FFI Forsvarets forskningsinstitutt

25/040

FFI-RAPPORT

Styrket sikkerhet og beredskap i kraftforsyningen

– tiltak og prioriteringer

Stig Rune Sellevåg
Karina Barnholt Klepper

Styrket sikkerhet og beredskap i kraftforsyningen
– tiltak og prioriteringer

Stig Rune Sellevåg
Karina Barnholt Klepper

Forsvarets forskningsinstitutt (FFI) 30. oktober 2025

Emneord
Nasjonal sikkerhet
Kraftforsyning
Sårbarhet
Beredskap
Totalforsvar

FFI-rapport
25/040

Prosjektnummer
5953

Online ISSN
2704-2383

Engelsk tittel
Strengthening Security of Supply and Preparedness for the Norwegian Power System – Measures and Priorities

Godkjennere
Janet Martha Blatny, *forskningsdirektør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Sammendrag

Pålitelig kraftforsyning er avgjørende for verdiskaping, befolkningens velferd og Norges sikkerhet. Sikkerheten og beredskapen i Norges kraftforsyning vil i årene fremover påvirkes av flere faktorer: krigen i Ukraina, Russlands militære utvikling, stormaktsrivaliseringen mellom USA og Kina, Kinas dominans innen fornybar energi og behovet for en rask og omfattende energiomstilling for å møte klimautfordringene.

Forsvarets forskningsinstitutt (FFI) har, på oppdrag fra Norges vassdrags- og energidirektorat (NVE) og Statnett, vurdert hvordan forsyningssikkerhet og beredskap i kraftforsyningen kan styrkes. Basert på våre funn har vi utarbeidet syv overordnede råd:

1. *Helhetlig tilnærming til risiko i hele konfliktspekteret*: Dette innebærer blant annet å bruke realistiske verstefallsscenarioer, utvikle planforutsetninger for beredskap i krig og at en større del av kraftsektoren underlegges sikkerhetsloven.
2. *Proaktiv tilnærming til digital sikkerhet for å realisere gevinstene ved digitalisering*: Dette krever blant annet en helhetlig handlingsplan for forsvarlig digitalisering av kraftsystemet.
3. *Styrket sikkerhet i anskaffelser og leverandørkjeder*: Dette omfatter blant annet å legge vekt på langsiktige sikkerhetsvurderinger og utvide kraftberedskapsforskriften § 7-14 k.
4. *Videreføre krav til driftsradio og elektronisk kommunikasjon i driftskontrollsystemet.* I tillegg bør kravet til reservestrøm for driftsradio skjerpes til 72 timer i særlig viktige eller utsatte områder.
5. *Etablere sikringstiltak mot luftleverte våpen*: Dette inkluderer fysiske tiltak mot små sprengladninger. Sikring i fjellanlegg bør vurderes ved nyetablering eller utskifting av eksisterende kritiske anlegg som har lang teknisk levetid.
6. *Bygge opp reparasjonsberedskap dimensjonert for krigsscenarioer*: Dette innebærer større og flere regionalt spredte beredskapslagre, sikringskrav til lagrene og styrket nasjonal kompetanse og egenkapasitet.
7. *Trene og øve kraftforsyningens beredskapsorganisasjon (KBO) og styrke nordisk beredskapssamarbeid*: Dette inkluderer å oppdatere planverk, holde regelmessige øvelser for ekstraordinære situasjoner og krigsscenarioer og inkludere særlig viktige leverandørbedrifter i KBO.

Rådene er utdypet i 36 konkrete tiltak. Vi anbefaler at disse inngår i kunnskapsgrunnlaget Stortinget har bedt regjeringen om i arbeidet med å styrke beredskapen i kraftsystemet.

Videre utbygging av kraftsystemet og styrking av forsyningssikkerheten vil føre til betydelige kostnader. Forskning, utvikling og innovasjon må tas i bruk for å sikre at Norge fortsatt har rikelig tilgang på rimelig, sikker og fornybar elektrisk kraft i en verden preget av ustabilitet og usikkerhet.

Summary

Reliable power supply is critical for value creation, public welfare, and national security. The security and preparedness of Norway's power supply will be greatly impacted by external factors in the years ahead: the war in Ukraine, Russia's military developments, great power rivalry between the United States and China, China's dominance in renewable energy, and the urgent need for a rapid and comprehensive energy transition to address climate challenge.

