag først og fremst sikkerhetslovens lovhjemler som er relevante. Loven har tre bestemmelser som gir Kongen i statsråd kompetanse til å stille vilkår overfor virksomheter som eier eller kontrollerer digital infrastruktur i Norge, jf sikkerhetsloven §§ 2-5, 9-4 og 10-3.

Jeg nevner for ordens skyld at annen lovgivning også inneholder enkelte bestemmelser om tillatelser og inngrep som etter omstendighetene også gir hjemmel for å pålegge plikter til virksomheter som eier eller kontrollerer kritisk digital infrastruktur. Blant annet krever E-komloven tillatelse for ulike former for bruk av digital infrastruktur,[58] eksportkontrolloven krever tillatelse for eksport som også kan omfatte utførsel av data innhentet fra digital infrastruktur, og konkurranseloven både har bestemmelser om både inngrep og tillatelser for visse foretakssammenslutninger som også kan gi hjemmel for å stille vilkår til virksomheter som eier eller kontrollerer kritisk digital infrastruktur. [59]

I det følgende redegjør jeg for hovedinnholdet i sikkerhetsloven § 2-5, § 9-4 og 10-3 og hva slags vilkår de gir hjemmel for å pålegge, forholdet mellom bestemmelsene, og deretter om de er så generelle og vage at de ikke kan anvendes som rettsgrunnlag for å fastsette vilkår for virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge.

6.2 Inngrepshjemmelen - § 2-5

6.2.1 Ordlyden

Sikkerhetsloven § 2-5 første setning er en generell inngrepshjemmel. Bestemmelsen gir «Kongen i statsråd» kompetanse til å «fatte nødvendige vedtak for å hindre sikkerhetstruende virksomhet eller annen planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet»

Flere av begrepene i ordlyden er definert i lovens § 1-5. Forarbeidene har også omfattende kommentarer og merknader til flere av begrepene. For å klargjøre innholdet i bestemmelsen er det derfor nødvendig å tolke de enkelte delene av bestemmelsen i lys av både § 1-5 og forarbeidene.

6.2.2 «sikkerhetstruende virksomhet»

Bestemmelsens første alternativ, hindre «sikkerhetstruende virksomhet» er nærmere definert i lovens § 1-5 nr 4 og ytterligere utdypet i forarbeidene. Etter lovens § 1-5 nr. 4 skal

[58] Se bestemmelsene om nekting av tilkopling eller frakopling av radio- og terminalutstyr jf § 2-5 fjerde ledd og bruk av frekvenser i det elektromagnetiske frekvensspekteret jf § 6-2.
[59] Se også oversikten i NOU 2023: 28, kapittel 6.

uttrykket «sikkerhetstruende virksomhet» forstås som «tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser». Det nærmere innholdet i slike handlinger er presisert av departementet:

> «Tilsiktede handlinger som direkte kan skade vil si handlinger der intensjonen er å påføre en eller annen form for skade på nasjonale sikkerhetsinteresser, og hendelser forårsaket av slike handlinger. Dette vil blant annet kunne omfatte sabotasje- eller terroraksjoner der målet er å ramme en viktig samfunnsfunksjon, for slik å forsøke å skade myndighetenes styringsevne …. Med tilsiktede handlinger som indirekte kan skade, menes handlinger der intensjonen ikke nødvendigvis er å skade nasjonale sikkerhetsinteresser, men der konsekvensen eller hendelsen som følger av den tilsiktede handlingen kan skade sikkerhetsinteressene. Dette vil for eksempel kunne innebære etterretningsoperasjoner fra en fremmed stat, der målet ikke nødvendigvis er å skade norske interesser, men snarere å fremme egne interesser gjennom å skaffe sensitiv informasjon som kan gi den fremmede staten et fortrinn overfor Norge. Slik etterretningsinformasjon kan i en tilspisset situasjon eller i en forhandlingssituasjon mellom den fremmede staten og Norge potensielt skade norske interesser.».[60]

Etter bestemmelsens første ledd kan det derfor treffes vedtak for å hindre bestemte handlinger, som sabotasje- eller terroraksjoner eller etterretningsoperasjoner fra en fremmed stat, der målet ikke nødvendigvis er å skade norske interesser, men snarere å fremme egne interesser gjennom å skaffe sensitiv informasjon som kan gi den fremmede staten et fortrinn overfor Norge.

6.2.3 «nasjonale sikkerhetsinteresser»

Paragraf 2-5 andre alternativ, planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for at «nasjonale sikkerhetsinteresser blir truet» skal tolkes langt videre enn første alternativ. Begrepet om nasjonale sikkerhetsinteresser er ifølge departementet «en utvidelse av den tidligere lovs begrep om vitale nasjonale sikkerhetsinteresser:

> «Nasjonale sikkerhetsinteresser gis videre en legaldefinisjon i lovforslagets § 1-5, som omfatter både de tre overordnede interessene og underkategoriene i bokstav a til e. Dette gir en konkret avgrensning for hvilke interesser loven er ment å skulle beskytte, for å fjerne den usikkerheten som har vært knyttet til det sammenliknbare begrepet vitale nasjonale sikkerhetsinteresser i gjeldende sikkerhetslov. Ved å utelate vitale i angivelsen av interessene, mener departementet at lovens virkeområde skal tolkes videre enn hva tilfellet er med dagens lov, men innenfor tydelige rammer.»[61]

Slik «nasjonale sikkerhetsinteresser» er definert i sikkerhetslovens § 1-5 nr. 1, er det tale om et begrep som omfatter enkelte mer avgrensete kategorier av interesser som «landets suverenitet, territorielle integritet og demokratiske styreform», og en videre kategori, «overordnede sikkerhetspolitiske interesser». Etter loven er det et krav om at disse

[60] Prop. 153 L (2016 –2017), s. 36.
[61] Prop. 153 L (2016 –2017), s. 33.

sikkerhetspolitiske interessene må være «knyttet til» bestemte forhold angitt i § 1-5 nr 1. bokstav a til e.

Forarbeidene setter rammer for tolkningen av de forholdene som er listet opp i § 1-5 nr 1.[62] Det medfører at det er grenser for hva Kongen i statsråd kan påberope som grunnlag for å treffe vedtak etter § 2-5. Disse rammene er imidlertid ikke bare tydelige, deler av rammene er både vide og upresise. Rammene for hva som kan påberopes som grunnlag for å treffe vedtak etter § 2-5 er derfor ikke like «tydelige» som departementet forutsetter at de skal være.

Etter forarbeidene er det for så vidt klart at sikkerhetsloven bokstav § 1-5 a til c skal tolkes i lys av begrepet om statssikkerhet som har et avgrenset innhold, jf Prop. 153 L (2016-2017), s. 33. Det er først og fremst forholdene som nevnes i § 1-5 bokstav d og e som er vide og upresise.

Bokstav d gjelder «økonomisk stabilitet og handlefrihet». I proposisjonen legger departementet til grunn at dette blant annet kan omfatte «stabil utvikling i makroøkonomiske hovedstørrelser som inflasjon, valutakurs, vekst og sysselsetting, stabile kapitalforhold overfor utlandet, velfungerende systemer for å håndtere offentlige ytelser og inntekter, og stabilitet i den finansielle infrastrukturen og finansmarkedene for øvrig».[63] Etter dette alternativet kan altså Kongen i statsråd treffe vedtak etter § 2-5 dersom det er overordnete sikkerhetspolitiske interesser knyttet til risiko for at utviklingen i makroøkonomiske hovedstørrelser er truet.

Bokstav e gjelder «samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet», og skal ifølge departementet tolkes slik at det favner «både infrastruktur og objekter som er avgjørende for at sivilsamfunnet skal fungere» jf prop. 153 L (2016-2017), s. 35. Etter dette alternativet kan det altså treffes vedtak etter § 2-5 dersom det er overordnete sikkerhetspolitiske interesser knyttet til risiko for at blant annet kritisk digital infrastruktur er truet.

6.2.4 «planlagt eller pågående aktivitet»

Vedtak for å hindre «planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet» kan etter dette treffes for å hindre en rekke ulike former for aktivitet. Dette er tilsiktet av departementet, som i merknadene til bestemmelsen klargjør at uttrykket «aktivitet» skal tolkes vidt:

> «Begrepet aktivitet favner vidt. Både iøynefallende aktiviteter som f.eks. oppføring av bygninger eller utplassering av antenner, og mindre synlige aktiviteter, som f.eks. planer om utbygging, ferdsel i et område eller oppkjøp av virksomheter, omfattes av begrepet. […] Hvilke typer aktivitet bestemmelsen er ment å ramme er verken mulig eller hensiktsmessig å angi nærmere konkret. Bestemmelsen er ment å være en sikkerhetsventil for å kunne hindre enhver aktivitet, uavhengig av hvordan disse materialiserer seg. Det avgjørende vil være hvorvidt aktiviteten har potensial til å

[62] Prop. 153 L (2016-2017), s. 33-35.
[63] Prop. 153 L (2016-2017), s. 35

> innebære en ikke ubetydelig risiko mot nasjonale sikkerhetsinteresser. Det er ikke krav om at aktiviteten må rette seg direkte mot virksomheter som er omfattet av loven. Også aktivitet som mer indirekte eller avledet innebærer en ikke ubetydelig risiko mot nasjonale sikkerhetsinteresser, vil etter forholdene kunne omfattes av bestemmelsen», Prop. 153 L (2016 –2017), s. 168 (min understrekning).

En forutsetning for å stanse aktivitet etter sikkerhetsloven § 2-5 er at aktiviteten medfører en «ikke ubetydelig risiko» for at nasjonale sikkerhetsinteresser blir truet. Uttrykket forekommer så vidt jeg vet kun i sikkerhetsloven, men brukes her i flere bestemmelser enn i § 2-5. Uttrykket finnes blant annet også i lovens § 9-4 og § 10-3.

6.2.5 «ikke ubetydelig risiko»

Formuleringen «ikke ubetydelig risiko» kom inn som en del av flere nye bestemmelser i den nå opphevde sikkerhetsloven av 1998, ved en lovendring i 2016. En av de nye bestemmelsene hvor uttrykket ble brukt var § 5 a, som påla virksomheter en varslingsplikt ved «ikke ubetydelige risiko» for nærmere angitte sikkerhetstruende aktivitet, og som ga Kongen i statsråd vid kompetanse til å stanse den aktivitet det ble varslet om. Paragraf 5 a er derved en forløper til det som i dag er sikkerhetsloven § 2-5. Uttrykket «ikke ubetydelig risiko» var med i Forsvarsdepartementets høringsnotat til § 5 a, og i det lovforslag som ble fremmet i Prop. 97 L (2015–2016). Uttrykket «ikke ubetydelig risiko» ble likevel grundigst kommentert i forbindelse med forslaget til ny § 29 a i sikkerhetsloven av 1998 om anskaffelser til kritisk infrastruktur, jf Prop. 97 L (2015–2016), kapittel 11. Vurderingene av uttrykkets innhold har likevel overføringsverdi til tolkningen av den tidligere § 5 a og gjeldende § 2-5. Basert på en rekke høringssvar til regulering av varslingsplikt om offentlige anskaffelser, vurderer departementet innholdet i uttrykket slik:

> «Begrepet «ikke ubetydelig risiko» innebærer at det er situasjoner med risiko ut over det «normale» som skal varsles. Vurderingen vil måtte omfatte både sannsynlighet, sårbarhet og mulige konsekvenser. På sannsynlighetssiden innebærer kriteriet at det normalt ikke skal varsles dersom det kun foreligger en helt fjerntliggende eller rent teoretisk mulighet for at anskaffelsen skal kunne resultere i sikkerhetstruende virksomhet. Det bør være noe konkret med den aktuelle anskaffelsen som tilsier at risikoen er noe høyere enn ved andre anskaffelser. Bestemmelsen innebærer imidlertid ikke et krav om sannsynlighetsovervekt.»[64]

Det er altså klart at uttrykket «ikke ubetydelig risiko» var ment å favne svært vidt, at det ikke stiller krav om sannsynlighetsovervekt, og at det bare i normale tilfeller skal avgrenses mot en «helt fjerntliggende eller rent teoretisk mulighet» for at sikkerhetstrusselen skal inntreffe. For øvrig åpner departementet for at uttrykket «ikke ubetydelig risiko» må tolkes på bakgrunn av at det «i mange tilfeller kan være tilnærmet umulig å gjøre nøyaktige sannsynlighetsberegninger av risikoen» for at handlinger skal inntreffe, og at vurderingene da må konsentreres om «sårbarhet og mulige konsekvenser».[65]

[64] Prop. 97 L (2015–2016), s. 64.
[65] Prop. 97 L (2015–2016), s. 64.

