

HØRINGSNOTAT

TIL: Kommunal- og distriktsdepartementet

Nov 30, 2023

FRA: IKT-Norge

IKT-NORGES INNSPILL TIL DIGITALISERINGSSTRATEGIEN

Overordnede målsettinger

IKT-Norge mener at hovedformålet med en ny digitaliseringsstrategi er at det blir en mer langsiktig og forutsigbar politikk som faktisk fører til et "taktskifte i digitaliseringen av Norge" jfr. regjeringsplattformen. Næringspolitikk, skattepolitikk, utdanningspolitikk, klima- og miljøpolitikk, tilsyn, etater og reguleringer må ha samme overordnede formål og gå i samme retning.

Strategien må ha som mål å maksimere mulighetene digitalisering og bruk av teknologi har for å løse de store utfordringene vi allerede står overfor, samtidig som vi håndterer både de nye utfordringer og mulighetene som ny teknologi og innovasjon fører med seg.

Strategien må ha et tydelig målbilde, en klar oppfatning av hvilke gevinster som kan realiseres og vurdere dette opp mot ulemper og kostnader knyttet til innføring av ny teknologi. Riktig bruk av regulering, tilsyn og veiledning vil føre til både innovasjon, teknologiutvikling og økt digitalisering. Feil bruk vil føre til at prosjekter og teknologiutvikling stopper opp.

Strategien må også føre til et tettere, tillitsfullt og konstruktivt samarbeide på tvers av offentlig sektor, academia og privat næringsliv. Utgangspunktet må være en erkjennelse av at fremtidens utfordringer løses best i et konstruktivt samarbeid der de beste løsningene stimuleres uavhengig av om de i utgangspunktet ble unnfanget av det offentlige, academia eller i næringslivet. I den nye geopolitiske situasjonen må vi søke nærmere sammen for å skape det samfunnet vi ønsker, basert på tillit og felles verdier.

Vi vil også peke på at strategien må tydeliggjøre hvilke roller ulike offentlige etater og virksomheter skal ha generelt, i gjennomføringen av strategien spesielt, og hvordan samspillet mellom disse kan forbedres. I dag opplever vi stadig oftere at det kommer

direkte motstridende råd og tolkninger fra ulike offentlige etater, myndigheter og tilsyn, da fremst Digdir, Datatilsynet, Teknologirådet, Nkom og i noen grad DFØ.

Spesielle områder som må omtales spesielt

En digitaliseringsstrategi kan potensielt bli svært omfattende og inneholde "alt og ingenting". Vi anbefaler regjeringen om å spesielt omtale noen områder og tydeliggjøre retning, tiltak og eventuelle reguleringer på disse fremfor å "si litt om alt". Vi vil spesielt framheve digital infrastruktur/grunnmur, datasikkerhet, kunstig intelligens, kompetanse, grønn omstilling/twin transition og generell nærings- og skattepolitikk.

Vi er selvfølgelig klar over at det her er flere områder som ikke ligger under det nye digitaliserings- og forvaltningsdepartementets konstitusjonelle ansvarsområde, men som likevel må omtales og konkretiseres.

Digital infrastruktur/grunnmur

Den digitale infrastrukturen blir en stadig viktigere del av vår hverdag. Bedrifter, borgere, etater og institusjoner er helt avhengig av en velfungerende og robust digital infrastruktur. Dette er en utvikling som vil eskalere i tiden som kommer. Kombinert med utvikling av ny teknologi som kunstig intelligens og kvanteteknologi, vil den digitale infrastrukturen for svært mange være like viktig som infrastruktur knyttet til samferdsel (vei, bane og sjøtransport). Samtidig som betydningen av den digitale infrastrukturen øker, øker også behovet for å sikre infrastrukturen mot ny risiko som følge av ny geopolitisk situasjon og klimaendringer.

Regjeringen har flere ambisiøse målsettinger for digitaliseringen og digital infrastruktur knyttet til bredbåndsutbygging, mobildekning, robuste nett m.m. I tillegg kommer betydelige ambisjoner på områder som grønn industriutvikling, distriktpolitikk og beredskap som alle er helt avhengig av en oppdatert, sikker og velutbygd digital infrastruktur. Regjeringen har i mindre grad en plan, strategi eller målbilde for hvordan disse målene skal nås.

Norge har en digital grunnmur i verdensklasse, men videreutviklingen og forsterkningen av landets digitale infrastruktur går nå inn i en fase som krever tydeligere politiske prioriteringer og større grad av langsiktighet. I motsetning til annen infrastruktur, så er den digitale infrastrukturen i det alt vesentlige bygget ut og eid av private (og i noen grad kommunale) selskaper.

Etter IKT-Norges syn trenger Norge en politisk forankret langtidsplan for den digitale infrastrukturen etter modell av tilsvarende planer for bl.a. samferdsel (NTP), forsvar og forsknings- og høyere utdanning. En slik plan må bl.a. avklare forventninger mellom statlig ansvar og finansiering og markedsbasert utbygging og hvor gamle mål full dekningsgrad knyttet til hastighet på 100 Mb/s dekningsgrad erstattes av et nytt langsiktig mål om at tilnærmet alle husholdninger, bedrifter og offentlige kontorer skal ha tilgang til bredbånd/fiber med hastighet på minimum 1 Gb/s. Norge er et av få land i Europa som ikke har satt et slikt mål. Behovet for en slik langtidsplan understrekes for øvrig både i [NSMs sikkerhetsfaglige råd «Et motstandsdyktig Norge»](#) og Totalberedskapskommisjonens anbefalinger i [NOU 2013: 17 "Nå er det alvor - Rustet for en usikker fremtid"](#)

IKT-Norge har utarbeidet en egen rapport om hvordan en slik langtidsplan bør være og hva den overordnet bør inneholde. Se vedlegg 1.

Kunstig intelligens

Kunstig intelligens (AI) vil endre vår hverdag på måter vi knapt kan forestille oss. Potensialet er enormt: AI kan bidra til å løse store samfunnsutfordringer som klima, helseplager, eldrebølge, styrket konkurransekraften og nye næringer og jobber. Men veien dit er usikker og full av utfordringer. Vi trenger både politiske myndigheter og et næringsliv som vet hva man skal bruke kunstig intelligens til og hvordan bruken best skal reguleres.

IKT-Norge mener derfor at digitaliseringsstrategien både bør inneholde en overordnet visjon for regjeringens ambisjon og mål når det gjelder AI. Den bør inneholde en vurdering av hvordan Norge kan maksimere bruken av vår unike posisjon, ressurser og styrker for å fremme utvikling og anvendelse av AI og hvordan vi implementerer AI i ulike sektorer.

Det er også behov for en tydeliggjøring av hvordan vi styrke samarbeid mellom academia, næringsliv og offentlig sektor og konkretisering av bruk og innhold i "forskningsmilliard" til AI og hvordan vi skal styrke og/eller tilrettelegge utdanning av AI-kunnskapsarbeidere.

Strategien bør også omtale hvilken teknisk infrastruktur (som for eksempel datasentre, bredbåndsnett og skytjenester) som er nødvendig for å støtte utbredelsen av AI. Dette må sees i sammenheng med vårt forslag om en egen langtidsplan for den digitale infrastrukturen.

I tillegg må digitaliseringsstrategien etter vårt syn inneholde et sett av etiske retningslinjer for bruk av AI knyttet til bl.a. personvern og ikke-diskriminering. Strategien må klargjøre hvilket lovverk og hvilke reguleringer som er nødvendig for å sikre at utviklingen og bruken av AI er sikker, rettferdig og transparent, men samtidig ikke er til hinder for innovasjon og utvikling. Strategien bør i tillegg omtale hvilke initiativ og strukturer hvor Norge samarbeider med andre land, internasjonale organisasjoner, privat sektor, og sivilsamfunnet for å fremme våre AI-mål og ikke minst hvordan kan vi håndtere potensielle risikoer og trusler knyttet til AI, som for eksempel datasikkerhet, og mulig misbruk av AI.

IKT-Norge har utarbeidet en egen veiviser for AI i Norge, med forslag til prinsipper for bruk, utvikling og regulering av AI i tillegg til konkrete forslag for å stimulere AI. Se vedlegg 2.

Datasikkerhet

Norge er helt avhengig av en robust og god digital infrastruktur og digitale løsninger for at samfunnet skal fungere. Vi - både borgere og bedrifter - har krav og forventninger om at alt skal virke selv i en eventuell krise eller under angrep. Dette må få store konsekvenser for hvordan innsatsen og investeringene skal være fremover.

IKT-Norge er bekymret for Norges evne til å stå mot cybersikkerhet, bl.a. begrunnet med at cybersikkerhet ikke er prioritert høyt nok de siste årene og at det både utdannes og rekrutteres for få med spisskompetanse knyttet til cybersikkerhet. Dette understrekes i [NSMs sikkerhetsfaglige råd «Et motstandsdyktig Norge»](#), hvor det slås fast at Norges arbeid med cybersikkerhet har vært basert på "dugnad og valgfag".

EU og resten av verden bruker nå store ressurser for å skape fremtidens digitale konkurransekraft. For at Norge skal kunne følge med på dette, og får å kunne ta en ledende rolle innen cybersikkerhet, er det avgjørende både med en robust og sikker infrastruktur, og myndigheter og selskaper som tar ansvar for å skape nødvendige tillit.

Etter IKT-Norges syn trenger Norge å utvikle en omfattende nasjonal cybersikkerhetsstrategi som klart definerer nasjonens mål, ansvar, og forventninger. Denne bør etter vårt syn være en del av regjeringens digitaliseringsstrategi.

En slik cybersikkerhetsstrategi må oppdateres regelmessig for å reflektere det skiftende trussellandskapet. Strategien må sette felles mål på tvers av sektorer og privat, offentlig, akademia, den må definere tydelige roller og ansvar mellom offentlig og privat sektor, og styrke samhandlingen mellom EOS-tjenestene. Videre er det behov for å kartlegge nasjonale kritiske infrastrukturer, tjenester og avhengigheter og etablere en plan for måling, beredskap og respons ved cyberangrep.

IKT-Norge har utarbeidet et eget veikart for cybersikkerhet i Norge, med 10 ulike områder som bør inngå og forslag til konkrete tiltak for å styrke cybersikkerheten i Norge. Se vedlegg 3.

Kompetanse

Vi trenger et digitalt kompetanseløft som starter i grunnskolen og som gjennomsyrrer hele skole- og utdanningsløpet. Norge mangler arbeidskraft med IT-kompetanse, både generell IT-kompetanse, kompetanse innen IT-sikkerhet og innen kunstig intelligens. Rapporten «[Norges behov for IKT-kompetanse i dag og framover nå og fram mot 2030](#)» viser at nesten halvparten av norske foretak har problemer med å få fatt i IT-spesialister og at det er behov for 40.000 flere sysselsatte med IT-utdanning i 2030. [NHOs kompetansebarometer for 2022](#) viser at nesten halvparten av bedriftene har et udekket behov for IT-kompetanse.

Det samme budskapet gjentas i [Kompetansebehovsutvalgets rapport](#) som nylig ble overlevert til regjeringen. Der framgår det at det er størst behov for kompetanse innen ingeniør- og IKT-fag og at det kompetanseknappheten forsterkes med grønn omstilling.

[Tallene](#) fra årets opptak til høstens studieplasser viser etter vårt syn nettopp dette: Det er en økning i søkere med informasjonsteknologi som førstevalg med 6,9% sammenlignet med opptaket i fjor. Samtidig reduseres antall studieplasser med 3,6 prosent. Det var bare hver tredje som har IT som førstevalg, som faktisk ble tatt opp til studier denne høsten.

