



Digitaliserings- og
forvaltningsdepartementet

Handlingsplan

Nasjonal sikkerhetsplan for digital infrastruktur

Elektronisk kommunikasjon i fred, krise og krig



Nasjonal
kommunikasjons-
myndighet

Nasjonal sikkerhetsplan

Frekvensforum

Rune Kanck - 19. november 2025

Nasjonal sikkerhetsplan for digital infrastruktur



- Langsiktig handlingsplan 2026 – 2030 for å styrke den digitale grunnmuren
- Lansert av regjeringen 1. september 2025
- Konkrete satsninger for å gjøre mobil- og bredbåndsnettene mer robuste og for å styrke beredskapen
- 10 satsningsområder med 37 konkrete tiltak
- Program for gjennomføring eies av DFD og ledes av Nkom
- Tiltakene skal gjennomføres i samarbeid med og med bidrag fra ekomtilbyderne
- Foreslått 400 mill kr i årlig offentlig finansiering

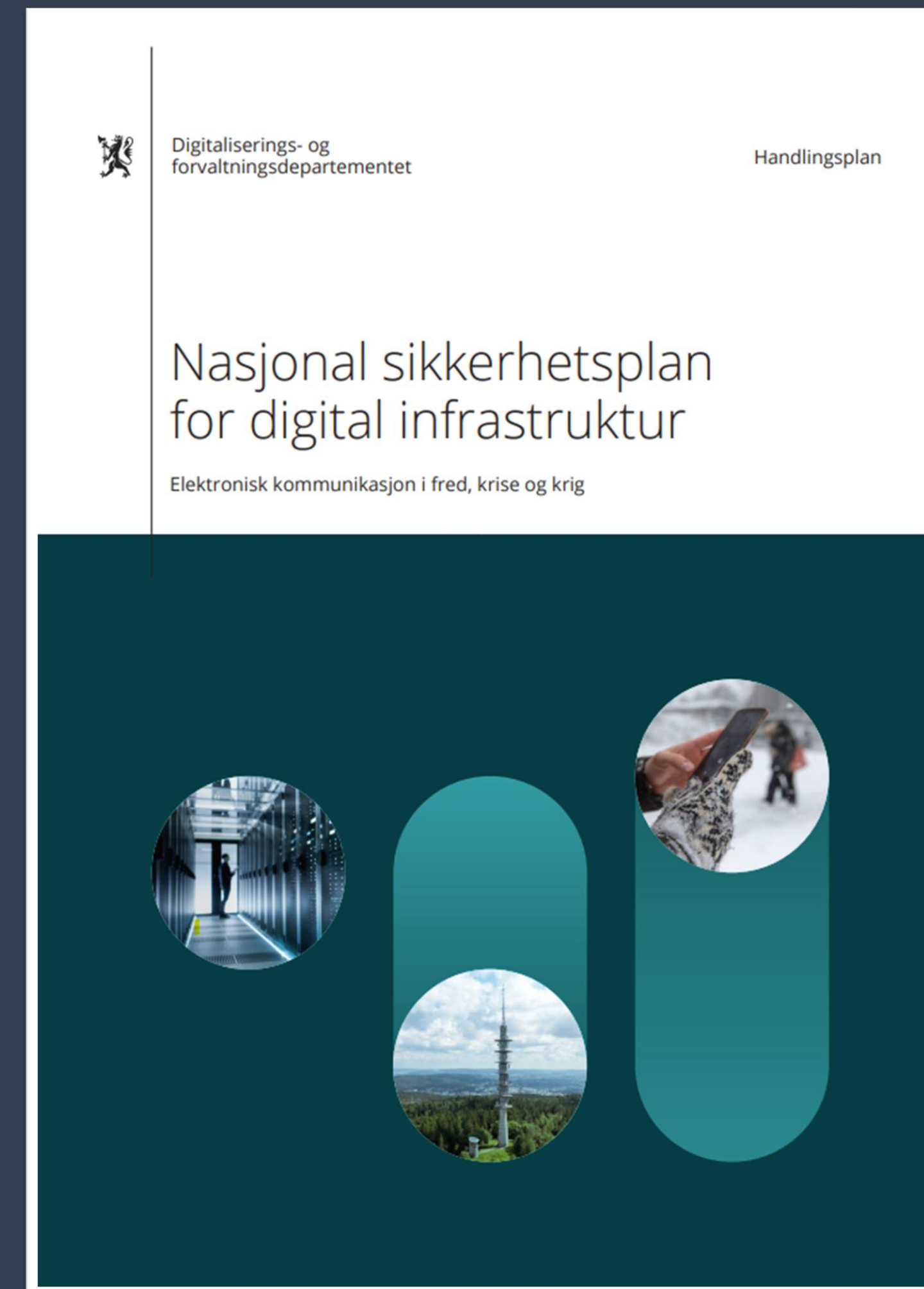
Bakteppe for nasjonal sikkerhetsplan



- Et sivil samfunn som er forberedt på krise og krig
- Et sivil samfunn som motstår sammensatte trusler
- Et sivil samfunn som understøtter militær innsats