The Norwegian Defence Research Establishment (FFI), commissioned by the Norwegian Water Resources and Energy Directorate (NVE) and Statnett, has assessed how security of supply and preparedness for the Norwegian power system might be strengthened. Based on our findings, we present seven overarching recommendations:

1. *Adopting a holistic approach to risk across the entire conflict spectrum*: This includes using realistic worst-case scenarios, developing planning assumptions for wartime preparedness, and subjecting more of the power sector to the Norwegian Security Act.
2. *Taking a proactive approach to digital security to realise the benefits of digitalisation*: This requires a comprehensive action plan for responsible digitalisation of the power system.
3. *Strengthening security in procurement and supply chains*: This involves emphasising long-term security assessments and expanding Section 7-14 k of the Regulation on Security and Emergency Preparedness in the Power Supply System.
4. *Maintaining current requirements for operational radio and communication systems.* And moreover, tightening the requirement for emergency power capacity for operational radio to 72 hours in particularly important or vulnerable areas.
5. *Implementing protective measures against airborne weapons*: This includes physical security against small explosive devices. Fortified facilities should be considered when establishing new critical assets with long technical lifetime or replacing existing ones.
6. *Building repair preparedness dimensioned for wartime scenarios*: This includes larger and more regionally distributed emergency stockpiles, introducing security requirements for these stockpiles, and strengthening national competence and self-sufficiency.
7. *Training and exercising the power supply's emergency preparedness organisation (KBO) and strengthening Nordic cooperation*. This includes updating plans, conducting regular exercises for extraordinary situations and wartime scenarios, and incorporating particularly important suppliers into KBO.

These recommendations are elaborated in 36 specific measures. We recommend that these be included in the knowledge base requested by the Norwegian Parliament for the government's plans to strengthen preparedness in the power system.

Further development of the power system and strengthening of security and preparedness will entail significant costs. Research, development, and innovation must be utilised to ensure that Norway continues to have abundant access to affordable, secure, and renewable electricity in a world marked by instability and uncertainty.

Innhold

1 Innledning

Pålitelig kraftforsyning er avgjørende for verdiskaping, befolkningens velferd og norsk sikkerhet. Kraftforsyningen spiller derfor en viktig rolle i å understøtte de tre hovedprioriteringene i Norges nasjonale sikkerhetsstrategi. Disse er styrket forsvarsevne, et mer motstandsdyktig samfunn og styrket økonomisk sikkerhet.[1]

Russlands fullskala invasjon av Ukraina 24. februar 2022 gjorde at Europa opplevde en energikrise.[2] I 2025 er energikrisen i stor grad over, og den europeiske energiomstillingen fortsetter i høyt tempo. Omstillingen er drevet både av behovet for å nå klimaforpliktelsene og av behovet for å bli uavhengig av fossilt brensel fra Russland raskest mulig.[3]

Samtidig har Norge blitt viktigere geopolitisk som følge av rollen vår som energileverandør til Europa. Russland anser seg å være i direkte konflikt med Vesten. Etterretningstjenesten mener at dette vil vedvare uavhengig av utfallet av krigen i Ukraina.[4] NATO-medlemskapet vårt, posisjonen vår som energinasjon og den geografiske nærheten vår til Russland gjør at vi kan bli utsatt for press og angrep. I tillegg fører energiomstilling til at Norges kraftforsyning vil spille en stadig viktigere rolle fremover.

Forsyningssikkerheten til kraftforsyningen (boks 1.1) vil avhenge av hvordan kraftsystemet utvikler seg. Statnetts markedsanalyse for 2024–2029 peker på at det trolig blir lite bygging av ny kraftproduksjon i Norge frem mot 2029,[5] men Norges vassdrags- og energidirektorat (NVE) forventer ikke kraftunderskudd i Norge i et normalår.[6] NVE forventer likevel at kraftbalansen vil svekkes i det sørlige Norge, mens den vil være tilnærmet uendret i Midt- og Nord-Norge.[7] Imidlertid ville realisering av alt forbruk som har reservert kapasitet, gitt 20–25 TWh i underskudd på energibalansen i 2029. Det er også behov for fornyelse av transmisjons- og regionalnettet siden mye av dette nettet nærmer seg sin tekniske levealder.[8]

Frem mot 2050 forventer Statnett det at utbygging av sol- og vindkraft i Europa vil fortsette.[9] Imidlertid gjøres det ikke nok for å jevne ut den uregulerbare fornybarproduksjonen etter hvert som kullkraft fases ut. I Norge vil forbruksveksten være avhengig av mer kraftproduksjon, men denne veksten forutsetter lave nok kraftpriser.[10] Det er derfor fortsatt behov for å forsterke kraftnettet og øke overføringskapasiteten mellom regioner i Norge.[11] Skal vi nå ambisjonene om

[1] Statsministerens kontor (2025).
[2] International Energy Agency (2022).
[3] EUs plan *REPowerEU* skal bidra til energieffektivisering, akselerert produksjon av og overgang til ren energi, diversifisering av energiforsyningen og smarte investeringer (European Commission, 2022).
[4] Etterretningstjenesten (2025, s. 6)
[5] Statnett (2024).
[6] Norges vassdrags- og energidirektorat (2025a).
[7] Norges vassdrags- og energidirektorat (2025a, s. 19).
[8] Norges vassdrags- og energidirektorat (2025a, s. 30).
[9] Statnett (2025a).
[10] Statnett (2025a).
[11] Statnett (2025a, s. 4).