Etter IKT-Norges syn lykkes vi ikke med digitaliseringen av Norge, dersom vi mangler relevant kompetanse til å gjennomføre den. Regjeringens egen stortingsmelding "[Utsyn over kompetansebehovet i Norge](#)" understreker både dette og at vi nå står midt i en omstilling drevet av både digitalisering og bærekraft. Felles for de langsiktige samfunnsutfordringene er at håndteringen av dem stiller store krav til kompetanse, kunnskap og innovasjon. Dette krever en gjennomgripende omstilling i norsk arbeids- og samfunnsliv og stiller økte krav til utdanningssektoren.

IKT-Norge er enig i at det stiller økte krav til utdanningssektorene med vi savner en overordnet plan eller strategi om hvordan vi skal sikre nødvendig kompetanse. Dette er ikke en problemstilling eller utfordring som kan overlates til utdanningssektoren alene, men som krever et sett med virkemidler bl.a. et skattesystem som både stimulerer til kompetanseopbygg og rekruttering av utenlandsk arbeidskraft, jfr. omtalen i utsynsmeldingen om at bruken av utenlandsk arbeidskraft øker særlig når det gjelder IT-utviklere, andre teknologer og faglig ansatte i universitets- og høyskolesektoren.

IKT-Norge forventer at digitaliseringsstrategien gir noen tydelige signaler på hvordan regjeringen ser for seg at dette kompetansegapet tettes fram mot 2030.

Grønn digital omstilling/twin transition

Grønn digital omstilling eller twin transition er helt nødvendig for å løse en rekke langsiktige samfunnsutfordringer. IKT-Norge mener at digitaliseringsstrategien må omtale og aller helst konkretisere hvordan integrering av digitale løsninger i større grad kan optimalisere ressursbruk, redusere miljøpåvirkning og fremme bærekraftige løsninger. Det foregår mye godt arbeid i ulike departement og i ulike sektorer, men også dette må settes inn i en større sammenheng. Områder som kan/bør omtales er etter vårt syn bl.a. hvordan bruk av teknologi kan stimulere smartbyer og bærekraftig urbanisering, forbedre effektiviteten, sikkerheten og bærekraften innenfor transport bl.a. gjennom intelligent trafikkstyring, og samkjøringstjenester, optimalisere produksjonen, distribusjonen og forbruket av fornybar energi, forbedre effektiviteten og bærekraften i landbruket og ikke minst hvordan digitalisering kan være en katalysator for overgangen til en sirkulær økonomi, der ressurser optimalt gjenbrukes og resirkuleres.

I tillegg handler twin transition i veldig stor grad om områder som er omtalt over: Digital kompetanse og utdanning, cybersikkerhet og personvern, innovasjon og FoU, regulering og internasjonalt samarbeid.

Nærings- og skattepolitikk

Stabile og gode rammevilkår er helt avgjørende for det digitale næringslivet som investerer stort i løsninger som skal stå seg over tid, og som er samfunnsøkonomisk svært lønnsomme. Uforutsigbare rammebetingelsene medfører redusert overskudd, og dermed mindre investeringer i bl.a. løsninger som kommer fellesskapet til gode, fare for utflytting av arbeidsplasser, dårligere konkurranseforhold mot utenlandske aktører og vanskeligere å få tak i kompetent arbeidskraft.

Vi er inneforstått med at det i en digitaliseringsstrategi neppe vil komme forslag om konkrete skatteendringer som sikrer bedre rammebetingelser for det digitale næringslivet, eller som stimulerer til utvikling av digitale løsninger, men vi mener at det er viktig at det også i en slik strategi understrekes betydningen av nettopp stabile rammebetingelser som en avgjørende faktor for å lykkes med digitaliseringen og en ambisjon om å bruke skatte- og avgiftssystemet til å stimulere digitalisering og twin transition.

Et annet viktig område når det gjelder rammevilkår er reguleringer. Vi passerte nylig 5 år med GDPR, men det var bare begynnelsen på reguleringene som følge av EUs digitale strategi og agenda, og som norske myndigheter og bedrifter må forholde seg til. Reguleringer av digitale markeder og den digitale økonomien står høyt på EUs agenda, og det vil i løpet av de neste årene komme en rekke ytterligere rettsakter fra EU knyttet til blant annet regulering av AI, digital sikkerhet, deling av data, skytjenester, digitale plattformer og forbrukerrettslige spørsmål. Konkret snakker vi bl.a. om [AI Act](#), [AI Liability Directive](#), [CER](#), [NIS 2](#), [DORA-forordningen](#), [Data Act](#), [Data Government Act](#), [Digital Services Act](#) og [Digital Markets Act](#)

For IKT-Norge er det viktig at det signaliseres i digitaliseringsstrategien at disse og andre store EU-reguleringen implementeres i norsk rett så raskt som mulig og med minst mulig særnorske tillegg eller endringer som svekker norsk konkurransekraft eller som skaper usikkerhet rundt norske rammebetingelser.

Vi viser for øvrig til [IKT-Norges alternative statsbudsjett for 2024](#) der det er en rekke forslag til en bedre nærings- og skattepolitikk som stimulerer digitalisering og grønn omstilling.

IKT Norge

Langtidsplan for den digitale infrastrukturen [2022-2030]



august 2022

Forord

I dette notatet begrunner IKT-Norge hvorfor vi mener det er behov for en politisk forankret langtidsplan for den digitale infrastrukturen på lik linje med tilsvarende langtidsplaner for bl.a. samferdsel, forsvar og energisektoren. Vår begrunnelse er tredelt:

For det første medfører både det nye globale trusselbildet og klimaendringer med større hyppighet av ekstremvær at det er behov for å ha en nasjonal digital grunnmur og en mer robust digital infrastruktur.

For det andre har politikere – bl.a. fra dagens regjeringspartier – kommet med betydelige og omfattende lovnader knyttet til f.eks. utbygging av høyhastighetsbroadband, bedre mobildekning og robuste nett som vil kreve betydelige offentlige bidrag, i denne rapporten anslått til 20 mrd. kroner de neste 8 årene, litt avhengig av tempo og ambisjoner.

For det tredje vil en utbygging av den digitale infrastrukturen i hele landet, være minst like viktig for bosetting, arbeidsplasser og det grønne skiftet som annen infrastruktur.

For å sikre en mer robust digital infrastruktur, og en infrastruktur alle norske borgere og bedrifter kan være en del av, er det behov for en langt større grad av forutsigbarhet enn hva tilfeller er i dag. Derfor er det behov for en forpliktende langtidsplan. En slik plan må ikke minst tydeliggjøre det offentliges roller, ansvar og prioriteringer.

Vi har ikke alle svar på hvordan en slik langtidsplan skal utformes, hvordan den skal vedtas og hvordan grunnlaget for den skal utarbeides. Dette notatet er å anse som et første skritt på veien. Vi – og våre medlemmer – er innstilt på å bidra konstruktivt i en prosess som forhåpentligvis bidrar til at felles mål nås og hvor det offentlige og private utbyggere i samarbeid sikrer både et robust nett og tilfredsstillende tilbud til alle uavhengig av geografisk beliggenhet.

Oslo, august 2022



Øyvind Husby
Administrerende direktør i IKT-Norge

Langtidsplan for den digitale infrastrukturen

Norge har en digital grunnmur i verdensklasse, men videreutviklingen og forsterkningen av landets digitale infrastruktur går nå inn i en fase som krever tydelige politiske prioriteringer. I dette notatet tar IKT-Norge til orde for at det bør utarbeides en langtidsplan for den digitale infrastrukturen.

Den geopolitiske situasjonen er dramatisk endret som følge av krigen i Ukraina, med et helt annet trusselbilde mot Norges digitale infrastruktur enn for få måneder siden. I tillegg eskalerer klimakrisen, og vi må forvente mer ekstremvær i tiden fremover enn tidligere antatt. Dette øker vår digitale sårbarhet, og tilsier at forsyningssikkerhet i landets digitale infrastruktur nå bør løftes høyere på den politiske agendaen og gis samme politiske oppmerksomhet og prioritet som forsyningssikkerheten for strøm, vann og mat.

Den digitale infrastrukturen griper inn i alle deler av nærings- og samfunnslivet, og den samfunnsmessige verdien av denne infrastrukturen vil øke i årene fremover. Investeringer i forsterket robusthet, utvidet dekning og høyere kapasiteter i landets digitale grunnmur vil derfor gi store positive effekter for samfunnet. Dette gjelder særlig innenfor viktige politikkområder som:

- **Norges sikkerhet og beredskap i fred, krise og krig**
- **Det grønne skiftet og utviklingen av den datadrevne økonomien**
- **Bosetning og arbeidsplasser i hele landet**

Infrastruktur- og teknologikonkurranse mellom tre nasjonale mobiloperatører og en rekke nasjonale, regionale og lokale utbyggere av bredbåndsinfrastruktur har sørget for et vedvarende høyt investeringsnivå i norske ekom-nett, og stadig bedre tjenester og større valgfrihet for norske kunder. Samlet sett har utbyggere av mobil- og bredbåndsnett i Norge investert mer enn 10 mrd. kroner hvert år siden 2015. I 2021 ble det investert hele 13,2 mrd. kroner, som tilsvarer 36 % av omsetningen i ekom-sektoren. Prinsippet om mest mulig markedsbasert utbygging bør derfor ligge fast, og det er viktig med politiske rammebetingelser som også i årene fremover legger til rette for et høyt investeringsnivå hos de kommersielle nettutbyggerne. I tillegg er det nå nødvendig å ta ekom-politikken et steg videre.

Utbyggere av mobil- og bredbåndsnett har investert mer enn 10 mrd. kroner hvert år siden 2015.

Etter at St. Meld 28 (2021-2022) «Vår felles digitale grunnmur» ble behandlet i Stortinget våren 2021, har nye analyser synliggjort et stort gap mellom nivået på de siste års statlige bevilgninger til utbygging og forsterkning av ekom-nett og behovet for offentlige midler for å sikre at landets digitale grunnmur er god nok for å understøtte sentrale samfunnsmål. Vi har i dette notatet vist til fire analyser fra det siste halvåret som i sum indikerer et behov for offentlige bevilgninger på mer enn 20 mrd. kroner fram mot 2030 for å sørge for gigabit-nett til alle landets husstander og bedrifter, oppnåelse av Nkoms målbilder for robuste transmisjonsnett i Norge, tette

hull i mobildekningen langs landets riksveier og sikre god mobildekning i alle landets togtunneler.

Det er behov for offentlige bevilgninger på mer enn 20 mrd. kroner fram mot 2030.

IKT-Norge vil understreke at behovet for offentlige midler for å sikre at landets digitale grunnmur er god og fremtidsrettet ikke er en konstant størrelse. Det er ingen målstrekk for infrastruktur-investeringer i ekom-nett. Sett i lys av at staten i løpet av de siste 8 årene har bevilget ca. 2,3 mrd. kroner til bredbåndsutbygging i ikke-kommersielle områder og til telesikkerhet/-beredskap, er 20 mrd. kroner de neste 8 årene uansett et svært høyt beløp.

Samtidig må behovet for offentlige midler sees i sammenheng med den digitale infrastrukturens samfunnsmessige verdi. Eksempelvis indikerer rapporten «Samfunnsnyttene av gigabitsamfunnet», som Samfunnsøkonomisk analyse utarbeidet i februar 2022, at en forsering av utbyggingstakten, slik at ambisjonene innfris i 2025 i stedet for i 2035, vil gi en mervest i fastlandsøkonomiens verdiskapning på 75 mrd. kroner i perioden 2021–2030. En slik mervest i verdiskapningen vil langt overstige det offentlige støttebehovet for å oppnå full gigabit-dekning, som Analysys Mason på oppdrag for Kommunal- og distriktsdepartementet i desember 2021 estimerte til 10 – 12,7 mrd. kroner.