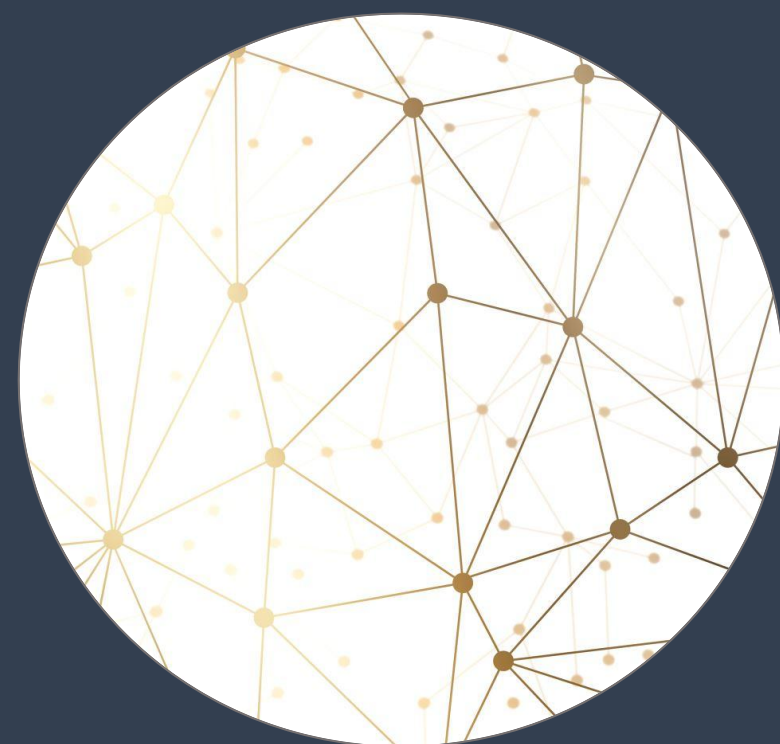


- Styrket forsvarsevne
- Motstandsdyktig samfunn
- Økonomisk sikkerhet



- Robuste nett og tjenester
- Regional robusthet og nasjonal samordning
- Nasjonal kontroll og sikkerhet i verdikjeden
- Samvirke og helhetlig beredskap

Fire hovedprinsipper i sikkerhetsplanen



Robuste nett og tjenester

Digital infrastruktur skal være robust og motstandsdyktig, med evne til å opprettholde eller raskt gjenopprette kritiske funksjoner i fred, krise og krig. Dette innebærer redundans, reservestrøm og alternative kommunikasjonsløsninger.



Regional robusthet og nasjonal samordning

Tiltak skal bygge på regionale risiko- og sårbarhetsanalyser, men være koordinert nasjonalt for å sikre lik beredskap i hele landet. Dette inkluderer forsterket ekom i sårbare kommuner og styrket transportnett.



Nasjonal kontroll og sikkerhet i verdikjeden

Kritisk digital infrastruktur og tjenester skal være under norsk kontroll eller sikret gjennom avtaler som ivaretar nasjonale sikkerhetsinteresser. Dette gjelder både fysisk infrastruktur, datasentre og digitale tjenester.



Samvirke og helhetlig beredskap

Planen skal understøtte totalforsvaret og bygge på samarbeid mellom stat, kommuner, næringsliv og frivillige aktører. Digital sikkerhet er en del av samfunnets samlede motstandskraft, og tiltak må sees i sammenheng med fysisk sikkerhet, energiforsyning og nødkommunikasjon.

Satsningsområder/tiltak

Forsterkningstiltak kritisk digital komm. Infrastruktur	Doble takten for å gjennomføre regionale risiko- og sårbarhetsanalyser
	- herunder oppdatere de eksisterende regionale analysene
	Tiltaksarbeid etter sårbarhetsanalyser
	Regional autonomi og datasentre
Økt motstandsevne for mobilnettene	Doble utbyggingstakt for forsterket ekom
	Styrket beredskap til 100 tettsteder og 300 utvalgte basestasjoner
	Ny bransjestandard for fysisk sikkerhet for kommunikasjonskabler
Sjø-fiber	Sikkerhet for undersjøiske kommunikasjonskabler
Satellitt	Satellittbasert kommunikasjon – dekning og beredskap
Nasj. kontroll	Nasjonal kontroll med kritisk digital infrastruktur

Posisjonerings og tidstjenester	Detektere, analysere, motstå og fjerne kilder til forstyrrelser av GNSS-signaler
	Nasjonal tjeneste for distribusjon av nøyaktig tid
	Nasjonal kontroll for posisjonerings-tjenester med bruk av 5G-posisjonering
Nordisk samarb.	Styrket nordisk samarbeid om digital sikkerhet og beredskap
Øvelse	Gjennomføre minst en årlig øvelse innenfor ekomsektoren og med andre myndigheter
Digitale angrep	Styrke motstandsevnen og håndteringen av digitale angrep med kunstig intelligens
	Styrke nasjonal kompetanse for digitalt forsvar av kritisk infrastruktur
Egenberedskap	Digital egenberedskap for befolkningen
	Digital egenberedskap for offentlige og private virksomheter
	Pilot for styrket lokal involvering med digital beredskap (satellitt)