I sikkerhetsutvalgets utkast til ny sikkerhetslov i NOU 2016: 16 ble det foreslått å heve terskelen for i hvilke tilfeller Kongen i statsråd kunne gripe inn. I utkastet til § 2-5 ble uttrykket «ikke ubetydelig risiko» erstattet med uttrykket «stor grad av sannsynlighet». Departementet var imidlertid ikke enig i at terskelen burde heves og begrunnet standpunktet slik:

> «Departementet er enig med Utenriksdepartementet i at utvalgets forslag til skjerping av kravet til sannsynlighet etter gjeldende § 5 a, kan medføre at bestemmelsen mister sin selvstendige funksjon. Departementet har forståelse for at utvalget ut fra bestemmelsens inngripende karakter ønsker å etablere ytterligere rettssikkerhetsgarantier. Bestemmelsen er imidlertid ment å være en sikkerhetsventil, jf. Prop. 97 L (2015–2016) side 19. Bestemmelsen vil eksempelvis kunne benyttes hvor det ikke foreligger andre rettslige grunnlag for å stanse en aktivitet som innebærer en risiko mot nasjonale sikkerhetsinteresser. At vedtaksmyndigheten er lagt til Kongen i statsråd, og skal baseres på råd fra relevante fagmyndigheter, vil sikre at saken er tilstrekkelig godt opplyst, både hva gjelder den konkrete risikoen og hva gjelder hvilke konsekvenser et eventuelt vedtak vil kunne få. Videre vil det sikre at vedtakene dermed er velbegrunnede og proporsjonale ut fra hensynet til nasjonal sikkerhet. Som det framgår av Prop. 97 L (2015–2016) side 21, vil det også måtte vurderes konkret i hvert enkelt tilfelle hvor bestemmelsen vurderes benyttet, hvorvidt vedtaket vil være i overensstemmelse med Grunnloven, menneskerettighetsloven og Norges internasjonale forpliktelser. Departementet har på denne bakgrunn kommet til at det materielle innholdet i gjeldende § 5 a bør videreføres, med nødvendige tilpasninger til den nye loven. Bestemmelsens natur som sikkerhetsventil tilsier at den i likhet med gjeldende § 5 a skal favne vidt, og bør være anvendelig på alle typer aktiviteter som kan innebære en ikke ubetydelig risiko mot nasjonale sikkerhetsinteresser.»[66]

I merknadene til § 2-5 har departementet ytterlige kommentert hva som ligger i uttrykket «ikke ubetydelig risiko»:

> «Bestemmelsen stiller ikke krav om at det må foreligge en viss bestemt sannsynlighet for at aktiviteten vil innebære en risiko mot nasjonale sikkerhetsinteresser dersom den etableres eller gjennomføres. At aktiviteten skal kunne medføre» en ikke ubetydelig risiko, innebærer derimot at vedtaksmyndigheten ikke inntrer hvis dette framstår som usannsynlig, eller det kun er en teoretisk mulighet for det. Terskelen for sannsynlighet må ellers ses i sammenheng med de mulige konsekvensene av den aktuelle aktiviteten. Dersom konsekvensen for nasjonale sikkerhetsinteresser kan bli katastrofal, vil også terskelen for når det fattes vedtak bli lav. Motsatt vil terskelen kunne heves dersom konsekvensen av den aktuelle aktiviteten regnes som liten.»[67]

Basert på departementets vurderinger er det uklart akkurat hvor mye som skal til for at det skal foreligge en «ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet». Samlet sett tilsier forarbeidene at uttrukket «ikke ubetydelig risiko» ikke skal tolkes som et

[66] Prop 153 L (2016-2017), s. 54.
[67] Prop 153 L (2016-2017) s. 168-169.

krav om at det skal foretas bestemte vurderinger av sannsynlighet, men at det i realiteten er tale om en sammensatt helhetsvurdering som i praksis vil være svært vanskelig å etterprøve for domstoler.

6.2.6 «nødvendige vedtak»

Paragraf § 2-5 gir ikke Kongen i statsråd en ubegrenset frihet til å treffe vedtak, ordlyden krever at det kun kan fattes vedtak som er «nødvendige». Etter departementets merknader til bestemmelsen er det klart at kravet om nødvendighet skal innebære en vid forholdsmessighetsvurdering: «at Kongen i statsråd ikke skal fatte mer byrdefulle vedtak enn det som er påkrevd, og som vurderes som rimelig i den konkrete saken.»[68]

6.2.7 Derogasjonshjemmel

Videre fremgår det av § 2-5 annen setning at det kan fattes vedtak etter bestemmelsen «uten hensyn til begrensningene i forvaltningsloven § 35 og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak». Det innebærer at Kongen i statsråd med hjemmel i sikkerhetsloven § 2-5 kan omgjøre ethvert gyldig vedtak, og forby enhver annen lovlig aktivitet (derogasjon). Dette gir en ytterligere utvidelse kompetansen etter bestemmelsen:

> «Bestemmelsen tar høyde for tilfeller der forvaltningen allerede har fattet et vedtak, og det av hensyn til risiko mot nasjonale sikkerhetsinteresser anses nødvendig å omgjøre vedtaket. Videre slås det i bestemmelsen fast at vedtak etter første punktum også kan fattes uten hensyn til om aktiviteten er tillatt etter annen lov eller annet vedtak. Et vedtak av Kongen i statsråd kan derfor i praksis sette til side en rekke ulike former for vedtak og aktiviteter som i utgangspunktet er tillatt, f.eks. nekte gjennomføring eller stille ytterligere vilkår for en byggetillatelse, frekvenstillatelse, ferdselsrett, jaktrett, en våpentillatelse eller et privat oppkjøp av en virksomhet.»[69]

Departementet angir uttrykkelig at bestemmelsen gir hjemmel til å stille ytterligere vilkår til allerede tillatt aktivitet, og det følger for så vidt også av at loven gir hjemmel til å fatte vedtak for å hindre en rekke ulike typer aktiviteter. Det er vanskelig å trekke en grense mot vilkår som ikke kan settes med hjemmel i bestemmelsen, i og med at det som nevnt ovenfor er forutsatt av departementet i lovforarbeidene at «[b]estemmelsen er ment å være en sikkerhetsventil for å kunne hindre enhver aktivitet, uavhengig av hvordan disse materialiserer seg.». Stortinget har derfor ved vedtakelsen av loven akseptert at loven var ment å favne svært vidt. Vilkårene som vedtas med hjemmel i bestemmelsen må likevel være egnet til å fremme lovens formål, og ikke være uforholdsmessig tyngende. Videre gir bestemmelsen ikke hjemmel for å vedta vilkår som kan krenke menneskerettighetene nedfelt i Grunnloven.

6.2.8 Vedtakenes virkeområde

Endelig setter ikke sikkerhetsloven § 2-5 noen grenser for hvem vedtak kan rettes mot. Kongen i statsråd kan derfor med hjemmel i bestemmelsen treffe vedtak rettet både mot virksomheter som er underlagt sikkerhetsloven og andre virksomheter, i tillegg til fysiske personer. Med hjemmel i § 2-5 kan det derfor treffes vedtak om å ikke bare pålegge plikter

[68] Prop 153 L (2016-20176), s. 169.
[69] Prop.153 L (2016–2017), s. 169.

på selskaper som eier eller kontrollerer kritisk digital infrastruktur i Norge. Dersom slike selskap inngår i en konsernstruktur eller i en annen kompleks eierstruktur, kan det også treffes vedtak rettet mot andre deler av konsernet eller eierne, såfremt lovens vilkår er oppfylt og folkerettens jurisdiksjonsregler etterleves (se nedenfor punkt 8).

6.3 Anskaffelser- § 9-4

Sikkerhetsloven § 9-4 gjelder anskaffelser av skjermingsverdig informasjonssystem, objekt eller infrastruktur som «kan innebære en ikke ubetydelig risiko for at … infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet.» Dette skal som nevnt ovenfor tolkes slik at det må foreligge risiko for bestemte handlinger, som sabotasje- eller terroraksjoner eller etterretningsoperasjoner fra en fremmed stat. Er dette vilkåret oppfylt kan Kongen i statsråd etter § 9-4 vedta «at anskaffelsen ikke skal gjennomføres, eller om at det skal settes vilkår for den […] også dersom det er inngått avtale om anskaffelsen».

Bestemmelsen gjelder ikke sikkerhetsgraderte anskaffelser, som er regulert etter lovens § 9-2 og § 9-3. For øvrig forutsetter bestemmelsen at underliggende organer har vurdert sikkerhetsrisiko ved anskaffelsen og varslet departementet om anskaffelsen innebærer risiko, etter henholdsvis sikkerhetsloven § 9-4 første og andre ledd. Kongen i statsråd må likevel kunne fatte vedtak etter bestemmelsen, selv om slikt varsel ikke er gitt, såfremt de øvrige vilkårene er oppfylt.

Etter bestemmelsen er det et vilkår for å treffe vedtak at det foreligger en «ikke ubetydelig risiko for at … infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet». Selv om det er et lavt og ubestemt krav til sannsynlighet, gir definisjonen av uttrykket «sikkerhetstruende virksomhet» en forholdsvis klar avgrensning av i hvilke tilfeller kompetanse kan utøves etter bestemmelsen. For å treffe vedtak er det en forutsetning at det er en viss risiko for at infrastrukturen kan bli rammet av eller brukt til sabotasje- eller terroraksjoner eller etterretningsoperasjoner fra en fremmed stat. Dette er et vilkår som domstolene kan kontrollere.

Videre har departementet i forarbeidene forutsatt at Kongen i statsråd har stor frihet med tanke på hva slags vedtak som kan fattes, dersom vilkårene er oppfylt: «Det kan i prinsippet fattes alle typer vedtak. Den mest inngripende typen vedtak vil være å stanse en anskaffelse som sådan eller å forby bruk av visse leverandører. En mindre inngripende type vedtak er å stille vilkår om å innføre risikoreduserende tiltak.», se Prop.97 L (2015–2016), s. 76

Det er likevel klart at vilkårene må ha saklig sammenheng med vurderingen om å tillate anskaffelsen. Det må med andre ord fastsettes vilkår for å motvirke risiko for at infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet, som blant annet sabotasje- eller terroraksjoner eller etterretningsoperasjoner fra en fremmed stat. Som nevnt i forarbeidene setter formålet med bestemmelsen og loven grenser, slik at det ikke er adgang til å fatte vedtak for å «gripe inn ved risiko for industrispionasje som kun er egnet til å skade en enkeltbedrifts forretningsvirksomhet». Tilsvarende må gjelde ved vilkår, slik at det heller ikke kan stilles vilkår etter bestemmelsen kun for å begrense risiko for slik industrispionasje som kun rammer enkeltbedrifter. Prop.97 L (2015–2016), s. 65.

Videre er det i samsvar med alminnelige tolkningsprinsipper klart at vilkårene ikke kan være uforholdsmessig tyngende. Er det tale om anskaffelse innenfor EØS skal vurderingen av forholdsmessighet foretas i relasjon til eventuelle EØS-rettigheter vilkårene griper inn i.

6.4 Erverv - § 10-3

Sikkerhetsloven § 10-3 gjelder visse kvalifiserte erverv av eierandeler som «kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet». Foreligger slik risiko kan Kongen i statsråd vedta «at ervervet ikke kan gjennomføres, eller om at det skal settes vilkår for gjennomføringen […] også dersom det allerede er inngått avtale om ervervet».

Bestemmelsen er en del av det systemet for investeringskontroll som etableres av lovens kapittel 10. Hovedelementene i dette systemet består av tre trinn, privates meldeplikt, departementets vurderingsplikt og Kongen i statsråds kompetanse til å stanse eller pålegge vilkår for erverv.

Det første trinnet følger av sikkerhetsloven § 10-1 første ledd som pålegger en meldeplikt for «[den som vil erverve en kvalifisert eierandel i en virksomhet som er underlagt [sikkerhets]loven». Meldingen skal sendes til departementet. For virksomheter som ikke er omfattet av «noe departements ansvarsområde» følger det av bestemmelsen at meldingen skal «sendes til sikkerhetsmyndigheten».