I tillegg til økte statlige bevilgninger, blir det i årene fremover viktig med en helhetlig og tverrsektoriell plan for den samlede offentlige virkemiddelbruken, på tvers av sektormyndigheter og forvaltningsnivåer. En slik plan bør bl.a. tydeliggjøre det offentliges roller, ansvar og prioriteringer som henholdsvis:

- 1. tilrettelegger og planmyndighet for mest mulig kostnadseffektiv markedsbasert utbygging av ekom-nett gjennom gode og forutsigbare rammebetingelser**
- 2. etterspørre av forsterket digital infrastruktur gjennom målrettede og koordinerte offentlige innkjøps-/anbudsprosesser**
- 3. bevilger av offentlige tilskudd til ikke-kommersiell og/eller samfunnspålagt utbygging av ekom-nett**

På denne bakgrunn mener IKT-Norge at tiden nå er inne for å utarbeide en langtidsplan for Norges digitale infrastruktur. Vi viser i dette notatet til at det vil være en naturlig utvikling fra de tidligere stortingsmeldingene om ekom-politikken.

Den kommersielle utbyggingen av digital infrastruktur er basert på langsiktige planer og strategier. En tilsvarende langsiktighet bør gjenspeiles i ekom-politikken. Stortinget bør eksempelvis mene noe om statlige bevilgninger til videreutvikling og forsterkning av den digitale infrastrukturen over tid, og ikke kun stykkevis og delt gjennom de årlige budsjettprosessene. Det samme gjelder for målsetningene i ekom-politikken, som i dag oppleves som kortsiktige.

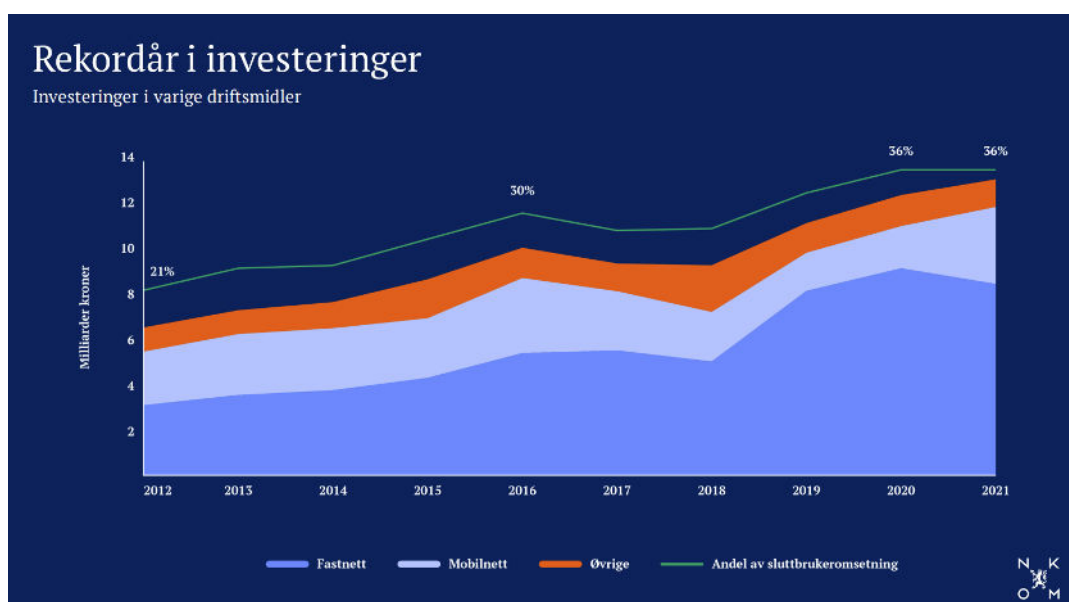
På samme måte som for langtidsplaner for forsvarssektoren, transportsektoren og energisektoren bør det etablere en tilsvarende plan for den digitale infrastrukturen.

IKT-Norge mener det i årene fremover blir viktig med tydelige politiske prioriteringer som understøtter langsiktige målbilder som Stortinget fastsetter i en langtidsplan for landets digitale grunnmur. På samme måte som for langtidsplaner innen forsvarssektoren, transportsektoren og energisektoren bør det derfor etableres en strukturert prosess for regelmessig oppfølging og revisjon av delmål, milepæler og tiltak som sikrer at den digitale infrastrukturen videreutvikles og forsterkes i tråd med de langsiktige politiske målbildene. Langtidsplanen bør ved hver revisjon også omtale relevante prioriteringer knyttet til digital infrastruktur i planer for andre sektorer enn ekom-sektoren.

Norge har en digital grunnmur i verdensklasse, men videreutviklingen og forsterkningen av landets digitale infrastruktur går nå inn i en fase som krever tydelige politiske prioriteringer

Politiske mål og ambisjoner innen viktige samfunnsområder stiller stadig høyere krav til landets digitale grunnmur. Det er en tid før og etter Russlands invasjon av Ukraina, som gjør at den digitale infrastrukturens samfunnskritiske betydning i et sikkerhets- og beredskapsperspektiv øker i tiden fremover. I tråd med ambisiøse mål for den videre digitaliseringen og omstillingen av Norge, øker også avhengigheten til den digitale infrastrukturen innen både offentlig og privat sektor. En velfungerende og robust digital grunnmur i hele landet er avgjørende for å opprettholde og videreutvikle en rekke viktige samfunnsfunksjoner, samt sikre bosetning og arbeidsplasser i hele landet. En moderne og godt utbygd digital infrastruktur er dessuten en forutsetning for det grønne skiftet.

Et vedvarende høyt investeringsnivå i norske mobil- og bredbåndsnett gjennom mange år, og infrastruktur- og teknologikonkurranse mellom tre nasjonale mobiloperatører og en rekke nasjonale, regionale og lokale utbyggere av bredbåndsnett, har gitt Norge en digital grunnmur i verdensklasse. Figur 1 viser at utbyggere av faste og mobile ekom-nett i Norge samlet sett har investert mer enn 10 mrd. kroner hvert år siden 2015. I 2021 ble det investert hele 13,2 mrd. kroner (36 % av omsetningen i ekom-sektoren). Det er ca. 570 mill. kroner mer enn året før, som også var et rekordår.¹



Figur 1 - Årlige ekom-investeringer i Norge 2012-2021 (Kilde: Nkom)

¹ <https://www.nkom.no/aktuelt/5g-utbyggingen-okker-investeringene-i-elektroniske-kommunikasjonsnett>

Dynamikken i markeds- og teknologiutviklingen i ekom-sektoren gjør imidlertid at vi ikke kan hvile på laurbærene, og det er ingen målstrek for infrastrukturinvesteringer i vår felles digitale grunnmur.

På veien inn i gigabitsamfunnet vil utbyggere av høykapasitets fibernett og neste generasjons mobilnett (5G-nett) fortsette å investere store beløp hvert år for å oppgradere og videreutvikle den digitale infrastrukturen. I tillegg er det stor investeringsvilje for å utvikle Norge til en attraktiv datasenternasjon.

Politiske rammebetingelser må derfor i årene fremover legge til rette for mest mulig markedsbasert utbygging av digital infrastruktur, og gi insentiver til et kontinuerlig høyt investeringsnivå, samtidig som konkurransen og valgfriheten i ekom-markedene sikres.

I tillegg vil den fasen vi nå går inn i, kreve tydeligere prioriteringer og mer langsiktighet i ekom-politikken. Det skyldes at den samfunnsmessige verdien av den digitale infrastrukturen, og tjenester som produseres og leveres via denne infrastrukturen, innen flere viktige samfunnsområder vil være langt høyere enn den bedriftsøkonomiske lønnsomheten for utbyggerne i årene fremover.

Det innebærer at investeringer i forsterket robusthet, utvidet dekning og høyere kapasiteter i landets digitale grunnmur vil gi store positive effekter for samfunnet selv om noen av disse investeringene isolert sett ikke er kommersielt lønnsomme for den enkelte utbygger.

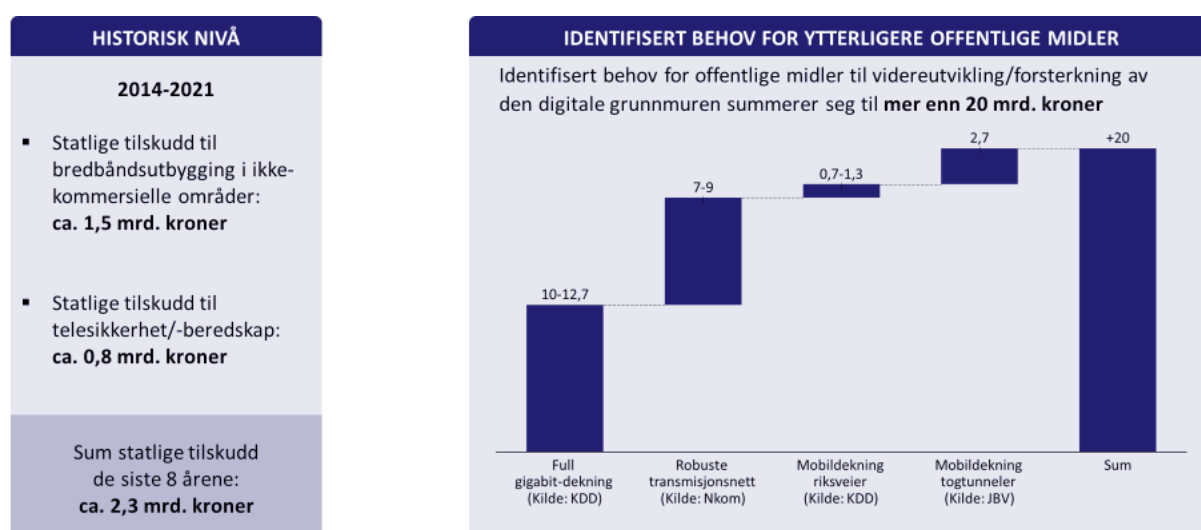
Det fremgår av St. Meld 28 (2021-2022) Vår felles digitale grunnmur at staten i perioden 2014-2021 har bidratt med tilskudd til bredbåndsutbygging i ikke-kommersielle områder på i overkant av 1,5 mrd. kroner. Dette utgjør under 2 % av de markedsbaserte investeringene i ekom-nett i samme periode. I tillegg fremgår det at staten i perioden 2014-2020 til sammen bevilget om lag 500 mill. kroner til forsterket telesikkerhet/-beredskap gjennom programmet for forsterket ekom, og 180 mill. kroner til fiberkabler til utlandet og pilot for alternative kjernenett/transportnett over den samme budsjettposten.

I 2021 ble det bevilget ca. 125 mill. kroner til forsterket telesikkerhet/-beredskap. Dette betyr at staten i sum har bidratt med ca. 2,3 mrd. kroner til å videreutvikle og forsterke landets digitale grunnmur i løpet av de siste 8 årene. Disse bevilgningene har gradvis økt, men kommet stykkevis og delt. Regjeringen og Stortinget kunne gjennom en mer langsiktig plan sikret bedre måloppnåelse i ekom-politikken.