energiomstilling og ny industriutvikling, trengs det, i tillegg til større nettkapasitet, også mer effektiv og fleksibel energibruk på alle områder, at vi utnytter alle kilder til mer fornybar kraft, og raskere saksbehandling for ny kraftproduksjon.[12]

Samtidig kan naturhensyn, folkelig motstand, høye kostnader og lange ledetider føre til at kraftutbyggingen og forsterkingen av kraftnettet går saktere eller stopper opp. Norske politikere og myndigheter kan derfor bli stilt i en situasjon der de må velge mellom å godta overgangsperioder med stram eller negativ kraftbalanse, å utsette elektrifiseringsprosjekter eller å begrense tilknytningen av ny kraftkrevende industri.[13]

Boks 1.1 – Hva er forsyningssikkerhet i kraftforsyningen?

Forsyningssikkerhet for strøm er beskrevet som «kraftsystemets evne til å kontinuerlig levere strøm av en gitt kvalitet til sluttbrukere, og omfatter energisikkerhet, effektsikkerhet og driftssikkerhet/leveringspålitelighet»:[A]

- Energisikkerhet er «evnen til å dekke strømbruk over lengre tid».
- Effektsikkerhet er «kraftsystemets evne til å dekke den momentane strømbruken».
- Driftssikkerhet er «kraftsystemets evne til å unngå driftsforstyrrelser».
- Leveringspålitelighet er «knyttet til tilgjengeligheten av strøm og kan måles i antall avbrudd i strømforsyningen og avbruddenes varighet».

[A] NOU 2023: 3 (s. 148–149).

Behovet for å styrke norsk og europeisk sikkerhet og forsvarsevne vil også ha betydning for den fremtidige utviklingen av kraftforsyningen. NATOs medlemsland har forpliktet seg til å integrere sivil beredskapsplanlegging i NATOs forsvarsplanlegging[14] og bruke opp mot 1,5 % av BNP årlig på blant annet kritisk infrastruktur og sivil beredskap som er viktig for sikkerhet og forsvarsevne.[15] Dette kan medføre nye krav til forsyningssikkerhet og beredskap i kraftforsyningen. I Norge har et enstemmig Storting gått inn for å gi «særskilt prioritering av strømnett» for «forsvarsindustrien og andre kritiske samfunnsfunksjoner med betydning for nasjonale sikkerhetsinteresser»,[16] og et forslag om å endre energiloven om prioritert nettilknytning av hensyn til nasjonale sikkerhetsinteresser ble sendt på høring i 2025.[17]

[12] NOU 2023: 3 (s. 9–25).
[13] NOU 2023: 3 (s. 24).
[14] NATO (2024).
[15] NATO (2025).
[16] Innst. 224 S (2024-2025) .
[17] Energidepartementet (2025).

Når samfunnet skal elektrifiseres i høy fart og gamle anlegg skal fornyes, blir forsyningssikkerhet viktigere, men også mer krevende å opprettholde.[18] Dette skal skje i en tid med stormaktsrivalisering, krig i Europa og dyp usikkerhet. Erfaringer fra Ukraina viser at kraftforsyningen kan bli utsatt for omfattende militære angrep i krig (dette er nærmere omtalt i kapittel 7). Imidlertid har verken totalberedskapsmeldingen[19] eller langtidsplanen for forsvarssektoren[20] behandlet behovet for forsyningssikkerhet og beredskap i kraftforsyningen i et skjerpet sikkerhetspolitisk utfordringsbilde i nevneverdig grad. Gjennom behandlingen av totalberedskapsmeldingen ba Stortinget regjeringen om å «utarbeide planer for styrket beredskap i kraftsystemet og komme tilbake til Stortinget på egnet måte».[21] Det er derfor behov for å styrke kunnskapsgrunnlaget som er nødvendig for å utarbeide gode planer for styrket kraftforsyningsberedskap.

1.1 Formål og metodisk tilnærming

I 2023 fikk Forsvarets forskningsinstitutt (FFI) i oppdrag av NVE og Statnett å utrede hvordan forsyningssikkerhet og beredskap i kraftforsyningen kan styrkes. Denne rapporten er sluttrapporten for oppdraget. Utredningsbehovet var særlig knyttet til digitalisering og virtualisering av kraftsystemet og nye forretningsmodeller, elektronisk kommunikasjon og nødsamband i kraftforsyningen, reparasjonsberedskap og globale forsyningskjeder, og analyse av sårbarhetsreduserende tiltak og beredskapstiltak. Utredningen av de nevnte temaene ble gjennomført i form av delutredninger som er dokumentert i egne rapporter og notater.[22] Sentrale forskningsspørsmål og hypoteser for utredningen er oppsummert i vedlegg A.