Jeg legger til at det i lovvedtak av 20. juni 2023 er besluttet å utvide meldeplikten, slik at den ikke bare gjelder den som vil erverve en eierandel, men også avhenderen av eierandelen og virksomheten ervervet gjelder, jf. § 10-1 andre ledd. Lovendringen er per 28. oktober 2024 ennå ikke satt i kraft.

Forøvrig forutsatte departementet at det ville være kjent hvilke virksomheter som er underlagt sikkerhetsloven:

> «Informasjon om hvilke virksomheter som er underlagt loven vil …også være tilgjengelig hos det departement som har truffet vedtak om å underlegge virksomheten loven, og hos sikkerhetsmyndigheten som vil ha en oversikt over alle virksomheter som er underlagt loven. I dag er informasjonen om hvilke virksomheter som er underlagt loven tilgjengelig på NSMs hjemmesider.»[70]

I dag er det imidlertid ikke offentlig kjent hvilke selskaper som er underlagt loven, og dette får som nærmere utdypet nedenfor i punkt 6.6 betydning for vurderingen av om lovens kapittel 10 etablerer en tilstrekkelig åpen og tilgjengelig prosedyre for investeringskontroll.

Det andre trinnet i lovens system for investeringskontroll innebærer at departementet eller sikkerhetsmyndigheten skal vurdere og «ta stilling til meldingen» jf § 10-2 første ledd, første setning. Videre bestemmer § 10-2 annen setning at den som har meldt inn ervervet skal orienteres innen en frist på «60 arbeidsdager», om ervervet er godkjent eller om saken skal behandles av Kongen i statsråd. Fristen kan avbrytes dersom det fremsettes krav om ytterligere opplysninger jf. § 10-2 andre ledd siste setning.

[70] Prop 153 L (2016-2017), s. 151.

Det er ikke forbudt å gjennomføre ervervet før det er godkjent. I forarbeidene er det likevel forutsatt at det er mest sannsynlig at erverv ikke blir gjennomført før godkjennelse:

> «Departementet ser ikke behov for et gjennomføringsforbud fram til godkjennelse foreligger. Risikoen for at ervervet blir stanset eller reversert, vil etter all sannsynlighet medføre en utsettelse av gjennomføringen til melderen har fått beskjed om ervervet er godkjent, jf. § 10-2, eller om det skal behandles av Kongen i statsråd, jf.§ 10-3.», Prop. 153 L (2016 –2017), s. 151.

Ved lovvedtak av 20. juni 2023 er det besluttet at det ikke lenger skal være adgang til å gjennomføre erverv før utløpet av 60 dagers fristen. Etter den nye ordlyden kan ikke erverv gjennomføres før meldingen er behandlet etter § 10-2, jf. § 10-1 fjerde ledd. Lovendringen er per 28. oktober 2024 ennå ikke satt i kraft.

For departementets vurdering av om erverv skal godkjennes hadde sikkerhetsutvalget foreslått enkelte retningslinjer:

«Ved spørsmål om anvendelse av unntaket må det foretas en konkret vurdering i den enkelte sak. Det må vurderes hvilken sikkerhetsinteresse som skal beskyttes, hva som er sammenhengen mellom sikkerhetsinteressen og inngrepet i eierskapet for det relevante selskapet, og endelig hvorfor det er nødvendig å kontrollere eierskapet for å verne om sikkerhetsinteressen.», jf. NOU 2016:19, s. 239.

Videre forutsatte sikkerhetsutvalget at unntaket kun skal brukes i de tilfeller som er omfattet av EØS-avtalen artikkel 123. Det ville medført at det var en høy terskel for å ikke godkjenne erverv.

Som nevnt ovenfor gir EØS-avtalen artikkel 123 staten adgang til å treffe tiltak i strid med EØS-avtalens regler i tre typer av tilfeller. Det vil være en vesentlig forskjell mellom lovens vilkår for den adgang Kongen i statsråd har til å treffe vedtak etter § 10-3, og departementets vurdering av erverv skulle godkjennes etter § 10-2, dersom departement skulle godkjenne alle erverv med mindre vilkårene var oppfylt etter artikkel 123. Etter § 10-3 kan Kongen i statsråd treffe vedtak når et erverv medfører «en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet». Som nevnt ovenfor skal dette tolkes slik at det ikke gjelder noe krav om sannsynlighetsovervekt for en slik risiko, det er tilstrekkelig at det er en viss risiko for at sikkerhetsinteressene blir truet. Selv om det er usikkerhet om hvordan EØS-avtalen artikkel 123 skal tolkes, tilsier ordlyden at bestemmelsen stiller krav om at det det ikke er tilstrekkelig at det er en viss risiko for at nasjonale sikkerhetsinteresser blir truet, for at staten kan påberope seg unntakene i artikkel 123 bokstav a-c.

Unntaket etter artikkel 123 bokstav a gjelder kun de i tilfeller staten «anser det nødvendig for å hindre spredning av opplysninger som er i strid med dens vesentlige sikkerhetsinteresser». Kravet om nødvendighet er strengere enn «en ikke ubetydelig risiko». Videre, etter artikkel 123 bokstav b er det et unntak for tiltak som angår «produksjon av eller handel med våpen, ammunisjon og krigsmateriell eller andre varer som er uunnværlige for forsvarsformål, eller forskning, utvikling eller produksjon som er uunnværlig for forsvarsformål» (bokstav b). Etter dette alternativet er det avgjørende om et tiltak er begrunnet i forsvarsformål. Det er en

snevrere kategori enn «nasjonale sikkerhetsinteresser» jf. sikkerhetsloven § 1-5 nr. 1. Endelig er det etter artikkel 123 bokstav c unntak for tiltak som staten «anser vesentlig for sin sikkerhet i tilfelle av alvorlig indre uro som truer den offentlige orden, i krigstid eller ved alvorlig internasjonal spenning som innebærer en fare for krig, eller for å oppfylle forpliktelser den har påtatt seg med sikte på å opprettholde fred og internasjonal sikkerhet». Disse tilfellene er langt mindre omfattende enn de tilfellene som omfattes av uttrykket «en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet».

Departementet sluttet seg heller ikke til sikkerhetsutvalgets forutsetning om unntaket om å ikke godkjenne erverv kun skal brukes i de tilfeller som er omfattet av EØS-avtalen artikkel 123:

> «Stans av et erverv i en virksomhet vil i utgangspunktet være i strid med EØS-avtalens regler om fri etableringsrett og den frie bevegelighet av kapital, jf. EØS-avtalens artikkel 31 og 40. Imidlertid vil et inngrep bare gjøres i særlige tilfeller, hvor formålet med inngrepet ikke kan oppnås på en mindre inngripende måte. Det må videre være forholdsmessighet mellom den konkrete risiko for skadevirkning for nasjonale sikkerhetsinteresser og negative konsekvenser for de involverte aktørene. Departementet antar at artikkel 123, men også i enkelte tilfeller artikkel 33, da vil kunne hjemle inngripen.» Prop. 153 L (2016-2017), s. 152.

Når det antas at departementet kan unnlate å godkjenne erverv etter EØS-avtalen artikkel 33 innebærer dette at det blir en vesentlig lavere terskel for å ikke godkjenne erverv. Det åpner i prinsippet for at departementet kan unnlate å godkjenne et erverv når det er et egnet og nødvendig tiltak for å ivareta nasjonal sikkerhet.

For øvrig er det ikke i forarbeidene angitt noen konkrete retningslinjer for departementets vurdering av om ervervet skal godkjennes. I forslaget til endringer i eierskapskontrollreglene i Prop. 95 L (2022 –2023) heter det kun at «vurderingen beror på en helhetsvurdering og skjer på grunnlag av meldingen fra kjøper», Prop. 95 L (2022 –2023), s. 18. Hva meldingen fra kjøper skal inneholde er likevel spesifisert i virksomhetssikkerhetsforskriften § 93.

Det tredje trinnet i systemet for investeringskontroll gir Kongen i statsråd kompetanse til å vedta «at ervervet ikke kan gjennomføres, eller om at det skal settes vilkår for gjennomføringen […] også dersom det allerede er inngått avtale om ervervet». Forutsetningen er at ervervet «kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet». Vilkåret er identisk med vilkåret i lovens § 2-5, og skal i utgangspunktet tolkes på samme måte. Jeg viser derfor til redegjørelsen for denne bestemmelsen ovenfor. Som jeg kommer tilbake til nedenfor ser det imidlertid ut til at departementet har forutsatt at terskelen for å anvende § 2-5 skal være noe høyere enn terskelen for å anvende § 10-3, selv om vilkåret for å utøve kompetanse etter begge bestemmelser bygger på den samme ordlyden.

Det er ikke i forarbeidene sagt noe konkret om hvilke «vilkår» som kan settes for gjennomføringen av et erverv, utover at «vedtak etter bestemmelsen må ligge innenfor formålet med sikkerhetsloven [og] må også være forholdsmessig, slik at hensynet til

nasjonale sikkerhetsinteresser må veie opp for de negative økonomiske konsekvensene av vedtaket» jf Prop L (2016-2017), s. 152.

For øvrig setter sikkerhetsloven formål vide rammer for hvilke vedtak som kan fattes. Formålet med loven er blant annet å trygge Norges «nasjonale sikkerhetsinteresser» jf. § 1-1 bokstav a. Som nevnt ovenfor under redegjørelsen for lovens § 2-5 er uttrykket «nasjonale sikkerhetsinteresser» definert slik at det omfatter mer avgrensete kategorier interesser som «landets suverenitet, territorielle integritet og demokratiske styreform», og en videre kategori, «overordnede sikkerhetspolitiske interesser». Det sistnevnte kan være knyttet til forhold som er både vide og upresise, slik som «økonomisk stabilitet og handlefrihet» og «samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet». Slik loven skal tolkes etter forarbeidene betyr dette at det etter § 10-3 kan stilles ulike typer vilkår for erverv, herunder vilkår som gjelder overordnete sikkerhetspolitiske interesser knyttet til risiko for trusler mot utviklingen i makroøkonomiske hovedstørrelser eller risiko for trusler mot kritisk digital infrastruktur.

De konkrete vilkårene som stilles må for øvrig ha en saklig sammenheng med godkjenningen av ervervet, og ikke være uforholdsmessig tyngende. Oppfylles disse kravene kan det etter § 10-3 stilles vilkår om at en sensitiv eiendel eller eiendom blir ekskludert fra et oppkjøp, eller at en ny minoritetseier ikke skal få styreplass eller tilgang til sensitiv informasjon i et selskap, eller at stemmeretten for visse eiere oppheves.

Sikkerhetsloven § 10-3 sier ikke hvem det kan stilles vilkår til. Ut ifra sammenhengen i lovens kapittel 10 må det imidlertid være klart at det kan stilles vilkår til den som erverver, og det selskapet ervervet skjer i. Jeg ser ikke holdepunkter i verken ordlyd eller forarbeider for at det kan stilles vilkår overfor andre. De folkerettslige rammene for anvendelse av § 10-3 i utlandet kommer jeg tilbake til i punkt 8 nedenfor.

6.5 Forholdet mellom bestemmelsene

Ordlyden i sikkerhetsloven § 2-4, § 9-4 og § 10-3 har et delvis overlappende anvendelsesområde, i den forstand at § 2-5 overlapper både med § 9-4 og § 10-3, mens § 9-4 og § 10-3 ikke overlapper i det de har ulikt anvendelsesområde.

Av de tre bestemmelsen er det høyest terskel for å anvende § 9-4. Bestemmelsen kan i motsetning til § 2-5 og § 10-3 kun brukes når det er tale om at infrastruktur eller andre nærmere angitte innretninger «kan bli rammet av eller brukt til sikkerhetstruende virksomhet», altså «tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser» jf. § 1-5 nr. 4. Derimot kan kompetansen etter § 2-5 og § 10-3 anvendes når det er en viss mulighet for at «nasjonale sikkerhetsinteresser… blir truet».

Videre ser det, som nærmere utdypet nedenfor, ut til å være forutsatt av departementet at terskelen for å anvende § 2-5 skal være høyere enn for å anvende § 10-3. Denne forutsetningen er imidlertid ikke gjenspeilet den konkrete ordlyden i bestemmelsene, slik departementet selv har kommentert de enkelte delene av denne ordlyden.