Etter at St. Meld 28 (2021-2022) Vår felles digitale grunnmur ble behandlet i Stortinget våren 2021, har nye analyser synliggjort et stort gap mellom nivået på de siste års statlige bevilgninger til utbygging og forsterkning av ekom-nett og behovet for offentlige midler for å sikre at landets digitale grunnmur er god nok for å understøtte sentrale samfunns mål:

- Estimert offentlig støttebehov for å oppnå full gigabit-dekning i hele landet (gigabit-aksess til alle norske husstander og virksomheter): Mellom 10 og 12.7 mrd. kroner, ref. analyse utført av Analysys Mason på oppdrag for KDD (desember 2021)²
- Summen av kostnadsestimer for å oppfylle målbildene i Nkom-rapporten Robuste transmisjonsnett for Norge mot 2030 (januar 2022): Ca. 7-9 mrd. kroner³
- Kostnadsestimat for å tette hull i mobildekningen langs Norges riksveier: Mellom 775 og 1323 mill. kroner (avhengig av terskelverdi for minste signalstyrke), ref. utredning utført av Analysys Mason på oppdrag for KDD (mai 2022)⁴
- Jernbaneverkets kostnadsestimat for å få god mobilnettdækning i alle togtunneler innen 2027: 2679 mill. kroner, ref. Inside Telecom-artikkel 3. juni 2022⁵

Figur 2 viser at disse fire analysene i sum har identifisert et behov for ytterligere offentlige midler til videreutvikling og forsterkning av den digitale grunnmuren på mer enn 20 mrd. kroner.



Figur 2 – Statlige tilskudd til utbygging av ekom-infrastruktur i perioden 2014-2021, og identifisert behov for ytterligere offentlige midler for å videreutvikle og styrke den digitale grunnmuren (Kilde: St. Meld 28 (2021-2022) Vår felles digitale grunnmur og fire analyser utført det siste halvåret av KDD/Analysys Mason, Nkom, KDD/Analysys Mason og Jernbaneverket)

Samtidig er det et stort gevinstpotensial for samfunnet dersom staten bidrar med midler til den type videreutvikling og forsterkning av ekom-nett som er beskrevet i disse analysene. Beregninger fra Samfunnsøkonomisk analyse⁶ viser eksempelvis at en

² <https://www.regjeringen.no/no/aktuelt/kostnadsanalyse-2021-bredbandsdekning-i-ulike-varianter/id2911903/>

³ <https://www.nkom.no/rapporter-og-dokumenter/robuste-transmisjonsnett-for-norge-mot-2030>

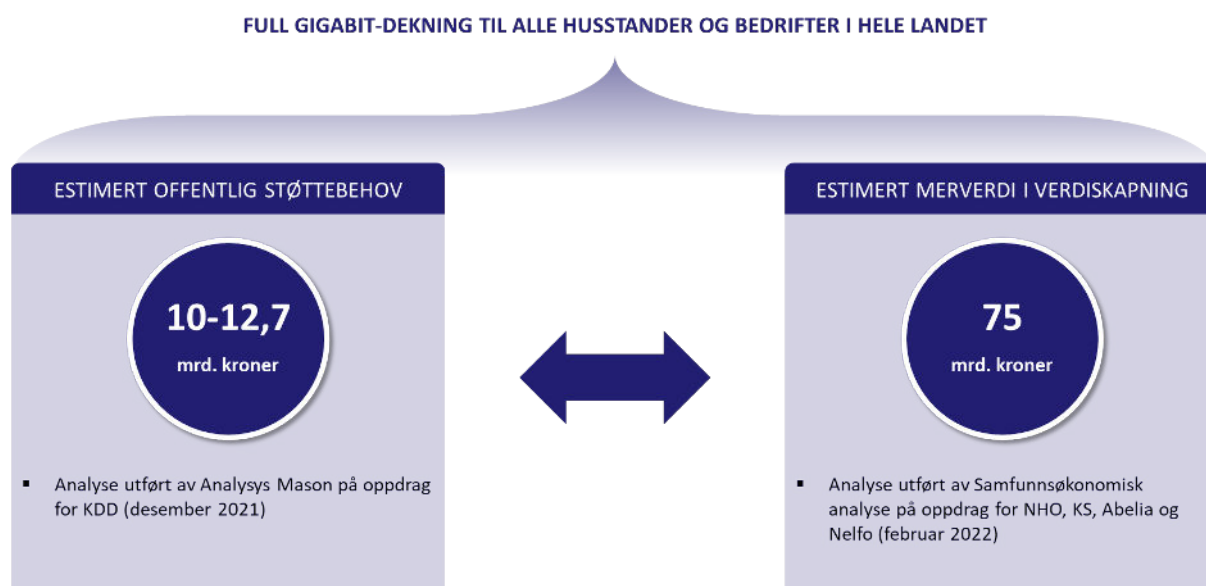
⁴ <https://www.regjeringen.no/no/dokumenter/utredning-mobildekning-langs-riksveier/id2911286/>

⁵ <https://www.insidetelcom.no/artikler/jernbanedirektoratet-alle-togtunneller-skal-fa-god-nettdækning-innen-2027/519987>

⁶ <https://www.samfunnsokonomisk-analyse.no/rapporter/2022/2/15/r3-2022-samfunnsnyttens-av-gigabitsamfunnet>

forsering av utbyggingstakten for gigabit-nett, slik at ambisjonene for gigabitsamfunnet innfris i 2025 i stedet for i 2035, vil gi en mervekst i fastlandsøkonomiens verdiskapning på 75 mrd. kroner i perioden 2021-2030.

Selv om dette forutsetter økte offentlige tilskudd til bredbåndsutbygging de nærmeste årene, viser Figur 3 at estimert mervekst i verdiskapningen for samfunnet (75 mrd. kroner) langt overstiger det estimerte offentlige støttebehovet (10 - 12,7 mrd. kroner) for å oppnå full gigabit-dekning til alle husstander og bedrifter i Norge.



Figur 3 – Sammenligning av estimert offentlig støttebehov og estimert mervekst i verdiskapningen for samfunnet av full gigabit-dekning til alle landets husstander og bedrifter (Kilde: KDD/Analysys Mason og Samfunnsøkonomisk analyse)

Markedsaktørene har ambisiøse og langsiktige planer for å oppgradere og videreutvikle ekom-nettene i Norge og å etablere bærekraftige datasentre, men er samtidig avhengig av at det er et bedriftsøkonomisk grunnlag for sine investeringsbeslutninger. Når den samfunnsmessige verdien av å videreutvikle og forsterke landets digitale infrastruktur i økende grad vil overstige summen av de kommersielle utbyggernes bedriftsøkonomiske lønnsomhet av ytterligere utbygging, bør dette gjenspeiles i ekom-politikken i tiden fremover.

Ekonomi-politikken må reflektere at mål og ambisjoner innen viktige politikkområder stiller stadig høyere krav til landets digitale grunnmur

I tillegg til en økonomi-politikk som fortsatt legger til rette for konkurranse, valgfrihet og tjenestemangfold i økonomi-markedene, og sikrer at den digitale infrastrukturens dekning og kapasitet videreutvikles i takt med markedets behovet, bør økonomi-politikken i årene fremover også bidra til å understøtte sentrale samfunns mål og sørge for at det tas ut størst mulig samfunnsgevinst av landets samlede digitale infrastruktur. Dette haster, særlig i lys av den digitale grunnmurens økte rolle og betydning for:

- **Norges sikkerhet og beredskap i fred, krise og krig**
- **Det grønne skiftet og utviklingen av den datadrevne økonomien**
- **Bosetning og arbeidsplasser i hele landet**

Norges sikkerhet og beredskap i fred, krise og krig

Den digitale infrastrukturen blir stadig viktigere i et sikkerhets- og beredskapsperspektiv. I Meld. St. 28 (2020–2021) Vår felles digitale grunnmur kom dette til uttrykk gjennom en egen nasjonal strategi for sikker og robust økonomi-infrastruktur. I løpet av det siste året har dette også blitt understreket gjennom bl.a. Nasjonal sikkerhetsmyndighets (NSM) rapporter Nasjonalt digitalt risikobilde 2021 fra oktober 2021 og Norske datasenter og digital autonomi – Fire sikkerhetsfaglige anbefalinger ved datasenter fra januar 2022, samt Nkoms rapport Robuste transmisjonsnett for Norge mot 2030 – Målbilder og virkemidler fra januar 2022.

Krigen i Ukraina og endringene i Norges trusselbildet som følge av den nye geopolitiske situasjonen har ytterligere forsterket behovet for å sikre at landets samlede digitale grunnmur er god, robust og fremtidsrettet nok i et totalberedskapsperspektiv. I tillegg eskalerer klimakrisen, og vi må forvente mer ekstremvær i tiden fremover enn tidligere antatt. Dette øker vår digitale sårbarhet, og tilsier at forsyningssikkerhet i landets digitale infrastruktur nå bør løftes høyere på den politiske agendaen, og gis samme politiske oppmerksomhet og prioritet som forsyningssikkerheten for strøm, vann og mat. Ekonomi-politikken må i årene fremover reflektere den samfunnsmessige verdien av en velfungerende nasjonal digital infrastruktur i både fred, krise og krig.

I Nasjonalt digitalt risikobilde 2021 beskriver NSM hvordan den digitale infrastrukturens rolle for landets sikkerhet og beredskap har økt de senere årene som følge av økt frekvens av cybertrusler og tilhørende geopolitisk uro, digitale sårbarheter på grunn av mer omfattende bruk av digitale verktøy i kjølvannet av pandemien og flere cybertrusler på grunn av økt digital avhengighet. NSM skriver avslutningsvis i denne rapporten at taktiskiftet innenfor det digitale risikobildet må møtes med forebyggende sikkerhetsarbeid, og påpeker at økt digital grunnsikring krever en nasjonal innsats.

Selv om den nasjonale strategien for sikker og robust økonomi-infrastruktur i den siste stortingsmeldingen om økonomi-politikken inneholder flere viktige mål og virkemidler for å redusere sårbarheten i landets digitale grunnmur, fremstår ikke dagens økonomi-

politikk som langsiktig og konkret nok i et helhetlig sikkerhets- og beredskapsperspektiv. Målene for å redusere den digitale sårbarheten bør i større grad understøttes av en mer langsiktig innretning på den samlede offentlige virkemiddelbruken i sikkerhets- og beredskapspolitikken.

Det grønne skiftet og utviklingen av den datadrevne økonomien

En moderne og godt utbygd digital infrastruktur er avgjørende for det grønne skiftet. Det fremgår av Meld. St. 28 (2020–2021) Vår felles digitale grunnmur at ekom er en grunnleggende faktor som inngår i løsningene til mange av de 17 bærekraftsmålene i FNs 2030-agenda for bærekraftig utvikling.

Den digitale infrastrukturen tilrettelegger for redusert miljøavtrykk i de fleste andre sektorer, og det vises i Vår felles digitale grunnmur til ulike studier som tilsier at økt bruk av ekom innen f.eks. transport, helse og landbruk kan bidra til at klimagassutslippene fra disse næringene reduseres med i størrelsesorden 15–20 prosent. Bruk av ekom er dessuten en forutsetning for nye former for energiproduksjon og bedre utnyttelse av strømnettet.

Den digitale infrastrukturen griper inn i alle deler av nærings- og samfunnslivet, og den datadrevne økonomien vil få stadig større betydning for næringsutviklingen i Norge. Smarte byer/kommuner og Industri 4.0 er samlebegreper for konsepter som har som formål å utvikle gode og fremtidsrettede løsninger på miljø-, samfunns- og infrastrukturutfordringer gjennom digital innovasjon og bruk av ny teknologi i både privat og offentlig sektor. Moderne og velfungerende ekom-nett i hele landet er en forutsetning for at den datadrevne økonomien skal gi størst mulig samfunnsgevinst.