Formålet med denne rapporten har vært å lage en syntese av funnene fra delutredningene for å kunne gi helhetlige råd om hvordan forsyningssikkerhet og beredskap i kraftforsyningen bør styrkes. Rådene kommer frem via en risikobasert tilnærming, der FFI har vurdert mulige tilsiktede handlinger som kan true norsk kraftforsyning, og holdt dette opp mot funn og sårbarheter som er identifisert i de ulike delutredningene. Ut fra denne syntesen har FFI gjort en forenklet effekt-kostnadsvurdering av de ulike rådene (vedlegg B) og gitt forslag til prioriteringer. Den metodiske tilnærmingen er nærmere beskrevet i vedlegg A.

1.2 Avgrensninger og begrensninger

FFIs funn og anbefalinger er avgrenset til vurderinger av tilsiktede handlinger i hele konfliktspekteret. Rapporten gir derfor ikke en helhetlig beskrivelse eller vurdering av utfordringer som kan påvirke forsyningssikkerheten. Viktige problemstillinger knyttet til eksempelvis naturfarer

[18] NOU 2023: 3 (s. 148).
[19] Meld. St. 9 (2024-2025) .
[20] Prop. 87 S (2023-2024) .
[21] Innst. 242 S (2024-2025) .
[22] Flere av notatene og rapportene er unntatt offentlighet eller gradert etter sikkerhetsloven.

er derfor utelatt. Denne utredningen har heller ikke belyst problemstillinger knyttet til en eventuell etablering av kjernekraft i Norge.[23]

FFI har ikke systematisk gått gjennom litteraturen knyttet til forsyningssikkerhet og beredskap i kraftforsyningen. Dette var ikke formålet med oppdraget til FFI, og det har heller ikke vært vurdert som nødvendig. Selv om studien ikke er komplett, mener vi likevel at rapporten trekker frem viktige forhold som er av avgjørende betydning for forsyningssikkerhet og beredskap i kraftforsyningen.

Tidshorisonten for FFIs vurderinger er frem mot 2036.[24] Analysene og vurderingene er basert på en forutsetning om at det ikke skjer strategiske sjokk som utredningen ikke har tatt høyde for. Analysen har også lagt til grunn en forutsetning om at Norge vil fortsette å være medlem av NATO, EØS og Schengensamarbeidet, men ikke av EU i perioden frem mot 2036.

1.3 Slik er rapporten bygget opp

Hovedanbefalingene med forslag til prioriteringer er oppsummert i kapittel 2, og utdypet i kapitlene 3–9. Konklusjoner er gitt i kapittel 10. Rapportens metodiske tilnærming er gitt i vedlegg A. En forenklet effekt-kostnadsvurdering av anbefalingene er gitt i vedlegg B. Viktige forkortelser som er brukt i rapporten, er gitt i tabell 1.1.

Tabell 1.1 Forkortelser brukt i rapporten

Forkortelse	Forklaring
Ekom	Elektronisk kommunikasjon
FFI	Forsvarets forskningsinstitutt
GEI	Global Energy Interconnection
IoT	Tingenes internett (Internet of Things)
KBO	Kraftforsyningens beredskapsorganisasjon
KDS	Kraftforsyningens distriktssjefer
KSL	Kraftforsyningens sentrale ledelse
NSM	Nasjonal sikkerhetsmyndighet
NVE	Norges vassdrags- og energidirektorat
OT	Operasjonell teknologi
PST	Politiets sikkerhetstjeneste

[23] Denne problemstillingen har vært utenfor oppdraget som ble gitt til FFI fra NVE og Statnett. Se Kippe (2025) for en diskusjon rundt sikkerhetsaspekter ved kjernekraft i Norge.
[24] Tidshorisont for Norges forsvarsløft (Prop. 87 S (2023-2024)).

2 Anbefalte tiltak og prioriteringer

2.1 Hovedråd

Det er tre forhold som vil få avgjørende betydning for sikkerhet og beredskap for Norges kraftforsyning i årene fremover:

- krigen i Ukraina og Russlands militære utvikling, som gjør at Norge må være forberedt på storkrig[25]
- stormaktsrivaliseringen mellom USA og Kina, og Kinas dominans innen fornybar energi[26]
- behovet for rask og omfattende energiomstilling for å møte klimautfordringene

Basert på FFIs funn og vurderinger gir vi syv overordnede råd om hvordan forsyningssikkerheten og kraftforsyningsberedskapen bør styrkes:

1. Kraftsektoren må ha en helhetlig tilnærming til risiko i hele konfliktspekteret. Dette inkluderer blant annet å bruke realistiske verstefallsscenarioer, utvikle planforutsetninger for dimensjonering av kraftforsyningsberedskapen i krig og at en større del av kraftsektoren underlegges sikkerhetsloven.