Etter ordlyden har sikkerhetsloven § 2-5 og § 10-3 et felles vilkår. Etter begge bestemmelser kan Kongen i statsråd fatte vedtak for å hindre at visse forhold kan «innebære en ikke

ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet». Ordlyden skiller seg likevel på ett punkt, i tillegg til den forskjellen som består i at § 10-3 kun kan anvendes ved visse erverv som medfører nasjonal sikkerhetsrisiko, mens § 2-5 er langt videre fordi den kan anvendes for å hindre handlinger og aktivitet som kan innebære en nasjonal sikkerhetsrisiko. Etter ordlyden i § 2-5 kan det kun fattes vedtak som er «nødvendige». Tilsvarende begrensning er ikke angitt i ordlyden i § 10-3. Likevel er tilsvarende begrensning som nevnt ovenfor forutsatt å gjelde også ved anvendelse av § 10-3, jf. s. Prop L (2016-2017), s. 152.

På tross av at det tilsynelatende er felles vilkår for å anvende sikkerhetsloven §§ 2-5 og 10-3, har departementet som nevnt forutsatt at terskelen for å anvende § 2-5 skal være høyere enn § 10-3.

Dels fremgår det av forarbeidene at § 2-5 ikke skal være en regulær unntaksbestemmelse, men at det skal noe helt særskilt til for å anvende kompetanse etter den: «Bestemmelsen vil … være en sikkerhetsventil, og den forutsettes benyttet kun i helt spesielle tilfeller.» Prop 153 L. (2016-2017), s. 169. Tilsvarende er ikke forutsatt for § 10-3. Om denne bestemmelsen viser departementet riktignok til at «§ 10-3 kun vil bli anvendt helt unntaksvis»,[71] men omtaler den ikke som den samme sikkerhetsventilen som § 2-5.

Dels forutsetter forarbeidene at selv om vilkårene etter § 10-3 er oppfylt, så er det ikke gitt at vilkårene etter § 2-5 er oppfylt. I merknadene til § 10-3 heter det: «Bestemmelsene [om erverv av eierandeler] gir imidlertid ikke adgang til å gripe inn i beslutninger som er et resultat av forvaltningen av virksomheten, eksempelvis et salg av eiendeler eller overføring av rettigheter og forpliktelser til uønskede aktører. Skal sistnevnte tilfeller kunne stanses av hensyn til nasjonal sikkerhet må vilkårene i § 2-5 være oppfylt.»[72]

6.6 Er hjemlene tilstrekkelig presise?

Etter Grunnloven, EMK og EØS er det som redegjort for ovenfor i punkt 5, enkelte rettslige krav til presisjon for lovhjemler som gir forvaltningen kompetanse. Hovedtrekkene i de EØS-rettslige kravene er omtalt i sikkerhetsutvalgets utredning, NOU 2016: 9 *Samhandling for sikkerhet* (s. 237-240), men verken Grunnlovens eller EMKs presisjonskrav er omtalt i den nevnte utredningen eller andre forarbeider til sikkerhetsloven. I det følgende forutsetter jeg at virksomhetene kan påberope seg disse presisjonskravene, og vurderer i hvilken grad sikkerhetslovens hjemler for å stille vilkår oppfyller kravene til presisjon.

Etter Grunnloven stilles det ikke strenge krav til lovhjemlenes presisjon. Sentralt i vurderingen av om en lovhjemmel er for vid og upresis, er hva slags forvaltningsområde hjemmelen angår, om hele forvaltningsområdet er omfattet, og hvor vide grenser lovens formål setter for hvilke inngrep forvaltningen kan foreta.

Ut ifra disse kriteriene er det etter min vurdering temmelig klart at det forholdsvis snevre anvendelsesområdet for sikkerhetsloven § 9-4 og § 10-3, medfører at bestemmelsene ikke er strid med de krav Grunnloven stiller til lovhjemlers presisjon. Det er tale om hjemler som er begrenset til henholdsvis avtaler om anskaffelser og erverv av eierandeler, det vil si

[71] Prop 153 L. (2016-2017), s. 152.
[72] Prop 153 L. (2016-2017), s. 150.

disposisjoner som private parter ikke nødvendigvis har rettskrav på å gjennomføre, og etter omstendighetene kan avstå fra. Det er videre åpenbart at ivaretakelsen av nasjonal sikkerhet er et forvaltningsområde hvor myndighetene må ha nokså stor frihet til å vurdere hva som i de konkrete situasjonene utgjør relevante trusler.

Sikkerhetsloven § 2-5 reiser større utfordringer for Grunnlovens krav til lovhjemlers presisjon. Bestemmelsen gir som nevnt Kongen i statsråd kompetanse til å treffe vedtak for å «hindre planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet.»

For det første er det en utfordring for Grunnlovens presisjonskrav at vilkårene for å bruke kompetansen etter bestemmelsen ikke er tydelig angitt. Det er tilstrekkelig at det foreligger «en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet».

En sak er at nasjonale sikkerhetsinteresser er et begrep som ikke bare omfatter forholdsvis klart avgrensete kategorier som «landets suverenitet, territorielle integritet og demokratiske styreform», men også en videre kategori, «overordnede sikkerhetspolitiske interesser» jf. § 1-5 nr. 1. Som redegjort for i punkt 6.2 er det klart at det kan treffes vedtak etter § 2-5 når det er en viss risiko for at kritisk digital infrastruktur er truet. I tillegg gir bestemmelsen som nevnt hjemmel for å treffe vedtak i en rekke andre situasjoner, også når det er en viss risiko for at utviklingen i makroøkonomiske hovedstørrelser er truet, som blant annet «inflasjon, valutakurs, vekst og sysselsetting, og stabile kapitalforhold», jf. Prop. 153 L (2016-2017), s. 35.

En annen og mer upresis side av vilkåret for å anvende § 2-5, er at det er tilstrekkelig at en pågående eller planlagt aktivitet kan medføre en «ikke ubetydelig risiko» for at nasjonale sikkerhetsinteresser blir truet. Mangelen på presisjon ligger i at det ikke det ikke kreves klare holdepunkter for at nasjonale sikkerhetsinteresser skal anses for å være «truet».

Kongen i statsråd har på grunnlag av disse vilkårene kompetanse til å fatte vedtak for å hindre «enhver aktivitet, uavhengig av hvordan disse materialiserer seg», «uavhengig av begrensningene i forvaltningsloven § 35 og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak». Dette gir Kongen i statsråd stor frihet til selv å avgjøre om lovlige aktiviteter likevel skal forbys.

Videre angis det ingen konkrete retningslinjer for det skjønn som Kongen i statsråd skal utvise etter bestemmelsen, utover at vedtak må være «nødvendig», som i forarbeidene er presisert slik at vedtak må være forholdsmessige og rimelige. Det er derved vanskelig å forutsi hvordan Kongen i statsråd skal utøve kompetansen etter bestemmelsen.

De vide og upresise vilkårene for å treffe vedtak etter § 2-5, at det kun er lovens formål som setter rammer for vedtakets innhold, og fravær av andre retningslinjer enn et krav til forholdsmessighet ved utøvelse av skjønnet tilsier at bestemmelsen er så upresis at den er nær grensen for å utvanne hjemmelskravet i strid med det som i dag er Grunnlovens forutsetninger.

Det kan også reises spørsmål om mangelen på presisjon i bestemmelsen og omfanget av den kompetansen bestemmelsen gir, gjør at bruken av bestemmelsen ikke er underlagt

tilstrekkelig kontroll. Det er krevende for domstoler å kontrollere upresise bestemmelser som ikke setter rammer for hvilket innhold vedtak skal ha. Det kan ikke heller ikke klages over enkeltvedtak fattet av Kongen i statsråd til overordnet organ jf. forvaltningslovens § 34.

Det er likevel flere forhold som tilsier at det er kriterier for anvendelse av lovens § 2-5 som innebærer at hjemmelen er tilstrekkelig avgrenset og underlagt tilstrekkelig kontroll, slik at den ikke er i strid med Grunnlovens presisjonskrav. For det første er det en forutsetning for å anvende bestemmelsen at det er omstendigheter som tilsier en viss risiko for en trussel mot «landets suverenitet, territorielle integritet og demokratiske styreform» samt nærmere angitte «overordnende sikkerhetspolitiske interesser» jf. sikkerhetsloven § 1-5. Selv om domstolene ikke uten videre bør overprøve Kongen i statsråds vurdering av hva som utgjør slike trusler, gir ordlyden i loven likevel mulighet for at domstolene kan stille visse krav til statsrådets vurderinger av eventuelle trusler. For det andre er det forutsatt i forarbeidene at loven skal være en sikkerhetsventil. Det tilser at det skal være en høy terskel for å anvende kompetansen etter bestemmelsen. For det tredje kan kompetansen etter bestemmelsen kun utøves av Kongen i statsråd. Det sikrer at bruken av kompetansen er underlagt både parlamentarisk og konstitusjonell kontroll, i tillegg til ordinær domstolkontroll. Sett i lys av at ivaretakelsen av nasjonal sikkerhet er et forvaltningsområde hvor myndighetene må ha en viss frihet til å vurdere hva som i de konkrete situasjonene utgjør relevante trusler, er § 2-5 etter mitt syn forenelig med de hjemmelskravet som kan utledes av Grunnloven. Det er imidlertid en forutsetning at bestemmelsen forblir en sikkerhetsventil.

Vurderingen av om EMKs minstekrav til lovhjemlers klarhet vil i betydelig grad være sammenfallende med vurderingen av om Grunnlovens krav til presisjon er oppfylt. Som nevnt i punkt 5.2.3 er det likevel mulig at EMK artikkel 6 og retten til rettferdig rettergang om borgerlige rettigheter og plikter stiller strengere krav til presisjon i lovgivningen enn Grunnloven. EMD har blant annet kommet til at det var i strid med EMK artikkel 6 å anvende nasjonal lovgivning som ikke inneholdt substansielle eller presise bestemmelser for beslutninger truffet av et forvaltningsorgan, når loven ble tolket slik at domstolene bare kan prøve om skjønnet er utøvd innenfor rammene av lovens formål.[73] Hvorvidt EMK artikkel 6 også stiller tilsvarende strenge krav når det gjelder forvaltningen av sikkerhet er imidlertid mer usikkert. Jeg antar imidlertid at spørsmålet ikke vil komme på spissen ved anvendelse av sikkerhetslovens §§ 2-5, 9-4 og 10-3, så fremt bestemmelsene anvendes og tolkes i tråd med forarbeidenes presiseringer av ordlyden, slik at norske domstoler vil føre reell kontroll med bruken av bestemmelsene.

Når det gjelder EØS-rettens hjemmelskrav må sikkerhetslovens bestemmelser vurderes på en annen måte enn i relasjon til Grunnlovens og EMKs hjemmelskrav. EØS-rettens hjemmelskrav setter først og fremst krav til lovhjemlers presisjon på de områdene lovgivningen anses som restriksjoner på fri bevegelse av varer, personer, tjenester og kapital.

Det er klart at sikkerhetsloven kapittel 10 etablerer et system for investeringskontroll som må anses som en restriksjon på etableringsretten og kapitalfriheten, jf. EØS-avtalen artikkel 31 og 40. Loven pålegger erververe (og når lovendringen fra 2023 settes i kraft) også avhendere og

[73] Se Obermeier mot Østerrike 28. juni 1990, avsnitt 70.

de aktuelle virksomhetene, en meldeplikt om visse erverv. Selv om det (før lovendringen fra 2023 settes i kraft) formelt er tillatt å gjennomføre et erverv før departementet godkjenner ervervet, er det i realiteten tale om en type tillatelsesordning som både EU- og EFTA-domstolen tidligere har ansett for å være i strid med reglene om etableringsrett og kapitalfrihet. Hvorvidt ordningen likevel kan rettferdiggjøres vil da bero på om reglene kan begrunnes i hensynet til sikkerhet og om de er egnet og nødvendig tiltak for å ivareta hensyn til nasjonal sikkerhet. Ved denne vurderingen vil det være avgjørende om reglene er tilstrekkelig transparente, slik at investorene, ESA, Kommisjonen og andre land i EØS kan få innblikk i hvordan investeringer vil kunne bli screenet.