Norge har også de beste forutsetninger for å utvikle en bærekraftig datasenterindustri, som en del av det grønne skiftet. Kombinasjonen av god og sikker tilgang til fornybar kraft, kjølig klima, politisk og økonomisk stabilitet og en solid digital infrastruktur er et godt utgangspunkt for å gjøre Norge til en attraktiv datasenternasjon. Dessuten blir landets datasentre stadig viktigere for å sikre landets digitale suverenitet i et sikkerhets- og beredskapsperspektiv.

Politiske mål og ambisjoner i klima- og miljøpolitikken har et langsiktig perspektiv. Det tilsier at ekom-politiske mål og tiltak som skal fremme det grønne skiftet og den datadrevne økonomien også bør ha et tilsvarende langsiktig perspektiv.

Bosetning og arbeidsplasser i hele landet

Like muligheter for å bo og arbeide i hele landet forutsetter at den digitale infrastrukturens dekning, kapasitet og robusthet er god nok i alle kommuner og lokalsamfunn i Norge. I dag mangler om lag 240.000 husstander eller 500.000 nordmenn tilgang til høyhastighets bredbåndstilknytning.⁷ Om lag 165.000 husstander er i spredtbygde områder.

Den digitale infrastrukturen har nå blitt like viktig og samfunnskritisk som den fysiske infrastrukturen, både i by og bygd. Dette ble understreket i Demografiutvalgets rapport (NOU 2020:15 Det handler om Norge – Bærekraft i hele landet), hvor det påpekes at den digitale infrastrukturen er avgjørende for å bo og arbeide i distriktene,

⁷ [Nkom: Bredbåndssdekning 2021.](#)

men at det fortsatt er store forskjeller i bredbåndstilbudet mellom by og land selv om dette gapet gradvis reduseres.

Vi går nå inn i en ny fase av omstilling og digitalisering i Norge. Basert på en moderne og robust digital grunnmur i hele landet, vil summen av kunstig intelligens, IoT- og 5G-tjenester, skytjenester, sensorteknologi, robotisering, autonome kjøretøy etc. gi helt nye muligheter for digital innovasjon i både privat og offentlig sektor. For å oppnå størst mulig samfunnsnytte er det avgjørende at den digitale infrastrukturen er god og fremtidsrettet nok i hele landet. Gevinstpotensialet i distriktene er minst like stort som i de mest befolkningstette områdene i landet, og det er viktig å unngå at det utvikles digitale klasseskiller utfra hvor i Norge folk bor og arbeider.

Digitalisering og bruk av ny teknologi er også en forutsetning for å lykkes med å fornye offentlig sektor. I Hurdalsplattformen står det at regjeringen vil gjennomføre et taktskifte i digitaliseringen av offentlig sektor. Da må den digitale infrastrukturen være god og fremtidsrettet nok i alle kommuner og lokalsamfunn.

Utbyggingen av digital infrastruktur har hovedsakelig vært finansiert av markedsaktørene frem til nå, og slik bør det også være i fremtiden. Dersom potensielle samfunnsgevinster knyttet til sentrale distriktspolitiske mål likevel ikke lar seg realisere fullt ut basert på den videre kommersielle utbyggingen av digital infrastruktur, tilsier det at ekom-politikken bør tas et steg videre.

Norge trenger en langtidsplan for den digitale infrastrukturen som tydeliggjør hvordan landets digitale grunnmur skal videreutvikles og forsterkes i et langsiktig, tverrsektorielt perspektiv

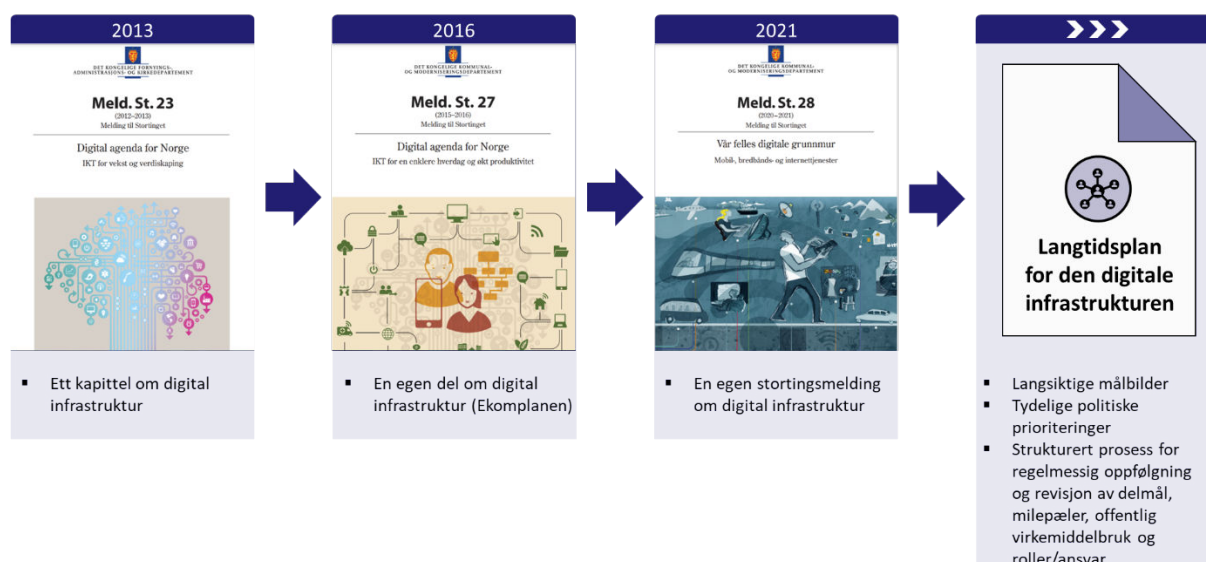
De første stortingsmeldingene om mobil- og bredbåndspolitikken etter liberaliseringen av telemarkedet på slutten av 1990-tallet dreide seg i hovedsak om å legge til rette for bærekraftig konkurranse, herunder sikre utbygging av minst tre konkurrerende mobilnett, finne en hensiktsmessig balanse mellom tilgangsregulering på grossistnivå og infrastrukturkonkurranse, samt sikre valgfrihet, tjenestemangfold og rimelige priser på teletjenester i sluttbrukermarkedet.

Stortingsmeldinger om ekom-politikk fra det siste tiåret har i tillegg inneholdt mål for bredbåndsdekningen i Norge de kommende 4-5 årene. Dessuten har utfall av ekom-nett som følge av ekstremvær og andre naturhendelser ført til at sikre og robuste ekom-nett har fått stadig større politisk oppmerksomhet, og den siste stortingsmeldingen om ekom-politikken (Meld. St. 28 (2020-2021) Vår felles digitale grunnmur) inneholdt en egen del med en nasjonal strategi for sikker og robust ekom-infrastruktur.

Fra stortingsmeldingene Digital Agenda for Norge i 2013 og 2016 til Vår felles digitale grunnmur i 2021 har stortingsmeldingene om digital infrastruktur hatt en utvikling både i form og innhold som gjenspeiler den digitale infrastrukturens økte samfunnsmessige betydning. I Digital Agenda for Norge fra 2013 var det kun ett kapittel som omhandlet den digitale infrastrukturen (Bredbånd – blant de beste i Europa), mens Nasjonal plan for elektronisk kommunikasjon (Ekomplanen) utgjorde en egen del i Digital Agenda for Norge i 2016.

I Vår felles digitale grunnmur fra 2021 ble digital infrastruktur for første gang skilt ut i en egen stortingsmelding. Denne meldingen inneholder gode beskrivelser av status og utviklingstrekk, i tillegg til en oppstilling av mål og tiltak frem mot 2025. Det fremkommer imidlertid ikke tydelig hvilken rolle det offentlige har i å nå målene. Det er heller ikke fastsatt mer langsiktige målbilder enn 2025-mål i Vår digitale grunnmur.

Ekom-politikken handler nå om mye mer enn pris og kvalitet på tale- og internett- og TV-tjenester. Den skal også sikre at landets digitale grunnmur samlet sett er solid og fremtidsrettet nok for å understøtte sentrale samfunnsmål innen viktige politikkområder. Det vil derfor være et naturlig neste steg at Regjeringen utarbeider en langtidsplan for den digitale grunnmuren, og at Stortinget får mulighet til å ta stilling til hvordan mål og ambisjoner for landets digitale infrastruktur skal understøttes av politiske prioriteringer og målrettet offentlig virkemiddelbruk i et mer langsiktig og helhetlig perspektiv enn i de tidligere stortingsmeldingene om ekom-politikken.



Figur 4 - Utvikling i stortingsmeldinger om ekom-politikk og digital infrastruktur siden 2013

Det kan i denne sammenheng nevnes at Stortingets transport- og kommunikasjonskomite, i sin innstilling til Vår felles digitale grunnmur (Innst. 511 S (2020–2021)) fra mai 2021, ba om at regjeringen kommer tilbake til Stortinget med en plan for hvordan man på egnet vis kan nå 2025-målene i Vår felles digitale grunnmur. Ettersom en slik plan fortsatt ikke foreligger, fulgte Stortingets kommunal- og forvaltningskomite nylig opp dette i sin innstilling til Kommuneproposisjonen 2023 (Innst. 460 S (2021–2022)), hvor det bes om at regjeringen kommer tilbake i statsbudsjettet for 2023 med status og plan for hvordan det kan legges til rette for at 2025-målene i Vår felles digitale grunnmur nås.

Dette tilsier at Stortinget ønsker at regjeringen utarbeider tydeligere planer for hvordan målene i ekom-politikken skal oppnås enn tilfellet har vært frem til nå, og at dette bør være en del av fremtidige stortingsmeldinger om den digitale infrastrukturen.

Bred politisk enighet

Stortingsdebatter om ekom-politikken det siste året har vist at det er bred politisk enighet om viktigheten av å sikre at den digitale infrastrukturen er god og fremtidsrettet nok i hele landet, og det er et sterkt tverrpolitisk engasjement for å videreutvikle og styrke Norges digitale grunnmur.

Behovet for en langtidsplan for den digitale infrastrukturen handler ikke om «mer marked» eller «mer statlig styring» i ekom-politikken. Formålet med en langtidsplan er heller ikke å endre på grunnprinsippene og hovedlinjene i norsk ekom-politikk som ulike regjeringskonstellasjoner og stortingsflertall har stilt seg bak siden liberaliseringen av telemarkedet på slutten av 1990-tallet, og som har bidratt til at Norge i dag har en digital grunnmur i verdensklasse. Dette handler om at det i årene fremover blir nødvendig med tydeligere politiske prioriteringer og en mer forutsigbar og koordinert offentlig virkemiddelbruk for å sikre at den digitale grunnmuren i Norge videreutvikles og forsterkes på en måte som reflekterer denne infrastrukturens samfunnskritiske rolle og betydning i et helhetlig og langsiktig perspektiv.

Dette tilsier at arbeidet med å utarbeide en politisk langtidsplan for den digitale infrastrukturen bør igangsettes så raskt som mulig.

Langtidsplan for den digitale infrastrukturen

Innen flere andre sektorer som jobber med langsiktige infrastrukturinvesteringer er det etablert prosesser for utarbeidelse, oppfølging og revisjon av politiske langtidsplaner. Dette gjelder eksempelvis for forsvarssektoren, transportsektoren og energisektoren.

Selv om disse sektorene i hovedsak er offentlig finansiert, og ikke er drevet av markedsbaserte investeringer på samme måte som ekom-sektoren, tilsier den digitale infrastrukturens samfunnskritiske rolle og betydning som er beskrevet i dette notatet at tiden nå inne for å ta stortingsmeldingene om digital infrastruktur et steg videre.