2. Kraftsektoren må ha en proaktiv tilnærming til digital sikkerhet for å realisere gevinstene som digitalisering av kraftsystemet kan gi.[27] Dette inkluderer blant annet å utvikle en helhetlig handlingsplan for forsvarlig digitalisering av kraftsystemet slik at gevinster realiseres og krav til forsyningssikkerhet og digital sikkerhet opprettholdes.

3. Kraftsektoren må styrke sikkerheten i anskaffelser og leverandørkjeder. Dette inkluderer å vektlegge langsiktige sikkerhetsvurderinger, utvide kraftberedskapsforskriften § 7-14 k og utforske muligheter for nasjonal produksjon av kritiske komponenter til kraftforsyningen.

4. Dagens krav i kraftberedskapsforskriften til driftsradio og samband i driftskontrollsystemet (§§ 7-14 og 7-17) må videreføres. Samtidig bør kravet til reservestrøm for driftsradioen skjerpes til 72 timer i særskilt viktige eller utsatte geografiske områder.

5. Kraftsektoren må etablere sikringstiltak mot luftleverte våpen. Dette inkluderer blant annet fysiske sikringstiltak mot små luftleverte sprengladninger for eksisterende kritiske

[25] Forsvarets forskningsinstitutt (2025).
[26] Loen og Gusdal (2025).
[27] Digitalisering av kraftsystemet inkluderer blant annet smart styring av forbruk, sensorsystemer i kraftforsyningen, nye markedsplattformer, automatisering og beslutningsstøtte og nye konstellasjoner av kraftprodusenter (Ulshagen et al., 2025).

kraftanlegg. I tillegg bør anlegg som NVE vurderer som mest kritiske, og som har lang teknisk levetid, sikres i fjellanlegg.

6. Kraftsektoren må etablere en reparasjonsberedskap som er dimensjonert for krigs-scenarioer. Dette inkluderer blant annet å etablere større og flere regionalt spredte beredskapslagre for å øke reparasjonsevnen og utholdenheten i en krise- eller krigssituasjon, etablere beredskapslagre for elektroniske komponenter som er kritisk viktige for forsyningssikkerheten, etablere sikringskrav til beredskapslagre og styrke nasjonal egenevne og kompetanse.

7. Kraftforsyningens beredskapsorganisasjon (KBO) må trenes og øves, og det nordiske beredskapssamarbeidet innen kraftforsyning må styrkes. Dette inkluderer blant annet at KBO må ha oppdatert planverk, og at KBO-enhetene, kraftforsyningens distriktssjefer (KDS) og kraftforsyningens sentrale ledelse (KSL) regelmessig øver på å håndtere ekstraordinære situasjoner og krigsscenarioer. I tillegg bør KBO utvides til å inkludere særlig viktige bedrifter i leverandørbransjen.

De syv hovedrådene er utdypet i kapittel 3–9 og konkretisert i 36 foreslåtte tiltak. Nedenfor oppsummeres tiltakene sammen med et forslag til prioritering av tiltakene.

2.2 Tiltak og prioriteringer

FFI har gjort en forenklet og kvalitativ (ikke-prissatt) effekt-kostnadsvurdering av tiltakene (vedlegg B). Formålet med dette har vært å kategorisere tiltakene for å gi råd om

- tiltak som vil gi stor positiv effekt, men som vil kreve store ressurser og ta lang tid å implementere, og derfor bør startes opp raskt
- tiltak som kan karakteriseres som «lavthengende frukter» fordi de medfører liten eller ubetydelig kostnadsvirkning
- tiltak som bør utredes nærmere for å realisere ønsket effektvirkning, gitt indikert kostnadsvirkning

Denne kategoriseringen kan danne grunnlag for prioriteringer. Hvilken effekt tiltaket har, er vurdert ut fra hvilken risikoreduserende virkning tiltaket kan ha for kraftforsyningen (se vedlegg A.3). Merk at effekt-kostnadsvurderingene *ikke* er ment som en rangering av tiltakene – de kan altså ikke benyttes for å sette ulike tiltak opp mot hverandre. Til det er tiltakene for forskjellige og usikkerhetene for store. FFI har heller ikke vurdert synergier mellom tiltakene. Dette bør utredes nærmere.

Ressurs- og tidkrevende tiltak med stor eller meget stor positiv effekt

Anbefalinger til Energidepartementet:

- KBO-enheter i geografiske områder som er av stor betydning for nasjonale sikkerhetsinteresser og forsvarsevne, bør underlegges sikkerhetsloven.

Anbefalinger til NVE:

- Det bør etableres fysisk sikring mot små[28] luftleverte sprengladninger for eksisterende anlegg som NVE vurderer som mest kritiske.
- Kritiske anlegg bør sikres i fjellanlegg ved nyetablering eller utskifting av eksisterende anlegg.
- Det bør etableres større og flere regionalt spredte beredskapslagre for å øke reparasjonsevnen og utholdenheten i en krise- eller krigssituasjon.
- Kraftberedskapsforskriften bør utvides til å sette krav til klassifisering og sikring av beredskapslagre.