Reglene om investeringskontroll i sikkerhetsloven kapittel 10 er upresise på to områder, som begge gjør det krevende for investorene, ESA, Kommisjonen og andre land i EØS å få innblikk i hvordan investeringer vil kunne bli screenet.[74]

For det første er det vanskelig for andre enn norske sikkerhetsmyndigheter og virksomhetene som er underlagt sikkerhetsloven å vite i hvilke tilfeller en investering er underlagt reglene i sikkerhetsloven kapittel 10. Det er som nevnt forutsatt i forarbeidene at Nasjonal sikkerhetsmyndighet skal ha en hjemmeside med oversikt over norske selskaper som er underlagt sikkerhetsloven, men etter dagens sikkerhetslov er dette informasjon som ikke er offentlig tilgjengelig. Det skaper usikkerhet om hvilke investeringer som er underlagt kontroll.[75]

For det andre er det verken i lov eller forarbeider angitt noen presise kriterier for vurdering av om investeringer skal godkjennes, utover at disse vurderingene skal være forholdsmessig.[76] Det vil derfor i praksis være svært krevende for domstoler å kontrollere lovligheten av avgjørelser om å stanse eller sett vilkår for godkjenning av investeringer. Det er klart at det er mulig å formulere klarere og mer presise kriterier både i lov og forarbeider.[77] En kunne for eksempel presisert at investeringer skal godkjennes med mindre visse vilkår er oppfylt. Sett i lys av EU- og EFTA-domstolens praksis antar jeg derfor at mangel på åpenhet om hvem som er underlagt reglene i kapittel 10 og mangel på presise retningslinjer for adgangen til nekte eller stille vilkår for erverv, kan medføre at reglene i sikkerhetsloven kapittel 10 går lenger enn det som er nødvendig i å begrense etableringsretten og kapitalfriheten, jf. EØS-avtalen artikkel 31 og 40, og at mekanismen i lovens kapittel 10 neppe kan forsvares etter EØS-avtalen artikkel 33 eller læren om allmenne hensyn.

Det er klart at det å treffe vedtak etter lovens § 10-3 i flere tilfeller kan tenkes å falle inn under unntaket i EØS-avtalen artikkel 123. Fordi departementet har forutsatt at det kan treffes vedtak etter § 10-3 også utenom de tilfellene som er nevnt i artikkel 123, kan imidlertid ikke hele mekanismen for investeringskontroll i kapittel 10 forsvares med bakgrunn i EØS-avtalen artikkel 123.

[74] Se også NOU 2023: 28, kapittel 13 og Hafstad 2023.
[75] Se også NOU 2023: 8, s. 93
[76] Se også NOU 2023: 8, s. 95-96.
[77] Se analysene og forslaget til ny modell for investeringskontroll i NOU 2023: 28.

På den bakgrunn er det betydelig risiko for at reglene i sikkerhetsloven kapittel 10 er i strid med EØS-avtalen artikkel 31 og 40.[78] Fordi begge bestemmelser gjelder som norsk lov, som ved motstrid skal gå foran annen norsk lovgivning jf. EØS-loven §§ 1 og 2, innebærer det i så fall at det i EØS-området ikke kan fattes gyldige vedtak etter sikkerhetsloven § 10-3. Det innebærer at det er betydelig risiko for at vedtak om stans av erverv og vedtak om vilkår for erverv vil være ugyldige.

Når det gjelder sikkerhetsloven § 2-5 og § 9-4 er det for det første grunn til å reise spørsmål om disse er å anse som restriksjoner. Jeg antar at kompetansen til å treffe vedtak etter § 9-4, som kun inntreffer når det er behov for å hindre «sikkerhetstruende virksomhet», er så avgrenset at den uansett kan forsvares som et egnet og nødvendig tiltak for å ivareta nasjonale sikkerhetsinteresser. Av den grunn er derfor bestemmelsen i seg selv neppe i strid med EØS-regler, såfremt den tolkes og anvendes i samsvar med ordlyden og departementets forutsetninger.

Sikkerhetsloven § 2-5 gir i motsetning til § 9-4 Kongen i statsråd en svært vid kompetanse som ikke er avgrenset av transparente kriterier. Det kan derfor reises spørsmål ved om bestemmelsen kan være en restriksjon på etableringsretten eller kapitalfriheten, fordi den skaper en usikkerhet som kan begrense investeringer, eller i hvert fall gjøre det mindre attraktivt å investere i norske selskaper. Hafstad har antatt at det er vanskelig å «forene med EU- og EØS-rettens krav til at inngrep i grunnleggende friheter forutsetter «specific, objective conditions», som kan gi veiledning med tanke på om transaksjonen godkjennes eller ikke», og at den «åpenbart heller ikke [oppfyller] grunnkravene etter forordning 2019/452 artikkel 3 annet ledd om at reglene og prosedyrene for screening skal være åpne og tilgjengelige samt angi omstendighetene som utløser screeningen, begrunnelsen for screeningen, og tilhørende detaljerte prosedyrer».[79]

Jeg er enig med Hafstad i at de vagt formulerte vilkårene for å treffe vedtak etter sikkerhetsloven § 2-5 gjør det vanskelig å forene bestemmelsen med EØS-rettens krav til presist hjemmelsgrunnlag, forutsatt at bestemmelsen er en restriksjon på etableringsretten og kapitalfriheten jf. EØS-avtalen artikkel 31 og 40. Etter min vurdering er det imidlertid ikke opplagt at bestemmelsen i seg selv utgjør en slik restriksjon. Riktignok har EU-domstolen uttalt at retten til fri bevegelighet ikke kan være avhengig av forvaltningsskjønn, og lagt til grunn at bestemmelser som gir forvaltning et vidt skjønn i seg selv kan være restriksjoner på fri bevegelighet. Det er likevel få saker hvor EU-domstolen har kommet til at et vidt skjønn til å gjøre inngrep i seg selv er en restriksjon. Når forarbeidene forutsetter at § 2-5 er en sikkerhetsventil som ikke vanligvis skal brukes, tilsier det at det skal svært mye til for at bestemmelsen skal anvendes, selv om ordlyden i seg selv setter få formelle skranker for bruken av bestemmelsen. På den bakgrunn er det derfor grunn til å anta at bestemmelsen ikke vil anses som en restriksjon, forutsatt at den blir anvendt i tråd med forarbeidenes forutsetninger. Vurderingen er imidlertid usikker. Slik jeg ser det er det betydelig tvil om

[78] Se i samme retning, Hafstad 2023.
[79] Hafstad 2023, s. 323.

hvorvidt staten vil få medhold i en eventuell rettssak om hvorvidt § 2-5 er i strid med EØS-retten, og om det eventuelle tapet av konkurransekraft og investeringslyst i norske selskaper, som bestemmelsen kan medføre, i realiteten er ulovlig.

7 Håndheving av vilkår

7.1 Innledning – tvangskraft og tvangsfullbyrdelse

For å håndheve vilkår med tvang må krav om tvangsfullbyrdelse begjæres etter tvangsfullbyrdelseslovens regler. Tvangsfullbyrdelse av et krav kan bare gjennomføres når det foreligger et alminnelig eller et særlig tvangsgrunnlag for kravet, og dette tvangsgrunnlaget er tvangskraftig jf. tvangsfullbyrdelsesloven § 4-1.

Tvangsfullbyrdelsesloven definerer en rekke typer av alminnelige tvangsgrunnlag i lovens § 4-2. De mest aktuelle for spørsmålet om myndighetens adgang til å håndheve vilkår overfor utenlandske virksomheter er dom eller kjennelse av en norsk domstol (bokstav a), voldgiftsdom (bokstav d) og avgjørelse av utenlandsk domstol (bokstav g).

Tvangsfullbyrdelse kan gå ut på ulike tvangshandlinger. For pengekrav kan det tas utlegg etter lovens kapittel 7. Og den som har panterett løsøre kan kreve tvangssalg etter lovens kapittel 8, tilsvarende kan den som har panterett i finansielle instrumenter kreves tvangssalg etter lovens kapittel 10 II. Pengekrav kan inndrives etter lovens kapittel 10 III, og penger kan kreves utbetalt etter kapittel 10 IV, tvangsdekning i immatrialrettigheter kan gjennomføres med salg, utstedelse av lisenser eller utbetaling av inntekster fra allerede etablerte lisenser jf. kapittel 10 V, og andre formuesgoder kan dekkes inn ved tvang gjennom salg, leie eller andre disposisjoner jf. kapittel 10 VI. Det kan kreves salg eller bruk realregisterte formuesgoder etter kapittel 11, og krav som går ut på annet enn betaling av penger kan kreves gjennomført ved tvang etter kapittel 13.

Jeg antar at tvangsgjennomføring av strukturelle eller adferdsbaserte vilkår først og fremst vil gjelde krav som går ut på annet enn betaling av penger. Etter kapittel 13 kan andre krav enn penger blant annet gjennomføres ved utlevering av løsøre og verdipapir jf. § 13-8, fravikelse av fast eiendom jf § 13-11, sikkerhetsstillelse jf § 13-3, andre handleplikter jf. § 13-14, og unnlatelses- og tåleplikter jf. § 13-16.

Er det tale om å tvangsfullbyrde avtalte vilkår vil det i utgangspunktet være nødvendig å få en rettslig avgjørelse om at staten har et krav på at vilkårene skal gjennomføres, før slike krav kan kreves tvangsfullbyrdet. En avgjørelse fra en norsk eller utenlandsk domstol, eller en voldgiftsdomstol, kan være tvangsgrunnlag jf. lovens kapittel 4, og kan gi grunnlag for å begjære tvangsfullbyrdelse etter lovens kapittel 13.

De vedtak Kongen i statsråd treffer om vilkår etter sikkerhetsloven § 2-5, § 9-4 og § 10-3 er tvangsgrunnlag etter tvangsfullbyrdelsesloven kapittel 13. Det innebærer at vedtakene kan begjæres tvangsgjennomført etter kapittel 13 uten at staten først må kreve dom for sine krav.

For håndhevingen av de strukturelle og adferdsbaserte vilkår denne utredningen omfatter vil det først og fremst være spørsmål om de kan tvangsgjennomføres som handleplikter etter tvangsfullbyrdelsesloven § 13-14.

7.2 Tvangsgjennomføring av handleplikter

I prinsippet kan både strukturelle og adferdsbaserte vilkår gjennomføres ved at eierne foretar bestemte handlinger. Er det vilkår for en utenlandsks virksomhets erverv av eierandeler i et norske aksjeselskap at en sensitiv eiendel eller eiendom ekskluderes fra et oppkjøp, kan det gjennomføres blant annet ved vedtak om fisjon (deling av aksjeselskap) etter aksjelovens kapittel 14. Det krever at eierne må stemme for en fisjonsplan jf aksjeloven § 14-6. Tilsvarende kan vilkår om å oppheve stemmeretter i et norsk aksjeselskap, hindre en ny minoritetseier i å få styreplass eller tilgang til sensitiv informasjon i selskapet eller deler av dets virksomhet også gjennomføres ved vedtak på generalforsamlingen, forutsatt at vedtakene har et innhold som ikke går lenger enn generalforsamlingens myndighet etter aksjelovens bestemmelser og for øvrig treffes på den måte loven og vedtektene krever. Dette viser at de nevnte strukturelle og adferdsbaserte vilkår i realiteten forutsetter at det fremlegges bestemte forslag på aktuelle selskapers generalforsamling, og at eierne stemmer for disse forslagene. Spørsmålet er etter dette om det er adgang til å gjennomføre slike generalforsamlingsvedtak ved tvang etter tvangsfullbyrdelseslovens bestemmelser.

Etter tvangsfullbyrdelsesloven § 13-14 første ledd er det tre alternativer for fullbyrdelse av handleplikter. Det kan besluttes at saksøker, det vil her si staten, gis rett til å utføre handlingen, at namsmyndighetene skal utføre handlingen eller at saksøkte, det vil si eierne av det norske selskapet, pålegges en løpende mulkt for den tiden som går uten at handleplikten blir oppfylt.