En langtidsplan for den digitale infrastrukturen må i tillegg til langsiktige målbilder inneholde konkrete delmål og forpliktende milepæler, tydelige politiske prioriteringer og målrettede offentlige tiltak, samt en tydeliggjøring av ulike offentlige etaters og virksomheters roller og ansvar for måloppnåelse, på tvers av sektormyndigheter og forvaltningsnivåer.

For at en langtidsplan for den digitale infrastrukturen skal bidra til å ta ekom-politikken et steg videre, må det også etableres en strukturert prosess for oppfølging av mål og tiltak, både i form av rapportering til Stortinget gjennom årlige budsjettprosesser og gjennom revisjon av langtidsplanen hvert fjerde år. Det anses naturlig å se hen til tilsvarende etablerte prosesser for oppfølging og revisjon av langtidsplaner innen andre sektorer, eksempelvis den nye modellen for prosess og organisering av arbeidet med Nasjonal transportplan 2022-2033, som er beskrevet i brev fra Samferdselsdepartementet av 11. januar 2019⁸.

Dersom arbeidet med den første langtidsplanen for landets digitale infrastruktur kommer raskt i gang, er det naturlig å ta utgangspunkt i, og bygge videre på, situasjonsbeskrivelser, mål og virkemidler som fremgår av Meld. St. 28 (2020-2021) Vår felles digitale grunnmur, som det er bred tverrpolitisk enighet om.

Dessuten bør foreslåtte mål og anbefalte tiltak i relevante dokumenter som har blitt publisert etter Stortingets behandling av Vår felles digitale grunnmur i mai 2021 omtales i en slik langtidsplan, herunder:

- Nkom: Robuste transmisjonsnett for Norge mot 2030 – Målbilder og virkemidler (januar 2022)
- Nkom: Risikovurdering av ekomsektoren 2021 – En sektor i endring (oktober 2021)
- NSM: Nasjonalt digitalt risikobilde 2021 (oktober 2021)
- NSM: Norske datasenter og digital autonomi – Fire sikkerhetsfaglige anbefalinger ved datasenter (januar 2022)
- Rapport utarbeidet av Samfunnsøkonomisk analyse på oppdrag for NHO, KS, Abelia og Nelfo: Samfunnsnyttene av gigabitsamfunnet (februar 2022)

⁸ https://www.regjeringen.no/no/dokument/dep/sd/anbud-konsesjoner-og-brev/brev/utvalgte_brev/2019/ny-modell-for-prosess-og-organisering-av-arbeidet-med-nasjonal-transportplan-2022-2033/id2625689/

- Rapport utarbeidet av Analysys Mason på oppdrag for KDD: Utredning – mobildekning langs riksveier (mai 2022)
- Rapport utarbeidet av Analysys Mason på oppdrag for KDD: Kostnadsanalyse desember 2021 bredbåndsdekning i ulike varianter (desember 2021)

Oppsummert mener IKT-Norge at en langtidsplan for den digitale infrastrukturen bør inneholde:

1. Mer langsiktige mål enn i de tidligere stortingsmeldingene om ekom-politikken.

- Stortingsmeldingen Vår felles digitale grunnmur fra 2021 inneholdt 2025-mål. En langtidsplan for den digitale infrastrukturen bør ha et 10 års-perspektiv, tilsvarende andre langtidsplaner i sektorer med langsiktige infrastrukturinvesteringer.

2. Langsiktige målbilder for landets digitale grunnmur som fullt ut reflekterer den digitale infrastrukturens kritiske rolle og betydning innen sentrale politikkområder.

Dette gjelder særlig:

- Norges sikkerhet og beredskap i fred, krise og krig
- Det grønne skiftet og utviklingen av den datadrevne økonomien
- Bosetning og arbeidsplasser i hele landet

3. En helhetlig beskrivelse og drøftelse av utfordringer og muligheter for å oppnå de langsiktige målbildene, som bl.a. hensyntar:

- at investeringer i forsterket robusthet, utvidet dekning og høyere kapasiteter i landets digitale grunnmur kan gi store positive effekter for samfunnet selv om de isolert sett ikke nødvendigvis er kommersielt lønnsomme for den enkelte nettutbygger
- at noen av de langsiktige målbildene kan være sektoroverskridende og at det derfor i større grad enn frem til nå blir nødvendig med koordinert og forutsigbar offentlig virkemiddelbruk på tvers av sektormyndigheter og forvaltningsnivåer
- muligheten for å se Norges digitale infrastruktur i et mer helhetlig nordisk eller skandinavisk perspektiv innen politikkområder som sikkerhet/beredskap og det grønne skiftet hvor det vil være naturlig med mer koordinering på tvers av landegrenser

4. Konkrete delmål og forpliktende milepæler på veien mot måloppnåelse for hvert av de langsiktige målbildene, som følges opp i form av rapportering til Stortinget gjennom årlige budsjettprosesser og revisjon av langtidsplanen hvert fjerde år.

5. Tydelige politiske prioriteringer og målrettede offentlige tiltak for å sikre at langsiktige målbilder og delmål/milepæler nås.

- Dette betyr eksempelvis at offentlige tilskudd til videreutvikling og forsterkning av den digitale infrastrukturen må økes dersom analyser tilsier at de markedsbaserte investeringene ikke vil være tilstrekkelige for å nå ett eller flere av de langsiktige målbildene, eller de tilhørende delmålene/milepælene.
- I tillegg til økte statlige bevilgninger, blir det i årene fremover viktig med en helhetlig og tverrsektoriell plan for den samlede offentlige virkemiddelbruken, på tvers av sektormyndigheter og forvaltningsnivåer, for å sikre måloppnåelse. En slik plan bør bl.a. tydeliggjøre statens, fylkeskommunenenes, kommunenes, sektormyndigheters, og ulike offentlige etater og virksomheters roller, ansvar og prioriteringer som henholdsvis:

- tilrettelegger og planmyndighet for mest mulig kostnadseffektiv markedsbasert utbygging av ekom-nett gjennom gode og forutsigbare rammebetingelser
- etterspørre av forsterket digital infrastruktur gjennom målrettede og koordinerte offentlige innkjøps-/anbudsprosesser
- bevilger av offentlige tilskudd til ikke-kommersiell og/eller samfunnspålagt utbygging av ekom-nett



Figur 5 – Oppsummering av IKT-Norges forslag til innhold i en langtidsplan for den digitale infrastrukturen

VEIVISER FOR AI I NORGE (beta-versjon, august 2023)

IKT-Norge mener at debatten om AI de siste månedene viser at vi trenger et veikart med noen prinsipper for bruk, utvikling og regulering av AI i Norge. Vi har (foreløpig) skissert 10 områder og svar, i tillegg til 8 prinsipper knyttet til regulering og konkrete virkemidler for å styrke kunnskap om og bruk av AI i Norge.

Vårt forslag til veikartet er i utgangspunktet rettet mot myndighetens rolle i utviklingen og reguleringen av AI i Norge, men bør også kunne være retningsgivende for våre medlemmer og andre som bruker og utvikler AI.

IKT-Norge foreslår at følgende 10 områder og problemstillinger bør inngå i et slikt veikart:

1. **Visjon og mål:** Hva er Norges ambisjoner og målsettinger når det gjelder AI? Hvordan kan AI bidra til å oppnå nasjonale og regionale mål innen økonomisk vekst, bærekraft, helse og velvære, etc.?
2. **Nasjonale ressurser og kapasiteter:** Hvordan kan Norge maksimere bruk av sin unike posisjon, ressurser og styrker for å fremme utvikling og anvendelse av AI? Norge har sterke data fra offentlige registre, høy digital lese- og skrivekyndighet, rike naturressurser, etc.
3. **Forskning og utdanning:** Hvilke initiativer bør settes i gang for å styrke forskning på AI og utdanning av AI-kunnskapsarbeidere? Hvordan kan vi styrke samarbeid mellom akademia, næringsliv og offentlig sektor?
4. **Infrastruktur:** Hva slags teknisk infrastruktur (som for eksempel datasentre, bredbåndsnett og skytjenester) er nødvendig for å støtte utbredelsen av AI?
5. **Etiske retningslinjer:** Hvordan kan vi sikre at bruken av AI er etisk forsvarlig, og ivaretar grunnleggende rettigheter som personvern og ikke-diskriminering samtidig som vi sikrer innovasjon og full utnyttelse av mulighetene AI gir?
6. **Reguleringer:** Hvilke lovverk og reguleringer er nødvendig for å sikre at utviklingen og bruken av AI er sikker, rettferdig og transparent, men samtidig ikke er til hinder for innovasjon og utvikling?
7. **Samarbeid og partnerskap:** Hvordan kan vi fremme nasjonalt og internasjonalt samarbeid om AI? Hvordan kan vi jobbe sammen med andre land, internasjonale organisasjoner, privat sektor, og sivilsamfunnet for å fremme våre AI-mål?
8. **Implementeringsstrategier:** Hva er de beste strategiene for å implementere AI i ulike sektorer (for eksempel helse, utdanning, transport, energi, mm.)?

9. **Målingsmetoder:** Hvordan skal vi måle fremdrift mot våre AI-mål? Hvilke indikatorer og benchmarks skal vi bruke?

10. **Risikostyring og sikkerhet:** Hvordan kan vi håndtere potensielle risikoer og trusler knyttet til AI, som for eksempel datasikkerhet, og mulig misbruk av AI?

—

Hvert av disse elementene vil kreve grundig analyse og stakeholder-engasjement for å utforme passende strategier og tiltak. Veikartet bør også være fleksibelt nok til å kunne tilpasses etter hvert som teknologien og samfunnet utvikler seg. IKT-Norges forslag (betaversjon) er som følger:

VEIKART FOR AI I NORGE

Visjon og mål: Vår visjon er å gjøre Norge til en (global) leder i utvikling og bruk av ansvarlig og effektiv AI. Målet er å fremme bærekraft, forbedre helse, utdanning, cybersikkerhet, personvern, fremme teknologisk innovasjon i offentlig og privat sektor og sikre det økonomiske grunnlaget for velferdsstaten.

Nasjonale ressurser og kapasiteter: Norge må maksimere bruken av våre sterke offentlige dataregistre, høy digital kompetanse, rike naturressurser og sterke universiteter og forskningsinstitusjoner, og samtidig utnytte kompetansen som allerede finnes i det digitale i norsk næringsliv. Vi må fremme bruken av AI i offentlig forvaltning, helsevesenet, utdanning, energi, transport og andre nøkkelindustri.

Forskning og utdanning: Norge må styrke investeringene i forskning og utdanning knyttet til AI. Vi må få et tettere samarbeide mellom næringslivet, universiteter og forskningsinstitusjoner for å skape mer robuste AI-programmer og forskningsinitiativer. Det er også avgjørende at næringslivet sikrer at det er tilstrekkelig opplæring og omskolering for å forberede arbeidsstyrken for en AI-drevet økonomi.

[Se vedlegg 1: Forslag til konkrete tiltak for å støtte forskning og utdanning.]

Infrastruktur: Norge må sikre et fortsatt høyt investeringsnivå i nødvendig teknisk infrastruktur som bredbåndsnett (fiber, 5G), datasentre og skytjenester, for å støtte utvikling og utbredelsen av AI.

[Se vedlegg 2: IKT-Norges forslag til en langtidsplan for digital grunnmur.]

Etiske retningslinjer: Norge må utvikle klare etiske retningslinjer for bruk av AI, som sikrer personvern, forhindrer diskriminering og fremmer ansvarlig og transparent bruk av AI samtidig som den fremmer datadeling og innovasjon.

