



id: SI\_006

model: mistralai/mistral-large-2512

seeds:

04\_risiko: mulighet

03\_relasjon: makt

05\_handling: forhandle

01\_perspektiv: strategisk

02\_tidhorisont: langsiktig

## Instans SI\_006

---

**Seeds:** strategisk (maktbalanse), langsiktig (systemresiliens), makt (koordineringsautoritet), mulighet (teknologisk og politisk), forhandle (interessekonflikter)

---

### Strategisk maktfordeling: Kommandosenteret som forhandlingsarena

Ditt prosjekt er ikke bare en teknisk plattform, men en maktstruktur som omdefinierer hvem som tar beslutninger under krise. **Nøkkelspørsmålet:** Hvem eier dataene, og hvem har veto over prediksjonsmodellene? Etabler en **trelags-autoritet**:

1. **Operativt lag** (brannvesen, redningstjeneste, lokale myndigheter) – direkte kommando under innsats, men med mulighet til å eskalere til neste nivå.
2. **Strategisk lag** (nasjonale direktorater, fagmiljøer som NIBIO eller RISE Fire Research) – kalibrerer modeller og godkjenner avvik fra prediksjoner.
3. **Politisk lag** (regjering, EU, forsikringsbransjen) – setter langsiktige rammer (f.eks. prioritering av infrastruktur vs. naturvern).

**Eksempel:** I Australia bruker AFAC (Australasian Fire and Emergency Service Authorities Council) en slik modell, men sliter med at delstater forhandler seg til unntak fra nasjonale retningslinjer. Lær av dette: **Bygg inn forhandlingsmekanismer** fra dag én (f.eks. digitale “veto-knapper” med begrunnelseskrav).

---



## Langsiktig mulighet: Plattformen som infrastruktur

Behandl plattformen som **kritisk infrastruktur** – ikke et engangsprosjekt. Tre konkrete grep:

1. **Standardiserte grensesnitt** for å koble til eksisterende systemer (f.eks. Norges Nødnett, EUs RescEU, eller private værsatellitter som Spire). Unngå “lock-in” ved å kreve åpne API-er.
  2. **Dual-use teknologi**: Plattformen må kunne håndtere flom, skred og terror – dette åpner for finansiering fra både sivil beredskap og forsvar (f.eks. Forsvarets forskningsinstitutt).
  3. **Testregime som bygger tillit**: Ikke bare simuleringer, men kontrollerte branner (som i FireScapes-prosjektet i USA) der modeller testes mot reelle data.  
**Krav**: 90% nøyaktighet på prediksjoner innen 6 timer for å få godkjenning.
-



## Arbeidspakker med maktperspektiv

Pakke	Ansvarlig	Unikt grep	Risiko (og mottiltak)
<b>1. Dataintegrasjon</b>	Norsk Regnesentral + private aktører (f.eks. StormGeo)	Mandat til å kreve data fra el-nett, droner, og sosiale medier (f.eks. Twitter-analyse for røykvarsler).	Motstand fra teleoperatører → Forhandle med Nasjonal sikkerhetsmyndighet som garantist.
<b>2. Prediksjonsmodeller</b>	NIBIO + internasjonale partnere (f.eks. Canadian Wildfire Information System)	Hybridmodell: Fysikk-baserte simuleringer + maskinlæring (tren på 30 års historiske branndata fra Skogbrann.no).	Overfitting til norske forhold → Test i Portugal (samarbeid med ANEPC) og California (Cal Fire).
<b>3. Kommandosenter</b>	Direktoratet for samfunnssikkerhet og beredskap (DSB) + brannvesen	Hierarkisk beslutningsstøtte: AI foreslår handlinger, men mennesker må godkjenne (jfr. Avinors flykontroll).	Beslutningslammelse → Øv på tabletop-simuleringer med alle aktører kvartalvis.
<b>4. Sikkerhet</b>	NSM + Forsvarets forskningsinstitutt	Zero-trust arkitektur: Alle enheter (droner, sensorer) må autentiseres, selv på eget nett.	Kostnadsoverskridelser → Bruk offentlig-privat partnerskap (f.eks. Kongsberg Gruppen for cyberforsvar).

## Dissens: Hvorfor “mainstream” feiler

De fleste brannplattformer fokuserer på teknologi – du må fokusere på **makt og forhandling**. Tre kontroversielle påstander:

- 1. Brannvesenet bør ikke ha enerett på dataene** – de er part i saken (f.eks. prioriterer de å redde bygninger fremfor skog). Løsning: Uavhengig datatilsyn (som Datatilsynet for personvern).



2. **Prediksjoner må være feilbare** – hvis modellen alltid har rett, vil ingen stole på den når den enda har feil. Løsning: Vis usikkerhetsintervaller i sanntid (som ECMWF for vær).
  3. **Kommandosenteret bør ikke være permanent** – det skaper avhengighet. Løsning: Distribuerte noder (f.eks. ett senter per fylke) som kan overta ved cyberangrep.
- 

## Neste steg

1. **Maktkartlegging**: Send ut spørreundersøkelse til alle aktører (brannvesen, kommuner, forsikring, miljøorganisasjoner) med ett spørsmål: “Hvilken beslutning ville du ikke tåle at plattformen tok for deg?” Bruk svarene til å designe veto-mekanismer.
2. **Pilot med maktkamp**: Velg en kontroversiell brannrisikosone (f.eks. Oslo-skogen vs. boligområder) og kjør en simulert krise der aktørene må forhandle seg frem til en løsning. Dokumenter hvor systemet bryter sammen.
3. **Finansieringsforhandling**: Ta kontakt med EU Horizon Europe (prioriterer “resilient infrastructure”) og Norges forskningsråd (programmet Samfunnssikkerhet), men krev at 20% av budsjettet går til samfunnsvitenskapelig forskning på makt og tillit.