Anbefalinger til KBO-enhetene:

- KBO-enhetene bør øke egen reparasjonsevne med tanke på materiell og tilgjengelig kompetanse for å redusere avhengigheten av eksterne leverandører.

Tiltak med ingen, ubetydelig eller liten negativ kostnadsvirkning («lavthengende frukter»)

Anbefalinger til Energidepartementet:

- Det bør etableres planforutsetninger for dimensjonering av kraftforsyningsberedskapen i krig.
- Regjeringens strategi for å styrke motstandskraften mot desinformasjon bør operasjonaliseres i kraftsektoren.
- Det bør foretas en gjennomgang av transportplanleggingen for å avdekke om endringer i transportinfrastrukturen kan ha betydning for kraftforsyningsberedskapen (i samarbeid med Samferdselsdepartementet).
- Mulighetsrommet for å etablere produksjon av kritiske komponenter for kraft-forsyningen i Norge eller gjennom nordisk samarbeid bør utredes (i samarbeid med Nærings- og fiskeridepartementet).

[28] Hva som karakteriseres som små luftleverte sprengladninger, er opplysninger som er unntatt offentlighet (Lausund & Dullum, 2025).

Anbefalinger til Kunnskapsdepartementet:

- Det bør vurderes hvordan fagutdanninger innen elkraft kan styrkes for å øke rekrutteringen til kraftsektoren, for slik å styrke nasjonal egenevne innen kraftforsyningsberedskap (i samarbeid med Energidepartementet).

Anbefalinger til NVE:

- Veiledere for risikovurderinger og styring av risiko bør videreutvikles slik at de er oppdatert i forhold til forskningsfronten innen risikofaget.
- KBO-enhetene bør ha økt kunnskap om hvordan de kan utnytte scenarioanalyser.
- Arbeidet med å utvikle og vedlikeholde et overordnet trusselbilde for kraftforsyningen bør videreføres.
- Det bør skapes arenaer for erfaringslæring og deling av mønsterpraksis innen digital sikkerhet (i samarbeid med KraftCERT).
- Veiledere for sikkerhet i anskaffelser og leverandørkjeder for kraftsektoren bør videreutvikles (i samarbeid med Nasjonal sikkerhetsmyndighet (NSM)).
- De strategiske hovedprioriteringene[29] i nasjonal sikkerhetsstrategi bør inkluderes i konsesjonsbehandlingen av klassifiserte kraftanlegg.
- Det bør etableres forbud mot uautorisert droneflyging over kraftanleggene som NVE vurderer som mest kritiske.
- Politiet og Forsvaret må holdes oppdatert om hvilke anlegg som vurderes som mest kritiske for kraftforsyningen.
- Planverket som ligger til grunn for KBO, bør gjennomgås, og KBO-enhetene, kraftforsyningens distriktssjefer (KDS) og kraftforsyningens sentrale ledelse (KSL) bør regelmessig trene og øve.
- NVE bør gå i dialog med Forsvaret og Sivilforsvaret når det gjelder fritak fra militær- eller sivilforsvarstjeneste for personell i KBO-enheter ved krise og krig, herunder fritak fra rekvirering av transportmidler.

Anbefalinger til KBO-enhetene:

- KBO-enhetene bør gjennomgå leverandøravtalene sine for å sikre tilstrekkelig reparasjonsevne i hele konfliktspekteret.
- KBO-enhetene bør videreutvikle sikkerhets- og beredskapssamarbeidet sitt med nordiske kraft- og nettselskaper

[29] De strategiske hovedprioriteringene i den nasjonale sikkerhetsstrategien er: (1) raskt styrke forsvarsevnen, (2) gjøre samfunnet mer motstandsdyktig og (3) styrke vår økonomiske sikkerhet (Statsministerens kontor, 2025).

Tiltak med middels eller større positiv effekt, men med middels eller stor negativ kostnadsvirkning

Anbefalinger til NVE:

- Prosesser og metoder som gir oversikt over risiko i kraftforsyningen som helhet, bør videreutvikles.
- Evnen til å detektere og håndtere IKT-sikkerhetshendelser i kraftsektoren bør videreutvikles.
- Kravene i NIS2-direktivet bør danne minimumsnivået for digital sikkerhet på områder som ikke dekkes av kraftberedskapsforskriften.
- Regelverket for anskaffelser av utstyr til anlegg i klasse 1–3 bør skjerpes, eksempelvis ved at kraftberedskapsforskriften § 7-14 k gjøres gjeldende for et større omfang av driftskontrollsystemer enn dagens krav.
- Kravet i kraftberedskapsforskriften om at ekom til driftskontrollfunksjonen skal fungere uavhengig av funksjonssvikt i offentlige ekomtjenester, bør opprettholdes.
- Kravet i kraftberedskapsforskriften om at driftsradio skal fungere uavhengig av funksjonssvikt i offentlige ekomtjenester, bør opprettholdes.
- Kravet i kraftberedskapsforskriften til reservestrøm for driftsradioen bør skjerpes til 72 timer i områder som er viktige for nasjonale sikkerhetsinteresser og nasjonal forsvarsevne.
- Det bør forberedes tiltak for rask gjenoppretting dersom kritiske anlegg som ikke er sikret i fjellanlegg, skades eller ødelegges.
- Kraftforsyningens beredskapsorganisasjon bør utvides til å inkludere særlig viktige bedrifter i leverandørbransjen.
- Oppfølgingen og kontrollen med etterlevelse av kraftberedskapsforskriften § 2-7 bør styrkes, og veiledere for øvelser bør videreutvikles.

Anbefalinger til Statnett:

- Statnett (som systemansvarlig) bør i samarbeid med andre KBO-enheter utvikle en helhetlig handlingsplan for forsvarlig digitalisering av kraftsystemet slik at gevinster realiseres og krav til forsyningssikkerhet og digital sikkerhet opprettholdes.

Tiltak som bør utredes nærmere

Følgende tiltak bør utredes nærmere av NVE for å realisere ønsket effektvirkning:

- ordninger for validering og sertifisering av maskinvare som benyttes i kraftforsyningen
- dokumentasjonskrav til leverandører av programvare til kraftforsyningen[30]

[30] Såkalt *software bill of materials*.

3 Helhetlig tilnærming til risiko

Utfallsrommet for fremtidige tilsiktede handlinger som kan true norsk kraftforsyning, er stort og beheftet med stor usikkerhet. FFI har beskrevet følgende kategorier av tilsiktede handlinger som norsk kraftforsyningsberedskap må ta høyde for:[31]

- Trusler fra fremmedstatlige aktører:
    - sammensatte trusler i form av maktposisjonering, fordekt tvang, sabotasje eller tvangsdiplomati
    - væpnede angrep i form av ukonvensjonell krigføring, begrenset angrep eller strategisk overfall

- Trusler fra politisk motiverte ikke-statlige aktører:
    - ekstremisme

- Trusler fra kriminelle aktører:
    - datakriminalitet

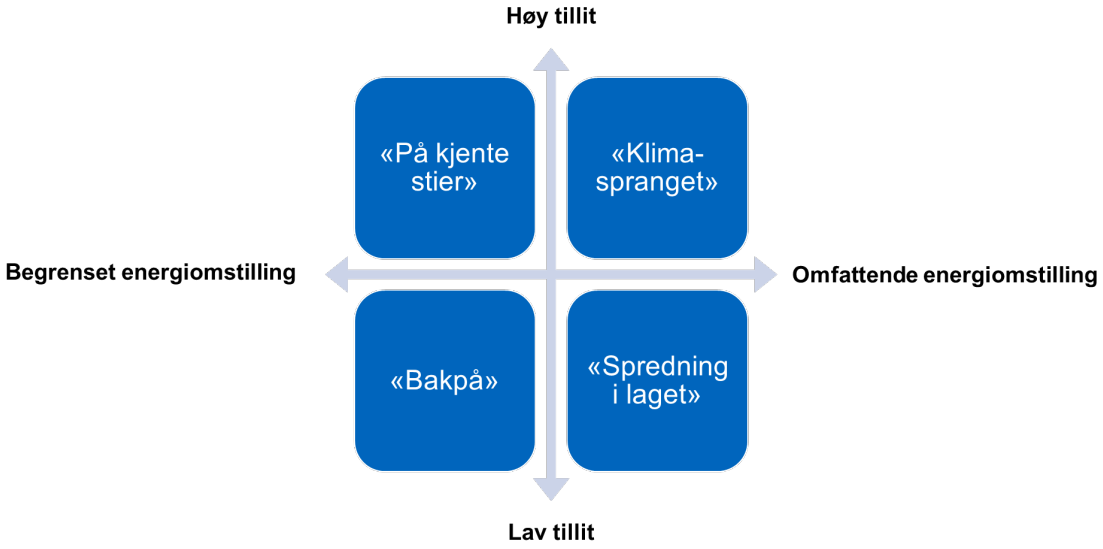
Som pekt på innledningsvis er det også usikkerhet knyttet til samfunnsutviklingen mot lav-utslippssamfunnet som er nødvendig for å nå Norges klimaforpliktelser. Usikkerheten er knyttet til (*i*) omfanget av og tempoet på energiomstillingen, (*ii*) hvor omfattende digitaliseringen av kraftsystemet blir (se kapittel 4), og (*iii*) i hvilken grad tilliten i samfunnet opprettholdes under energiomstillingen. FFI har beskrevet denne usikkerheten i form av fire fremtidsbilder som vi har kalt «På kjente stier», «Bakpå», «Spredning i laget» og «Klimaspranget» (figur 3.1). Hvilke konkrete scenarioer for tilsiktede handlinger som kan utspille seg, vil derfor også være avhengig av hvordan samfunnet utvikler seg på vei mot et lavutslippssamfunn.