Retten står ikke helt fritt i valget mellom alternativene for fullbyrdelse. Det er forutsatt i forarbeidene at dersom handlingen bare kan oppfylles av saksøkte selv, vil pålegg om løpende mulkt være det eneste fullbyrdingsalternativet.[80] I lovkommentaren er det videre antatt at det ikke kan besluttes at saksøker eller namsmyndighetene kan undertegne et dokument som saksøkte selv må undertegne, slik at det da kun er aktuelt å pålegge løpende mulkt, så lenge saksøkte ikke undertegner dokumentet.[81] Men er det tale om en handling som saksøkte ikke selv må foreta, men som frivillig kan overlates til andre, for eksempel en fullmektig, har Høyesteretts ankeutvalg lagt til grunn at det kan besluttes at både saksøker og namsmyndighetene kan gjennomføre handlingen:

> «Etter ankeutvalgets syn er imidlertid saksøktes medvirkning ikke på samme måte nødvendig for de handlingene saksøkte frivillig kan la andre utføre, typisk ved å gi fullmakt. Da er ikke handlingen personlig på en slik måte at den må utføres av saksøkte selv. Dersom saksøkte frivillig kan overlate handlingen til en annen, er det mulig å gjøre det samme ved tvang. Den åpne ordlyden i § 13-14 første ledd tilsier at bestemmelsen hjemler en slik tvangsoverføring. Tolkningen støttes av hensynet til å sikre mest mulig effektiv tvangsfullbyrdelse.»[82]

På grunnlag av denne lovtolkningen kom Ankeutvalget til at både saksøker og namsmyndighetene kan tvangsgjennomføre aksjeeiers plikt til å stemme i en konkret sak på

[80] Ot.prp.nr.65 (1990–1991), s. 50, se også HR-2023-782-U avsnitt 21.
[81] Se Thor Falkanger mfl., Tvangsfullbyrdelsesloven. Lovkommentar, § 13-14.
[82] Se HR-2023-782-U, avsnitt 22.

generalforsamlingen i et aksjeselskap, når det fremgår av tvangsgrunnlaget hva stemmegivningen skal gå ut på. Ankeutvalgets konkrete resonnement bygget også på at det følger av aksjeloven § 5-2 at en aksjeeier har rett til å delta på generalforsamlingen ved fullmektig, som kan pålegges plikter, blant annet om hvordan vedkommende skal stemme i en bestemt sak.[83]

Legges Ankeutvalgets lovtolkning til grunn kan de nevnte strukturelle og adferdsbaserte vilkår tvangsgjennomføres etter § 13-14, såfremt generalforsamlingen i et selskap har til behandling lovlig utarbeidede forslag om gjennomføring av de aktuelle vilkårene. I et slikt tilfelle kan både saksøker og namsmyndighetene tvangsgjennomføre aksjeeierens plikt til å stemme for forslagene. For handlinger som er personlig på en slik måte at den må utføres av saksøkte selv, er tvangsfullbyrdelsen begrenset til pålegg om løpende mulkt.

Jeg legger til at det ikke er opplagt at Ankeutvalgets tolkning av tvangsfullbyrdelsesloven § 13-14 er riktig. Ankeutvalget har ikke vurdert hvorvidt det å gi noen en fullmakt er «personlig på en slik måte at den må utføres av saksøkte selv». Det kan argumenteres for at det å overlate stemmegivning til andre er i strid med forarbeidenes forutsetning om at det ikke kan besluttes tvangsgjennomføring av handlinger som bare kan oppfylles av saksøkte selv. Jeg går ikke nærmere inn på dette her. Dersom domstolene i en konkret sak skulle komme til at Ankeutvalgets tolking er uriktig, vil virkningen være at handlepliktene kun kan tvangsgjennomføres med pålegg om løpende mulkt.

Jeg går ikke nærmere inn på hva et vedtak må gå ut på for at en virksomhet blir pålagt plikt som kan kreves gjennomført ved tvang, men forutsetter i det videre at både strukturelle og adferdsbaserte vilkår kan utformes på en slik måte at de kan kreves gjennomført etter tvangsfullbyrdelsesloven kapittel 13.

7.3 Prosessuelle forhold

Begjæring om tvangsfullbyrdelse skal rettes mot den som handleplikten, tåleplikten eller unnlatelsesplikten hviler på jf. tvangsfullbyrdelsesloven § 13-4. Departementet har forutsatt at det ved begjæring om utlevering/ fravikelse, sikkerhetsstillelser eller andre handleplikter skal vedkommende som er henholdsvis besitter, forpliktet og underlagt handleplikt, gjøres til saksøkt.[84] I den grad det er en juridisk person som er besitter, forpliktet eller underlagt en handleplikt, må det også kunne rettes begjæring om tvangsfullbyrdelse mot juridiske personer.

Krav om tvangsfullbyrdelse etter kapittel 13 skal rettes til namsmannen når det gjelder begjæring om utlevering av løsøre eller verdipapir og ved fravikelse av fast eiendom. Den kompetente namsmann er den som er i det distrikt hvor «formuesgodet» eller «eiendommen» er, jf. § 13-3.

Forøvrig skal begjæring om tvangsfullbyrdelse av andre krav enn utlevering og fravikelse settes fram for tingretten. Den kompetente tingretten er den som er «i det distrikt hvor

[83] Se HR-2023-782-U, avsnitt 23.
[84] Ot.prp.nr.65 (1990–1991), s. 264.

saksøkte har alminnelig verneting», men «begjæringen kan også settes fram for tingretten i det distrikt hvor det formuesgodet eller den gjenstand finnes som fullbyrdelsen gjelder» jf. § 13-3 tredje ledd

8. Folkerettslige rammer

8.1 Jurisdiksjonsregler

Folkerettens jurisdiksjonsregler handler om statenes myndighet til å vedta, anvende og håndheve regler overfor andre. For å klargjøre jurisdiksjonsreglene, er det hensiktsmessig å skille mellom ulike former for myndighetsutøvelse. Lovgivningsjurisdiksjon handler om lovgivningen kan gjøres gjeldende overfor noen eller noe. Domsjurisdiksjon handler om det kan treffes avgjørelser basert på lovgivningen. Tvangsjurisdiksjon handler om adgangen til å håndheve lovgivningen.

Jurisdiksjonsreglene bygger på suverenitetsprinsippet og den enkelte stats suverene rett til å bestemme over eget territorium (territorialhøyhet) og sine borgere (personalhøyhet). Territorialhøyheten gir alle statsmakter jurisdiksjon på statens eget territorium. Personalhøyheten innebærer derimot at staten bare kan regulere sine egne borgeres handlinger i utlandet gjennom lov og dom, ikke gjennom tvangsmakt på en annen stats territorium. Videre kan stater etter folkeretten samtykke til at andre stater og internasjonale organisasjoner utøver jurisdiksjon på deres territorium. Slik samtykke er gitt gjennom enkelte internasjonale avtaler.

Ved utøvelse av myndighet overfor utenlandske virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge, er det i utgangspunktet ikke grunnlag for å utøve jurisdiksjon som følge av personalhøyet. Grunnlaget for den jurisdiksjon statsmaktene eventuelt kan utøve, er derfor statens territorialhøyhet.

De rettskildene som jurisdiksjonsreglene kan utledes fra er foruten suverenitetsprinsippet nedfelt i FN pakten og folkerettslig sedvanerett, det vil den adferd stater har hatt over tid i den tro at praksisen har vært bindende. Hvilke slutninger som kan trekkes fra denne statspraksisen er imidlertid temmelig uklare fordi store deler av statspraksisen ikke er kjent. Det er likevel enighet om en viss kjerne i folkerettens jurisdiksjonsregler. I det følgende konsentrerer jeg meg om denne kjernen.

8.2 Lovgivnings- og domsjurisdiksjon

Både lovgivningsjurisdiksjon og domsjurisdiksjon handler om å fastlegge innholdet i normer, enten det skjer gjennom vedtakelse av generelle normer i lov og forskrift, eller vedtakelse av individuelle normer (enkeltvedtak og dommer).

Utgangspunkt etter folkeretten er territorialprinsippet. Det innebære at staten har lovgivningsjurisdiksjon og domsjurisdiksjon på eget territorium, det vil si adgang til å fastsette både generelle og individuelle normer innenfor sine grenser.

Territorialprinsippet er presisert gjennom henholdsvis et subjektivt og et objektivt territorialprinsipp.[85] Prinsippene klargjør i hvilke tilfeller en stat kan normere handlinger som er straffbare etter sin interne rett. De får også betydning for den utøvende makts jurisdiksjon til å vedta hvilke plikter virksomheter skal etterleve, fordi det er opp til den enkelte stat å avgjøre i hvilken grad brudd på plikter fastsatt av den utøvende makt skal anses straffbare.

En stat har etter det subjektive territorialprinsippet jurisdiksjon over handlinger som er påbegynt i staten, selv om virkningene skjer i en annen stat. Det innebærer at rent folkerettslig så kan staten stille visse vilkår overfor utenlandske virksomheter, selv om de får virkning utenfor Norge. Forutsetningen etter dette subjektive prinsippet er at det gjelder handlinger som påbegynnes i Norge. Er det tale om at utenlandske virksomheter gjennom oppkjøp av norske selskaper, blir eier eller får kontroll over kritisk digital infrastruktur i Norge, kan staten altså stille som vilkår at de norske selskapene skal være organisert på bestemte måter eller at de skal pålegges bestemte plikter også etter et eventuelt oppkjøp, selv om vilkårene da får virkning for de utenlandske selskapene utenfor Norge.

Etter det objektive territorialprinsippet, kan en stat også ha jurisdiksjon over handlinger som er påbegynt i andre stater. Forutsetningen etter dette objektive prinsippet er at handlingene utenfor statens grenser inngår som en del av grunnlaget for noe som først er fullført på statens territorium. Den norske staten kan altså stille vilkår ved for eksempel erverv av eierandeler som gjelder handlinger foretatt i utlandet av utenlandske virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge, når det er tale om handlinger som blir fullført i Norge. Er det tale om å regulere handlinger som kun gjelder kritisk digital infrastruktur i Norge, men som er resultat av beslutninger i utlandet, vil den norske staten klart nok ha jurisdiksjon over forholdet.

Videre forutsetter den såkalte effektdoktrinen at en stat også har jurisdiksjon til å normere handlinger som skjer utenfor statens grenser, når den har visse virkninger i staten. Dette reiser krevende grensespørsmål. Nesten alle handlinger kan ha mulige virkninger i alle stater, slik at det er et spørsmål hvor grensen skal trekkes mellom de virkninger av utenlandsk handling som gir en stat jurisdiksjon til å regulere handlingen, og de virkninger som ikke gir slik jurisdiksjon. Flere kilder, riktignok med ulike formuleringer, tilsier at en stat har jurisdiksjon over en handling som er påbegynt i utlandet når den har direkte, vesentlige og forutsigbare virkninger på statens territorium.[86]

Effektdoktrinen innebærer at den norske staten kan fastsette normer for utenlandske virksomheters handlinger, i den grad disse har direkte, vesentlige og forutsigbare virkninger i Norge. For å fastsette vilkår overfor utenlandske virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge, må altså vilkårene knytte seg til handlinger som har direkte, vesentlige og forutsigbare virkninger i Norge. Det innebærer også at norske myndigheter kan stille vilkår ved erverv av eierandeler i selskaper som eier eller kontrollerer

[85] Se generelt, James Crawford, *Brownlie's Principles of Public International Law*, 2012, s. 458-459.
[86] Se blant annet James Crawford*, Brownlie's Principles of Public International Law*, 2012, s. 458-459, og Eu-domstolens sak T-102/96, hvor Retten legger til grunn at EUs regler kan anvendes på fusjoner, når det «kan forudses, at en påtænkt fusion vil have en umiddelbar og væsentlig virkning» på EUs territorium, avsnitt 90. Se også avsnitt 92.

kritisk digital infrastruktur i Norge, såfremt vilkårene gjelder handlinger som har direkte, vesentlige og forutsigbare virkninger i Norge.

Endelig er det antatt det i folkeretten også er et beskyttelsesprinsipp som gir staten adgang til å regulere handlinger i utlandet som angår statenes sikkerhetsinteresser. Det er imidlertid ingen enighet om kriteriene for anvendelse av et slikt prinsipp, og det er antatt at det utøve jurisdiksjon på grunnlag av prinsippet «may be a matter of knowing it when one sees it».[87] Det å anvende dette prinsippet faller derfor utenfor den kjernen i folkerettens jurisdiksjonsregler det er en viss enighet om, og jeg går derfor ikke nærmere inn på prinsippet her.

8.3 Tvangsjurisdiksjon

Det klare utgangspunktet etter folkeretten er at staten bare kan utøve tvang på eget territorium. Videre er det antatt at det er tale om eksklusiv jurisdiksjon, slik at ingen uten samtykke kan håndheve sin lovgivning på en annen stats territorium. Dette er uttrykt av den Permanente Internasjonale Domstolen (PCIJ) i Lotus-saken, som her uttalte:

> "Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention." (avsnitt 45).

Det er klart at forbudet mot å utøve tvangsjurisdiksjon på en annen stats territorium, uten grunnlag i sedvanerett eller den aktuelle statens samtykke omfatter fysiske handlinger. En stats myndigheter kan ikke pågripe personer på en annen stats territorium, uten denne statens samtykke. Det er heller ikke adgang til å ta fysisk beslag i eiendeler på en annen stats territorium.