[Se vedlegg 3: IKT-Norges forslag til prinsipper for regulering av AI]

Reguleringer: Vi må ta aktivt del i diskusjonene om utvikling av rammeverket i EU, samtidig som vi sikrer vår egen tilnærming. Dagens teknologinøytrale lover gjelder også for AI, men vi må vurdere behovet for oppdatering av lovverk og reguleringer for å sikre at utvikling og bruk av AI er sikker, rettferdig og transparent, samtidig som vi stimulerer til innovasjon. Målet må være at Norge har den best tilpassede lovgivningen som legger grunnlaget for at Norge blir ledende innen AI.

[Se vedlegg 3: IKT-Norges forslag til prinsipper for regulering av AI]

Samarbeid og partnerskap: Norge må fremme nasjonalt og internasjonalt samarbeid om AI. Vi må samarbeide med andre land, internasjonale organisasjoner, privat sektor og akademia for å fremme Norges AI-mål.

[Se vedlegg 4: IKT-Norges prosjekt næringsliv/akademia/offentlig – GoForIT]

Implementeringsstrategier: Norge må utvikle sektorspesifikke implementeringsstrategier for AI, med fokus på helse, utdanning, transport, energi og andre nøkkelindustrier. I tillegg må det offentlige ha egen implementeringsstrategi for hver sektor, bl.a. justis, forsvar, offentlig forvaltning (NAV, Skatt etc.) mm.

Målingsmetoder: Norge må bruke flere indikatorer og benchmarks for å måle fremdriften mot AI-målene, inkludert nivåer av AI-adopsjon, investering i AI-forskning og -utdanning, og effekten av AI på økonomisk vekst og bærekraft.

Risikostyring og sikkerhet: Norge må utvikle robuste strategier for å håndtere potensielle risikoer og trusler knyttet til AI, inkludert datasikkerhet og potensielt misbruk av AI. Det er avgjørende med et tett, gjensidig og tillitsbasert samarbeid mellom det offentlige, industrien og akademia for å sikre at vi har de nødvendige verktøyene og ferdighetene for å møte disse utfordringene.

VEDLEGG 1:

Forslag til konkrete tiltak for å støtte forskning og utdanning

AI-plattform. Etablere en «AI-plattform» etter modell og omfang av [«Grønn plattform»](#) hvor det i en periode på tre år settes av midler over statsbudsjettet til en konkret satsing på kunstig intelligens og hvor de beste prosjektene som bl.a. bidrar til at det grønne industriløftet kan realiseres, støttes. Ordningen bør minimum ha en ramme på 150 mill. kroner per år.

Studieplasser. Minimum 1.000 nye IKT-studieplasser fra høsten 2024 (ifbm statsbudsjettet for 2024), med hovedvekt på kunstig intelligens og cybersikkerhet. Sammen med UH-sektoren må regjeringen legge fram en forpliktende plan som sikrer minst 2.500 flere studieplasser fra høsten 2025, i tråd med intensjonene i [«Utsynsmeldingen»](#), hvor det bl.a. framgår at antall studieplasser innenfor IT, helse og utdanning som er nødvendig for det grønne skiftet skal økes.

Etter- og videreutdanning av lærere. Lærere og skoleledere må tilbys relevant etter- og videreutdanning i digital kompetanse, herunder algoritmebruk og kunstig intelligens i skolen. Samtidig må digital kompetanse, herunder kunstig intelligens, bli en enda større del av lærerutdanningen.

Programmet for et digitalt Europa 2021–2027 (DIGITAL). Særlig prioritere utforming, innsats og deltakelse i områdene avansert digital kompetanse og kunstig intelligens knyttet til Norges deltakelse og bidrag i EU-programmet DIGITAL.

Forskning. Sikre at en andel av bevilgningene til næringsrettet forskning under NFD går til forskning knyttet til bruk av kunstig intelligens i viktige nærings- og industriprosjekter, bl.a. innen grønn omstilling. I tillegg må grunnforskningen strykes.

SkatteFUNN. Øke beløps- og prosentgrensen i [SkatteFUNN-ordningen](#) til FOU-prosjekter knyttet til kunstig intelligens. Det samlede beløp bør økes fra 25 til 50 millioner kroner og prosentsatsen økes fra 19 til 22 prosent = generell prosentsats.

VEDLEGG 2:

[IKT-Norges forslag til en langtidsplan for digital infrastruktur](#)

VEDLEGG 3:

IKT-Norges veiviser for regulering av AI

Målet er å utvikle effektive og fleksible reguleringer som både beskytter individer og samfunnet, samtidig som det fremmer innovasjon og realisering av de positive effektene AI kan ha innen ulike samfunnsområder. Målet er også at Norge skal bli ledende i Europa på utvikling og bruk av AI, ikke ledende i Europa på den strengeste reguleringen eller den strengeste fortolkningen av EU-regelverk.

1. **Fleksibel og dynamisk regulering:** Lover og forskrifter må utformes robust nok til å håndtere etiske og sikkerhetsmessige bekymringer, men også fleksibelt nok til å kunne oppdateres etter hvert som teknologien utvikler seg. Overdreven regulering kan kvele innovasjon, mens for lite regulering kan føre til misbruk og potensielt skadelige konsekvenser. Dette vil kreve kontinuerlig dialog mellom regulatorer, forskere, utviklere, og brukere.
2. **Eksisterende regulering:** Det finnes en rekke teknologinøytrale reguleringer som også gjelder for KI. Et eksempel er GDPR. Det er imidlertid viktig at ikke uklare tolkninger av eksisterende regelverk stopper innovasjonen innen AI.
3. **Én tydelig stemme:** Norske myndigheter, etater og tilsyn må være samkjørte og enige om veiledning, retning og tolkning av lov- og regelverk knyttet til AI.
4. **Prinsipper fremfor teknologier:** Det kan være mer hensiktsmessig å regulere prinsipper eller praksiser, snarere enn teknologier. Dette vil tillate regulering som kan tilpasses etter hvert som teknologien utvikler seg.
5. **Innflytelse fra industrien:** Det er viktig å involvere industrien i utformingen av AI-reguleringer. Dette vil sikre at reguleringene er både treffsikker og gjennomførbar. Et tett samarbeid mellom lovgivere, AI-utviklere og brukere vil bidra til bedre forståelse av de praktiske sidene, samt de mulige risikoene og fordelene.
6. **Etiske standarder:** Det bør etableres tydelige etiske standarder for utvikling og bruk som gir forskere, utviklere og brukere en ramme for AI. Det kan vurderes om det skal innføres obligatorisk opplæring og sertifisering innen deler av AI-implementering.
7. **Internasjonalt samarbeid:** AI påvirker hele verden, og internasjonalt samarbeid er nødvendig for å utforme effektive reguleringer. Dette sikrer at innovasjon ikke er begrenset av geografiske grenser, og at selskaper kun opererer i land med minimal regulering.
8. **Regulerende sandkasser:** Regulatorer kan skape trygge omgivelser der bedrifter kan teste og utvikle nye teknologier under rettledning og tilsyn, men uten de vanlige regulatoriske begrensningene.

VEDLEGG 4:

[IKT-Norges bærekrafts- og samarbeidsprosjekt næringsliv/akademia/offentlig – GoForIT](#)

CYBERSIKKERHET



VEIKART FOR NORGE

(Oktober 2023 - versjon 0.8)

IKT Norge

INNHALDSFORTEGNELSE

INNLEDNING	3
1. STRATEGI	3
2. SITUASJONSFORSTÅELSE	4
3. RESPONSEVNE	4
4. INFRASTRUKTURELL ROBUSTHET	5
5. LOVER OG REGLER	5
6. UTDANNING OG BEVISSTGJØRING	5
7. FORSKNING OG UTVIKLING	6
8. INTERNASJONALT SAMARBEIDE	6
9. MÅLING OG REGELMESSIGE VURDERINGER	7
10. UTVIKLE EN VERDENSLEDENDE SIKKERHETSINDUSTRI	7
VEDLEGG 1: Strategiske Sikkerhetsmål	8
VEDLEGG 2: Relevante ressurser og referanser	9
VEDLEGG 3: Langtidsplan for den digitale infrastrukturen	10
VEDLEGG 4: Forslag til bevilgninger i Statsbudsjettet 2024	10

INNLEDNING

EU og resten av verden bruker nå store ressurser for å skape fremtidens digitale konkurransekraft. For at Norge skal kunne følge med på dette, og får å kunne ta en ledende rolle innen cybersikkerhet, er det avgjørende både med en robust og sikker infrastruktur, og myndigheter og selskaper som tar ansvar for å skape nødvendige tillit.

Norge er også helt avhengig av digital infrastruktur og digitale løsninger for at dagens samfunnet skal fungere. Vi – både borgere og bedrifter – har krav og forventninger om at alt skal virke selv i en eventuell krise eller under angrep. Dette må få store konsekvenser for hvordan innsatsen og investeringene skal være fremover.

Med denne bakgrunnen har IKT-Norge identifisert ti områder vi mener bør inngå i et “Veikart for Cybersikkerhet” i Norge.

(Dette er en beta-versjon vi skal videreutvikle sammen med medlemmene. Første lansering blir som innspill til regjeringens digitaliseringsstrategi innen 30. november.)

1. STRATEGI

Norge trenger å utvikle en omfattende nasjonal cybersikkerhetsstrategi som klart definerer nasjonens mål, ansvar, og forventninger. Dette har vi ikke i dag. Denne strategien må oppdateres regelmessig for å reflektere det skiftende trussellandskapet.

Vi trenger å :

- a. Sette felles mål på tvers av sektorer og privat, offentlig, academia (se vedlegg 1).
- b. Definere tydelige roller og ansvar mellom offentlige og private sektorer, og styrke samhandlingen mellom EOS-tjenestene.
- c. Kartlegge nasjonale kritiske infrastrukturer, tjenester og avhengigheter.
- d. Etablere en plan for måling, beredskap og respons ved cyberangrep.
- e. Etablere strategien som en langtidsplan med årlige revisjoner med mål å realisere det digitale målbildet.

2. SITUASJONSFORSTÅELSE

Norge trenger en fortløpende og oppdatert situasjonsforståelse på tvers av samfunnet. Dette gjelder på tvers av sivilt og militært, departement og sektorer, privat og offentlig. Dette har vi ikke i dag.

Vi trenger å:

- a. Etablere tydelig ansvar for hvem som har ansvaret for innhenting, analyse og kommunikasjon på tvers av alle sektorer i Norge (i utgangspunktet justis og forsvar)
- b. Etablere løsninger for sikkerhetsgradert samhandling
- c. Opprette et rammeverk for obligatorisk rapportering av cyberhendelser (nå rapporteres 1% - ref. side 25 NSM).
- d. Etablere systematisk overvåkning av hybridoperasjoner inklusiv "virkelighetsmanipulering" som rapporteres inn sammen med det totale situasjonsbildet.
- e. Etablere økt evne til å avdekke skjult cyberaktivitet i virksomhetens infrastruktur.
- f. Gjennomføre en kvantitativ undersøkelse første halvår 2024 for å få status dekke dagens motstandskraft som utgangspunkt for prioritering
- g. Gjennomføre systematisk kartlegging av leverandørkjeder og tredjepartsrisiko - ref NSM Risiko 2023 ¹

3. RESPONSEVNE

Sikre responsmekanismer på tvers av samfunnet på bakgrunn av et felles oppdatert situasjonsbildet, og som reagerer koordinert på tvers av sektorer etter innøvde planer gjennom hele krisespekteret.