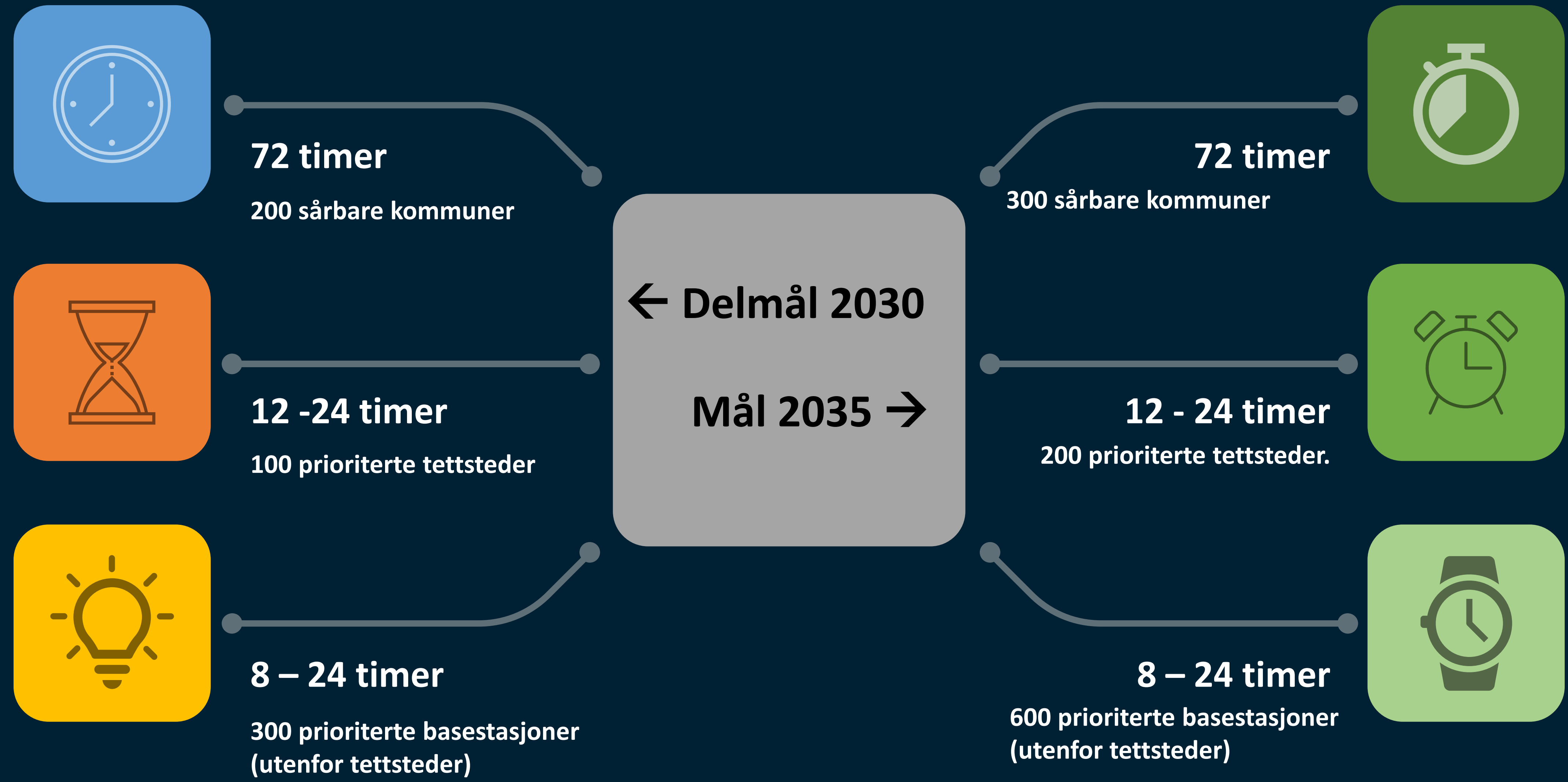


Prioritering av tiltak

- Sikkerhetsplanen krever betydelig tilgang på ressurser/personell for å sikre forventet fremdrift
- Alle tiltak kan ikke gjennomføres samtidig
- Gjennomføringsplan etablert
- Prioriterte tiltak for 2026:
 - Forsere regionale risiko- og sårbarhetsanalyser og tiltak
 - Doble utbyggingstakten for forsterket ekom programmet
 - Felles bransjestandard for fysisk sikring av fiberkabler
 - Pilotering
 - Økt reservestrøm
 - Reserverløsninger for gjenoppretting av mobildekning.
 - Nasjonal gjesting



Målbilde reservestrøm delmål 2030 og mål 2035



Regionale analyser

- Kartlegge og dokumentere sårbarheter i regionene
- Anbefalinger for å lukke sårbarheter
- Kompensasjonsordning for utpekte tiltak

«Robustifisering av Norge»



Programorganisering

**Forslag til
ny organisering**