I tillegg er også ikke-fysiske håndhevelsestiltak omfattet av forbudet mot å utøve tvangsjurisdiksjon på annen stats territorium. Det vil derfor i utgangspunktet være utøvelse av tvangsjurisdiksjon i strid med folkeretten dersom myndighetene i en stat pålegger fysiske eller juridiske personer i en annen stat å utlevere informasjon, uten å først å ha innhentet samtykke fra den aktuelle staten.[88] Tilsvarende er det antatt i folkerettslitteraturen at det må skilles mellom en stats pålegg til personer i utlandet, og en stats informasjon til personer i utlandet. Det er kun det første som kan anses som utøvelse av tvangsjurisdiksjon.[89]

I praksis kan grensen mellom håndhevelsestiltak og utøvelse av lovgivnings- og domsjurisdiksjon være vanskelig å trekke. To tilfeller som i de siste årene har vært oppe i norsk rettspraksis bidrar til å illustrere hvordan grensene skal trekkes med tanke på henholdsvis ransaking av servere, pålegg om utlevering av opplysninger, og tvangsmulkt.

[87] Crawford 2012, s. 462.
[88] Crawford 2012, s. 479.
[89] Se F.A. Mann, «The Doctrine of International Jurisdiction Revisited after Twenty Years", Collected Courses of the Hague Academy of International Law, 1984, s. 40-41.

Hvorvidt det er innenfor norske myndigheter jurisdiksjon å ransake servere i utlandet ble behandlet av Høyesterett i Tidal-saken, HR-2019-610-A.[90] Saken gjaldt en begjæring fra påtalemyndigheten om ransaking hos et selskap som selv ikke var siktet, for å få tilgang til datamateriale som selskapet hadde lagret på servere i utlandet. Det var tale om skybasert lagring, som selskapet selv hadde tilgang til fra Norge uten noe samtykke fra en annen stat. Høyesterett kom til at det var hjemmel for ransaking etter straffeprosessloven § 192, og foretok deretter en forholdsvis omfattende vurdering av om denne ransakingen var innenfor norske myndigheters jurisdiksjon:

Høyesteretts vurdering tok utgangspunkt i at folkeretten, som nevnt ovenfor, ikke tillater noen stat å «anvende tvangsmidler på en annen stats territorium uten samtykke fra vedkommende stat», og nevnte som eksempel at det er på «det rene at norsk politi og påtalemyndighet ikke kan foreta pågripelser utenlands eller ransake et hus i et annet land», avsnitt 40.

Videre viste Høyesterett til at folkerettens utgangspunkter ga «mindre veiledning når det gjelder ransaking og beslag av elektronisk lagret materiale» avsnitt 41. I vurderingen ble det blant annet vist til at det ved skybasert lagring både kan være tilfeldig hvor det konkrete fysiske lagringsstedet er, at dette kan endres uten informasjon som gir brukeren anledning til kontroll over hvor dataene oppbevares, slik at lagringslandet kan være ukjent for brukerne. Høyesterett viste blant annet også til at norske myndigheter har gått ut i fra at det er en viss anledning til foreta ransaking av servere i utlandet og tilsvarende tiltak, når en kan få tilgang til dataene fra en terminal i Norge.

I vurderingen viste Høyesterett også til at praksis fra andre land varierte, slik at det ikke var noen bindende sedvane på område, men at «mange land i praksis synes å godta en slik ransaking som i saken her». Det avgjørende vurderingstemaet for Høyesterett ble etter dette om ransakingen grep «inn i en annen stats eksklusive tvangsjurisdiksjon på en slik måte at denne statens suverenitet krenkes?». Blant annet ut ifra at beslutningen om tvangsmiddelet er truffet av norske myndigheter med ivaretakelse av rettssikkerhetsgarantier, satt i gang i selskapets lokaler Norge, uten at norske myndigheter på egenhånd trenger seg inn i materiale som ligger lagret i utlandet, og at ransakingen kun ville gi tilgang til det materialet selskapet selv hadde lagret, og som det selv fritt kunne hente tilbake fra serveren i utlandet, uten at det ble gjort endringer i det materialet som var lagret. På grunnlag av en slik konkret vurdering kom Høyesterett til at ransakingen ikke krenket en annen stats suverenitet, og at det på det grunnlag ikke var utøvelse tvangsjurisdiksjon i strid med folkeretten å gjennomføre den aktuelle ransakinger av servere i utlandet.

Hvorvidt det var innenfor norsk jurisdiksjon å gi to utenlandske selskaper pålegg om å utlevere opplysninger ble vurdert i en kjennelse fra Borgarting lagmannsrett i sak LB-2021-122818. Saken gjaldt en begjæring fra politiet om utlevering av opplysninger fra henholdsvis

[90] For en mer utførlig folkerettslig analyse av avgjørelsen, se Jørgen Skjold, «Suverenitet, jurisdiksjon og beslag i informasjon på server i utlandet – En kommentar til Høyesteretts kjennelse i Tidal-saken og Ruis kritikk», *Lov og rett* 2019, s. 617-639.

Facebooks og TikToks irske selskaper. Et sentralt spørsmål i kjennelsen var folkerettens grenser for beslutning om utleveringspålegg overfor de to utenlandske virksomhetene.

Borgarting viste innledningsvis til den ovennevnte Tidal-saken og at et lands politi i utgangspunktet ikke «kan foreta etterforskingsskritt som fordrer fysiske tiltak på andre lands territorium. Videre vurderte lagmannsretten det konkrete saksforholdet på grunnlag av den samme problemstillingen Høyesterett formulering i Tidal-saken: Vil en beslutning om det aktuelle tiltaket rettet mot forhold undergitt en annen stats jurisdiksjon, gripe «inn i denne statens eksklusive tvangsjurisdiksjon på en slik måte at statens suverenitet krenkes»?

I motsetning til Høyesteretts kjennelse i Tidal-saken kom lagmannsretten til at pålegget ville gripe inn en annen stats eksklusive jurisdiksjon, fordi det ikke var påvist noen «folkerettslig sedvane eller traktat eller annen avtale som åpner for at utleveringspålegg kan utstedes direkte overfor selskaper i andre land», og poengterte at utleveringspålegget ikke var rettet mot «selskaper eller selskapsansatte i Norge, men mot selskaper hjemmehørende i andre land».

Lagmannsretten kom likevel til at norske domstoler kunne treffe avgjørelse om at vilkårene for det aktuelle tiltaket var oppfylt etter norsk intern rett, og viste til at det ikke er

> «i strid med folkeretten å treffe avgjørelse om tvangsmidler som skal gjennomføres i andre land. Det er tvert om en utbredt praksis internasjonalt for at det treffes slike beslutninger, og det er uansett den anmodede stat som avgjør om tvangsmiddelet skal utføres. En slik beslutning er heller ikke i strid med norske regler…[…] En kjennelse eller beslutning om tvangsmidler i utlandet kan ha som slutning at tvangsmiddelet skal gjennomføres f.eks. at det skal utføres ransaking av en bestemt leilighet («fullbyrdingsavgjørelse»). Slike slutninger synes å være mest utbredt, men det ville antagelig være mer presist om slutningen angir at vilkårene for ransaking er tilstede (fastsettelsesavgjørelse), ettersom det er opp til utenlandske myndigheter å avgjøre om rettsanmodningen skal tas til følge.»[91]

Lagmannsrettens avgjørelse er godt begrunnet og illustrerer at norske domstoler kan ta stilling til om vilkårene for tvangstiltak er oppfylt etter norsk intern rett gjennom en fastsettelsesavgjørelse, men ikke treffe avgjørelse om konkrete tvangstiltak overfor utenlandske virksomheter.

Selv om det i utgangspunktet ikke er adgang for norske myndigheter til å anvende eller håndheve norsk lovgivning utenfor det norske territoriet, er det likevel flere internasjonale avtaler som åpner for at norsk myndighetsutøvelse kan få virkning i andre land. Jeg går igjennom enkelte slike grunnlag nedenfor i punkt 6.4.

8.4 Internasjonale konvensjoner om tvangsfullbyrdelse

8.4.1 Innledning

Det er flere europeiske og internasjonale avtaler om grensekryssende samarbeid om tvangsjurisdiksjon. Blant annet gir regelverket om den europeiske arrestordre et grunnlag for

[91] Se LB-2021-122818

at den norske påtalemyndighetens beslutninger får virkning i andre europeiske land. Andre sentrale internasjonale avtaler som åpner for at norsk myndighetsutøvelse kan få virkning i andre land er, er Lugano-konvensjonen (2007) og New York-konvensjonen (1958) av særlig interesse. Ingen av disse konvensjonene gjelder imidlertid forvaltningssaker,[92] og mens Lugano-konvensjonen ikke gjelder voldgiftssaker,[93] gjelder New York konvensjonen kun voldgiftssaker. Regelverket om den europeiske arrestsordren gjelder bare straffesaker, og faller utenfor temaet her.

Selv om staten ikke kan kreve fullbyrdet forvaltningsvedtak gjennom Lugano-konvensjonen og New York-konvensjonen, kan staten likevel påberope seg konvensjonene når staten har inngått privatrettslig avtaler med virksomheter i andre land, og det er aktuelt å begjøre tvangsfullbyrdelse av avtalevilkårene.

Jeg behandler ikke her de prosessuelle forutsetningene som må være oppfylt for at eventuelle tvister om avtaler skal behandles av norske domstoler eller internasjonal voldgift, og at norsk lovgivning skal anvendes. Det er imidlertid avgjørende at det offentlige ved eventuell avtaleinngåelse med virksomheter som eier eller kontrollerer kritisk digital infrastruktur i Norge i hvert enkelt tilfelle vurderer hva som er hensiktsmessig verneting og lovvalg i henhold til den internasjonale privatrettens regler.

8.4.2 Lugano-konvensjonen

Lugano-konvensjonen gjelder for EFTAs og EUs medlemsland, og gir mulighet for tvangsgjennomføring av avtale vilkår. Formålet med konvensjonen er blant annet å «å innføre en hurtig prosedyre for fullbyrding av dommer» jf konvensjonens fortale.

Etter Lugano-konvensjonen artikkel 38 skal «en dom som er avsagt i en Konvensjonstat og som er tvangskraftig der, fullbyrdes i en annen Konvensjonstat (mottakerstaten) når den er blitt erklært tvangskraftig i denne staten etter begjæring fra en part med rettslig interesse».

Jeg går ikke nærmere inn på betingelsene som må være oppfylt utover at konvensjonen ikke gjelder offentligrettslige forhold. For at Lugano-konvensjonen skal komme til anvendelse på avtaler mellom det offentlige og det private er det derfor en forutsetning at myndighetenes rettigheter etter avtalen ikke går utover rettigheter enhver privat part kunne hatt.

8.4.3 New York konvensjonen

New York-konvensjonen gjelder anerkjennelse og fullbyrdelse av utenlandske voldgiftsavgjørelser. Per 12. oktober 2024 er det 172 stater som har tiltrådt konvensjonen. Konvensjonen et forholdsvis enkelt og effektivt system for håndhevelse av voldgiftsavgjørelser i de fleste land.

Etter konvensjonens artikkel II nr 1 og 2 skal traktatpartene «anerkjenne» voldgiftsklausuler. Etter artikkel II nr 3 innebærer dette blant annet at nasjonale domstoler, etter begjæring fra en part, skal henvise en sak til voldgift dersom den gjelder et forhold regulert av en

[92] For Lugano-konvensjonens del følger dette av artikkel 1 nr 1
[93] Se Lugano-konvensjonen artikkel 1 nr 2 bokstav d.

voldgiftsklausul, med mindre domstolen finner at avtalen er «ugyldig, ute av kraft eller at den ikke kan gjennomføres».

Videre følger det av konvensjonens artikkel III at traktatpartene også skal fullbyrde voldgiftsavgjørelser:

> «På de vilkår som er fastsatt i de følgende artikler, skal enhver kontraherende stat anerkjenne voldgiftsavgjørelser som bindende og fullbyrde dem overensstemmende med prosessreglene på det territorium hvor avgjørelsen legges til grunn. Det må ikke pålegges vesentlig mer tyngende vilkår eller høyere gebyrer eller avgifter for anerkjennelse eller fullbyrdelse av voldgiftsavgjørelser som denne konvensjon gjelder for, enn for anerkjennelse eller fullbyrdelse av innenlandske voldgiftsavgjørelser.»