Vi trenger å:

- a. Etablere tydelig ansvar og ledelse på tvers av sektorer i hele krisespekteret
- b. Oppdatere beredskapsplaner for sivil sektor basert på krise- og krigsscenario.
- c. Videreutvikle dagens nasjonale cybersikkerhetssenter som kan koordinere responsen til store cyberhendelser, inklusiv vurdere etablere

¹ "Viktige samfunnsfunksjoner er avhengige av leverandører og underleverandører. Disse kan ha potensielt ukjente og alvorlige sårbarheter. Vi er ikke sikrere enn det svakeste ledd. Dette krever at vi evner å oppdage og avverge sikkerhetstruende virksomhet også i leverandørkjedene vi er så avhengige av"

- en SMB CERT, og tilby assistanse til berørte organisasjoner utover dagens mandat.
- d. Sikre tilgang på digitale komponenter

4. INFRASTRUKTURELL ROBUSTHET

Sikre at kritisk infrastruktur (telekom, datasenter, kraftnett, finans, transport, helsevesen) er spesielt beskyttet og kan gjenopprettes raskt etter et angrep for å understøtte totalforsvarsevnen gjennom krisespekteret.

Vi trenger å:

- a. Etablere en langtidsplan (etter mal for nasjonal transportplan) for digital infrastruktur som også dimensjonerer for krise og krig med målsetting, planer og tilhørende finansiering for å sikre nødvendig operativitet i hele krisespekteret.
- b. Stille krav om vurdering av sikkerhet ved definerte anskaffelser

5. LOVER OG REGLER

Utvikle, tilpasse og implementere robuste lover og regelverk for cybersikkerhet som dekker alle aspekter av den digitale infrastrukturen, og setter klare standarder for organisasjoner og enkeltpersoner.

Vi trenger å:

- a. Oppdater eksisterende lovgivning for å dekke dagens trusselbilde og etablere rapportering på status på tvers av sektorer inklusiv implementering av ny "Lov om digital sikkerhet".
- b. Innføre NIS 1 asap
- c. Forberede innføring av NIS 2. Flere av tiltakene iht NIS 2 vil omhandle flere av områdene omtalt under de andre områdene i dette veikartet. Kombinert med blant annet TIBER, DORA og etter hvert EUs Cyber Resilience Act vil samlet styrke situasjonen.

6. UTDANNING OG BEVISSTGJØRING

Styrke satsingen på utdanning innen cybersikkerhet på alle nivåer – fra grunnskole til universitet – og fremme bevissthet om cybersikkerhet blant befolkningen.

Vi trenger å:

- a. Gjøre NSMs grunnkurs obligatorisk for alle ledere i stat og kommune (ordførere, rådmenn etc)
- b. Utvikle og implementere andre opplæringsprogrammer på tvers (obligatoriske og frivillige)
- c. Gjennomføre nasjonale informasjonskampanjer med oppdaterte “best practice” inklusiv f.eks. insiderisiko etc.
- d. Utvikle spesielle programmer innen kryptografi, cyber og kvanteteknologi.

7. FORSKNING OG UTVIKLING

Investere i forskning og utvikling for å holde tritt med den raske utviklingen innen teknologi og trusler. Dette inkluderer også fremme av offentlig-private partnerskap for å støtte innovasjon.

Vi trenger å:

- a. Etablere flere sentre for forskning innen cybersikkerhet.
- b. Integrer cybersikkerhet i utdanningssystemet, fra grunnskole til universitetsnivå.
- c. Tilby spesialiserte kurs og sertifiseringer for profesjonelle.

8. INTERNASJONALT SAMARBEIDE

Arbeide tettere med allierte land og internasjonale organisasjoner for å dele trusselinformasjon, beste praksis og koordinere respons på grenseoverskridende trusler.

Vi trenger å:

- a. Inngå bilaterale og multilaterale avtaler om cybersikkerhet.
- b. Være en aktiv pådriver for mer nordisk samarbeid og økt aktivitet i internasjonale fora som NATO, EU og FN.
- c. Bidra til utviklingen av internasjonale standarder og normer
- d. Etablere Norden som en felles sikkerhetssone med felles sikkerhetsklarering av personell, lagring av kritiske komponenter, duplisering av funksjoner og redundante løsninger.

9. MÅLING OG REGELMESSIGE VURDERINGER

Innføre KPIer som måler trusselbildet og beredskapen, og gjennomføre regelmessige risikovurderinger og "red team"-øvelser for å identifisere sårbarheter i systemene, samt teste beredskap og responskapasitet.

Vi trenger å:

- a. Gjennomføre regelmessige kriseøvelser.
- b. Utvikle spesifikke planer for beskyttelse av kritiske infrastrukturer.
- c. Etablere hurtige responskapasiteter ved cyberhendelser.

10. UTVIKLE EN VERDENSLEDENDE SIKKERHETSINDUSTRI

Norge har et godt utgangspunkt for å utvikle en verdensledende sikkerhetsindustri som vil bidra til at Norge kan ligge i front på cybersikkerhet. Norge er blant verdens mest digitale land, har høy kompetanse og modenhet, og vi er et land kjent for sikkerhet, forutsigbarhet og etterrettelighet.

Vi trenger å:

- a. Utvikle målrettede programmer for næringsutvikling av norsk sikkerhetsindustri
- b. Målrette satsingen på utvikling av økosystemet rundt cybersikkerhet inkludert datasenterindustrien, industrielle programvare etc.

VEDLEGG 1: Strategiske Sikkerhetsmål

Vi støtter “Strategiske Sikkerhetsråd” gitt av NSM i sin rapport “Et motstandsdyktig Norge – Sikkerhetsfaglige råd, 9 mai 2023

1. Norske virksomheter skaper bærekraftige verdier og ivaretar forsvarlig sikkerhet.
2. Norske myndigheter har en omforent situasjonsforståelse av trussel- og risikobildet.
3. Regjeringen får rettidig beslutningsstøtte som sikrer målrettet respons ved hendelser som kan skade nasjonal sikkerhet.
4. Sikkerhetsarbeidet i det norske samfunnet bidrar til å opprettholde tillit og til å styrke motstandskraft og forsvarsvilje i hele befolkningen.
5. Myndigheter, virksomheter og enkeltindivider gjenkjenner og varsler om sikkerhetstruende aktivitet og påvirkningsoperasjoner.
6. Norge har tilstrekkelig nasjonal kontroll over funksjoner og infrastruktur med betydning for nasjonal sikkerhet.
7. Norge har høy kompetanse innen cybersikkerhet og teknologier av betydning for nasjonal sikkerhet.
8. Norge har robust infrastruktur og satellittbaserte tjenester som understøtter totalforsvarsevnen gjennom krisespekteret.
9. Norge evner å motstå cyberoperasjoner som truer nasjonal sikkerhet i fred, krise og krig.
10. Alle deler av det norske samfunnet har digital motstandskraft på et langt høyere nivå.
11. Norske myndigheter hindrer at trusselaktører får tilgang til data om enkeltindivider som kan brukes til å skade nasjonal sikkerhet.
12. Norge har en god nasjonal evne til å avdekke, forhindre og håndtere innsidevirksomhet.

VEDLEGG 2: Relevante ressurser og referanser

Accenture

[State of Cybersecurity Resilience 2023](#)

[How cybersecurity boosts enterprise reinvention to drive business resilience](#)

Deloitte

[Deloitte Global Future of Cyber Survey 2023](#)

KPMG

[Cybersecurity considerations 2023](#)

Microsoft

[Developing a National Strategy for Cybersecurity: FOUNDATIONS FOR SECURITY, GROWTH, AND INNOVATION](#)

NSM

[Et motstandsdyktig Norge – sikkerhetsfaglige råd](#)

Radar Group

[State of the Nation Norge](#)

[Digital- og sikkerhetsmognad små og mellomstore svenska företag](#)

[Lägesbild cyberhot Maj 2023](#)

[Cybersäkerhet 2023](#)

[Säker digitalisering med hjälp av NIS2](#)

Telenor

[Det blir alvor – Digital sikkerhet 2023](#)

VEDLEGG 3: Langtidsplan for den digitale infrastrukturen

[Les mer om IKT-Norges forslag og rapport om en langtidsplan for den digitale infrastrukturen.](#)

VEDLEGG 4: Forslag til bevilgninger i Statsbudsjettet 2024

(Spilt inn til finansdepartementet i juni 2023)

IKT-Norge er fortsatt bekymret for Norges evne til å stå mot cybersikkerhet, bl.a. begrunnet med at cybersikkerhet ikke er prioritert høyt nok de siste årene og at det både utdannes og rekrutteres for få med spisskompetanse knyttet til cybersikkerhet. Dette gjenspeiles også i Riksrevisjonens seneste undersøkelse av myndighetens samordning av arbeidet med digital sikkerhet i sivil sektor. [Undersøkelsen](#) konkluderer bl.a. med at Justis- og beredskapsdepartementet ikke ivaretar ansvaret for digital sikkerhet i sivil sektor godt nok, noe som igjen kan få alvorlige konsekvenser for kritiske samfunnsfunksjoner og nasjonale sikkerhetsinteresser.

IKT-Norge er særlig bekymret for den digitale sikkerheten i kommunene. Bare ca. 60 prosent av norske kommuner mener at de har sikret sine egne data godt nok. Rapporten «[IT i praksis](#)» (Rambøll 2022) viser at kun 38 prosent av kommunene mener at de selv har tilstrekkelig kompetanse på informasjonssikkerhet.

En undersøkelse fra [YouGov](#) viser at et stort flertall av innbyggerne ikke har tillit til at kommunene har nok kunnskap til å ivareta personlige data på en trygg måte eller har tillit til at kommunen prioriterer IT-sikkerhet i tilstrekkelig grad. Bare 26 prosent har tillit til at kommunene har ressurs nok til å stå imot mulige hackerangrep.

Dessuten er datainnbrudd i kommunesektoren svært dyrt. Datainnbruddet i Østre Toten kommune i januar 2021 kostet kommunen minst [32 millioner kroner](#), i tillegg til [bot fra Datatilsynet](#) på 4 millioner kroner. Av dette har igjen staten kompensert Østre Toten med [16 millioner kroner](#).

Vi etterlyser derfor resultater av de 50 millioner kroner som ble bevilget til økt sikkerhet i kommunesektoren i forbindelse med Stortingets behandling av Prop. 78 S (2021–2022) “Ukraina-pakken” i fjor vår og viser bl.a. til [Dokument nr. 15:1726 \(2022–2023\)](#) hvor det fremgår at regjeringen fortsatt ikke har en plan for hvordan disse midlene skal brukes.

Vi er videre kjent med at Simula i innspill til KDD har tatt initiativ til å starte et arbeid for å utarbeide og vedlikeholde en oversikt over Norges digitale avhengigheter mot fremmede makter. Dette er etter vårt syn både et viktig og helt nødvendig arbeid. Vi ber derfor regjeringen sette av nødvendige midler til et slikt forskningsarbeid i forbindelse med statsbudsjettet for 2024

Vi viser også til vårt [innspill til næringsministeren](#) om et økt samarbeid mellom næringslivet og myndighetene knyttet til cybersikkerhet, spesielt i de minste bedriftene og våre forslag til konkrete tiltak.

Konkret ber IKT-Norge regjeringen om:

- 1. Målrettede tiltak for å styrke den digitale sikkerheten i kommunesektoren i størrelsesorden 50–100 mill. kroner**
- 2. Styrke nasjonalt cyberkrimsenter (NC3) med 50 mill. kroner**
- 3. Opprette et nasjonalt beredskapslager for sentrale IKT-komponenter**
- 4. Sørge for fortgang i arbeidet med å etablere en felles informasjonsportal etter [dansk modell](#).**
- 5. Vurdere å opprette et eget bransjeprogram knyttet til datasikkerhet i små bedrifter.**
- 6. Sette i gang et forsknings- og kartleggingsarbeid med formål å utarbeide og vedlikeholde en oversikt over Norges digitale avhengigheter mot fremmede makter.**