Med denne forpliktelsen etablerer konvensjonen et rammeverk for fullbyrdelse og gjennomføring av avtalte vilkår, blant annet i de tilfeller en voldgiftsavgjørelse går ut på at slike vilkår er brutt av en avtalepart. Forpliktelsen til å fullbyrde avgjørelser er imidlertid ikke uten begrensninger. Ordlyden i konvensjonen begrenser både hva slags avtaler og hvilke voldgiftsklausuler som er omfattet av konvensjonsforpliktelsene, og også under hvilke vilkår som gir rett til å få fullbyrdet avgjørelser i et annet land. Jeg går ikke nærmere inn på dette, men nevner kun at i avtaler hvor det offentlige er part så vil ikke enhver avtale nødvendigvis anses som et forhold som kan avgjøres av voldgift, jf konvensjonen artikkel II nr 1. Ved inngåelse av avtaler med voldgiftsklausuler er det derfor avgjørende for muligheten til håndhevelse av dem, at de utformes slik at gjelder forhold som kan avgjøres av voldgift.

Christoffer Conrad Eriksen

Vedlegg 5

Tilbakemeldinger fra tilbyderne knyttet til nasjonal kontroll med kritisk digital infrastruktur

Vedlegg 5 Tilbakemeldinger fra tilbyderne knyttet nasjonal kontroll med kritisk digital infrastruktur

Utvalget innhentet våren 2024 informasjon fra ulike tilbydere av offentlige elektroniske kommunikasjonstjenester og datasentertjenester. Utvalget kontaktet 24 aktører, hvorav 18 har besvart utvalgets spørsmål. Valget av de 24 selskapene ble gjort etter en vurdering ut fra den kritiske digitale kommunikasjonsinfrastrukturen de eier eller råder over. Gruppen omfatter selskaper som råder over landsdekkende så vel som regional infrastruktur og tjenester, og den omfatter selskaper med privat eller offentlig eierskap. Utvalget har gjennomgått innspillene og tatt dem med i arbeidet. Nedenfor gis en kort oppsummering av hovedtrekkene i tilbakemeldingene.

Eierskap og nasjonal kontroll

Aktørene har ulike syn på viktigheten av eierskap. Flere av selskapene understreker viktigheten av nasjonalt eierskap for å bevare kontroll over samfunnskritiske funksjoner. Det legges i disses besvarelser vekt på at økt utenlandsk eierskap kan svekke evnen til å oppfylle krav fra samfunnskritiske kunder. Samtidig hevdes det fra andre aktører at nasjonal kontroll kan opprettholdes gjennom reguleringer som sikkerhetsloven, uavhengig av eierskapets nasjonalitet.

Regulering av utenlandske investeringer

Mange aktører peker på at for strenge begrensninger mot utenlandske investeringer kan hindre kapitaltilgang, tilgang til kompetanse og teknologi, samt virke hemmende på innovasjon innen tjenestene. Det oppfattes som viktig med klare og tydelige regler og prosesser for nasjonal kontroll med kritisk digital infrastruktur. En tilbakemelding er at eventuelle begrensninger må rettes mot høyrisiko eierskap som utgjør en trussel mot infrastrukturen, og innrettes slik at de ikke reduserer sunn konkurranse i markedet.

Leverandørvalg

Flere aktører peker på at nåværende regulering har vært avgjørende for virksomhetenes leverandørvalg, spesielt med tanke på nasjonalitet på leverandørenes eierskap. Vurderinger og føringer fra myndigheter knyttet til hvilke land som kan utgjøre en sikkerhetsrisiko, har stor betydning for aktørene. Flere trekker fram betydningen av god myndighetsdialog, og det pekes på at myndighetene gjerne må ta en mer aktiv rolle knyttet til rådgivning.

Det vises også til at gjeldende regulering ikke gir konkret veiledning når det gjelder leverandørvalg. Videre påpekes det også for leverandørvalg at et behov for styrket nasjonal kontroll må balanseres mot aktørenes behov for handlingsrom for å sikre tilgang til kompetanse og teknologi.

Beredskap og teknisk kompetanse

I flere besvarelser understrekes det et behov for nasjonal kontroll over leverandørkjeden og tilgangen til teknisk spesialkompetanse. Det anses som viktig med en helhetlig tilnærming til beredskap, som ser behovet for kompetanse, materiell og strømforsyning i sammenheng. Flere selskaper hevder å ha utviklet tjenestenett med stor grad av autonomi og nasjonal kontroll for å sikre samfunnskritiske funksjoner.

Utvalgets merknader

Utvalget har spesielt merket seg ønsket om en balanse mellom å sikre kapitaltilgang og forutsigbare rammevilkår for utenlandske investeringer, samtidig effektivt identifisere og avvise investeringer som truer sikkerheten. Videre er det verdt å merke seg et ønske om økt nordisk og EU-samarbeid for å fremme Norge som et gjenkjennelig marked for utenlandske kapitaleiere, og for å fremme ressurs- og teknologideling. En styrket dialog mellom myndigheter og industriaktører anses som nødvendig for å sikre forutsigbarhet og veiledning om forventninger og krav, noe som kan påvirke både leverandørvalg og de krav som må stilles til leverandøren.

Vedlegg 6

Informasjonsinnhenting april 2024 offentlige ekomtilbydere

Ekspertutvalget for nasjonal kontroll med digital infrastruktur
ekomsikkerhetsutvalget

Mottaker iht. liste

Deres ref | Vår ref: | Dato: 30. april 2024

Forespørsel om informasjon

I januar 2024 satte regjeringen ned et eget ekspertutvalg for å vurdere hvordan staten kan ivareta nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur. Bakteppet for oppnevnelsen kan sammenfattes med utviklingen i den sikkerhetspolitiske situasjonen i Europa og verden ellers, at kommunikasjonsnettene våre bærer stadig viktigere samfunnsverdier, samtidig med at man har sett eksempler på salg av eierandeler eller deler av viktig kommunikasjonsinfrastruktur.

Disse forholdene har aktualisert behovet for å avklare om myndighetene har tilgang til nødvendige virkemidler for å oppnå tilstrekkelig nasjonal kontroll over kritisk digital infrastruktur. Dette gjelder både eierskap, regulering eller også avtalerettslige virkemidler for de som eier infrastrukturen.

Det er særlig problemsstillinger som oppstår ved eierskapstransaksjoner utvalget skal se nærmere på, men utvalgets arbeid er delt inn i tre delmål:

- Identifisere kritisk infrastruktur på et overordnet nivå (til eget formål)
- Status for nasjonal kontroll og dagens virkemidler
- Vurdere tiltak for styrket nasjonal kontroll

Dere kontaktes nå fordi vi i ekomsikkerhetsutvalget har identifisert dere som ett av flere selskap med vesentlig, kritisk eller avgjørende betydning for utbygging, drift, akutt reparasjon/feilretting og vedlikehold av kritisk digital infrastruktur som definert i mandatet til utvalget. For mer informasjon se vedlagte tabell med oversikt over de ulike typer kritisk infrastruktur vi mener er relevant for selskapet deres.

Når det gjelder kretsen av aktuelle selskap så skal utvalget også vurdere avhengigheter til for eksempel viktige underleverandører og entreprenører som kan være av avgjørende betydning for utbygging, drift eller vedlikehold av infrastrukturen.

Ekspertutvalget skal levere sin rapport tidlig i 2025 og man har derfor kort tid til rådighet for å komme opp med konkrete anbefalinger til Digitaliserings- og forvaltningsdepartementet. Vi håper derfor at dere vil være behjelpelige med å besvare følgende spørsmål og belyse problemstillinger utvalget har fått i oppdrag å jobbe med:

1. Hva er deres betraktninger om hvordan endringer i eget eierskap, fortrinnsvis økt andel utenlandske eierskap innenfor/utenfor Norden/EU/NATO kan påvirke:
    a) egen styringsstruktur/styringsevne?
    b) evne til å ivareta krav fra samfunnskritiske kunder?
    c) evne til å ivareta kritiske samfunnsfunksjoner?[1]
2. Hva er deres betraktninger om hvordan økte myndighetsstyrte begrensninger i utenlandske eierskap /-kapitaltilgang vil kunne påvirke muligheter for videreutvikling av tjenester og/eller nett, samt innovasjon fremover?
3. Hva er deres betraktninger angående å tilby tilgang/innplassering osv. i deres infrastruktur til potensielt sikkerhetstruende (utenlandske) aktører, som f.eks. salg av fiberpar i egen infrastruktur eller tilgang til innplassering i eget datasenter?
4. Hvilke selskaper er fra deres perspektiv avgjørende for utbygging, drift og vedlikehold for den type kritisk digital infrastruktur dere har, mht.:[2]
    a) Leverandører av (i) infrastruktur, (ii)) nettverksutstyr, og (iii)) programvare,
    b) Leverandører/entreprenører for (i) utbygging, (ii)) drift og vedlikehold, (iii) beredskap/feilretting
    c) Leverandører av reservedel- /beredskapslagre og beredskapslogistikk?
5. Hvor betydningsfull mener dere at nåværende regulering (ekomloven/sikkerhetsloven), samt eventuell myndighetsdialog har vært for deres egne leverandørvalg i verdikjeden mtp. leverandørenes nasjonalitet/eierskap? Er det mulig å gi eksempler på hvordan slik dialog for eksempel har påvirket innholdet i avtalen med tanke på for eksempel endringer i eierforholdene eller annet som kan påvirke nasjonal kontroll med underleverandøren?
6. Hvordan ser dere utviklingen fremover mtp. aktørbildet/nasjonal kontroll, hva slags bekymringer ser dere, og ev. hva slags handlingsrom ønsker dere slik at utvalget ikke fremmer forslag som vil kunne ramme dere på en uintendert måte?

[1] Med kritiske samfunnsfunksjoner kan det her tas utgangspunkt i DSBs rapport fra 2016 «Samfunnets kritiske funksjoner» som er det gjeldende rammeverket for vurderinger knyttet til samfunnssikkerhet. Ekomnett og -tjenester er direkte identifisert i rapporten blant de 14 kritiske funksjonene, men man må også ta med i betraktningen at disse understøtter også flere av de andre kritiske samfunnsfunksjonene.

[2] Ekomsikkerhetsutvalgets intensjon er ikke først og fremst å kartlegge konkrete leverandør/underleverandører i den enkeltes verdikjede, men få en bred oversikt over de mest fremtredende aktørene i det norske markedet. Samtidig er det ønskelig å få et visst overblikk over hvilke underleverandører som faktisk benyttes.

7. Har dere mulighet til å gi noen betraktninger rundt egen beredskap og avhengigheter når det kommer til materiell og personell i en krisesituasjon, og eierskapet til de enheter dere har et avhengighetsforhold til?[3]
8. Er det andre forhold dere tenker at utvalget bør vurdere eller ta stilling til, ut over det som er nevnt over?

Vi gjør oppmerksom på at det sendes likelydende brev til en rekke aktører og vi erkjenner at enkelte av spørsmålene derfor ikke nødvendigvis vil være like relevante for alle mottakerne. Dersom dere velger ikke å besvare spørsmål ut fra relevansbetraktning eller annet grunnlag så hadde det vært fint å få en indikasjon om dette.

Fra utvalgets side er vi klar over at flere av de svarene og vurderingene vi her etterspør, kan være av sensitiv karakter og utvalget vil behandle mottatt informasjon konfidensielt i tråd med forvaltningslovens regler. Dersom dere har gradert informasjon som ikke kan deles skriftlig så ber vi om tilbakemelding om dette slik at vi eventuelt kan avtale møte for videre dialog.

Svar på denne henvendelsen sendes til ekomsikkerhetsutvalget@dfd.dep.no **innen 31. mai 2024**. Eventuelle spørsmål til henvendelsen kan gjerne sendes til samme e-postadresse (helst med kopi til iam@nkom.no og hje@nkom.no).

Med vennlig hilsen,

Olav Lysne, utvalgsleder

Vedlegg:
- Mandat ekomsikkerhetsutvalget
- Tabell med oversikt over virksomheter som kontaktes
- Svarskjema

[3] Her er det særlig interessant å få betraktninger om krisesituasjon i høyere krisespenn, slik som ved sikkerhetspolitisk krise og konflikt.

Utgitt av:
Digitaliserings- og
forvaltningsdepartementet

Publikasjonen er tilgjengelig på:
www.regjeringen.no
Publikasjonskode: D-2009 B

Design: Konsis
Foto forside: Gunnstein Myhre (Nkom)
Trykk: Departementenes sikkerhets- og
serviceorganisasjon 02/2025 – opplag 50

Trykksak
2041 0446