Det trengs helhetlig tilnærming til risiko i kraftsektoren
Det er også usikkerhet knyttet til om det er mulig å gjennomføre en rask og omfattende energi-omstilling uten at Norge blir svært avhengig av tilgang til kinesiske råmaterialer og teknologier innen fornybar energi. Usikkerheten er ikke bare knyttet til sannsynligheter for ulike hendelser, men også om hvor god kunnskap vi har om temaene, og hvorvidt det kan oppstå overraskelser.

Videreutviklingen av Norges kraftforsyning må ta hensyn til denne usikkerheten. I situasjoner med høy usikkerhet kan det oppstå et «informasjonsgap» mellom hva som *er* kjent, og hva som *må* være kjent for å ta gode valg.[32] Betydningen av usikkerhet står sentralt i forskning innen risikofaget. I risikofaget vurderes risiko ut fra konsekvenser og usikkerhet, der konsekvensene relateres til en gitt referanse (for eksempel dagens nivå eller tilstand).[33,34] I situasjoner der

[31] Sellevåg (2023).
[32] Ben-Haim (2019).
[33] Aven (2016); Aven (2017).
[34] Bruk av tradisjonelle risikomatriser som uttrykker risiko i form av sannsynligheter og konsekvenser, er en fremgangsmåte som ikke kan forsvares faglig (Aven, 2017).

usikkerhetene blir så store at det ikke er meningsfullt å uttrykke risiko, bør risikoanalyser erstattes med scenarioanalyser.



Figur 3.1 Alternative fremtider som kan oppstå som følge av usikkerhet knyttet til tillit i samfunnet og energiomstilling. Illustrasjon: FFI.[35]

Det er også nødvendig med gode strategier for risikostyring. Viktige strategier for risikostyring er å være risikoinformert, bruke forsiktighetsprinsippet og føre-var-prinsippet (inkludert å bygge robusthet og motstandsdyktighet) og benytte konsensusorienterte strategier basert på dialog, deltagelse og involvering.[36] For situasjoner som preges av høy usikkerhet, bør det velges robuste strategier som fungerer godt over et bredt spektrum av mulige utfall.[37] Slike strategier inkluderer adaptiv risikostyring[38] og bruk av realistiske verstefallsscenarioer.

FFI anbefaler at kraftsektoren har en helhetlig tilnærming til risiko i hele konfliktspekteret, og at vitenskapelig risikotenkning[39] legges til grunn. NVE bør videreutvikle veiledere for risiko-vurderinger og styring av risiko i møtet med en ustabil omverden og dyp usikkerhet. NVE bør også bidra til at KBO-enheter får økt kunnskap om hvordan de kan utnytte scenarioanalyser for å styrke forsyningssikkerheten og kraftforsyningsberedskapen.

Helhetlig tilnærming til risiko betyr at KBO-enhetene må inkludere hele konfliktspekteret i risikoanalysene sine, inkludert krigsscenarioer. Dette finner FFI at de ikke i tilstrekkelig grad

[35] Sellevåg (2023).
[36] Aven et al. (2018).
[37] Lempert et al. (1996); Rosenhead et al. (1972).
[38] Adaptiv risikostyring innebærer at ulike beslutningsalternativer vurderes, et alternativ velges og observasjoner gjøres. Basert på analyse av observasjonene, oppnås læring som igjen gir grunnlag for å gjøre justeringer og tilpasninger (Klinke & Renn, 2012).
[39] Aven (2016); Aven (2017).

gjør i dag.[40] Kraftberedskapsforskriften § 2-3 setter som krav at KBO-enheter skal gjennomføre risikovurderinger knyttet til ekstraordinære forhold, men det er ikke eksplisitt spesifisert at scenarioer for militære anslag og angrep skal inkluderes, verken i kraftberedskapsforskriften eller veilederen til forskriften.

Det trengs planforutsetninger for kraftforsyningsberedskap i krig
Både FFI[41] og Totalberedskapskommisjonen[42] har pekt på behovet for planforutsetninger for sivil beredskap. Gjennom totalberedskapsmeldingen har regjeringen besluttet å vurdere dette nærmere.[43] FFIs scenariovurderinger av konsekvenser av krigshandlinger rettet mot kraftsystemet tilsier at planforutsetninger for KBO-enhetene er nødvendig.[44]

FFI anbefaler at Energidepartementet etablerer planforutsetninger for dimensjonering av kraftforsyningsberedskapen i krig. Planforutsetningene må gjøres kjent for Forsvaret og andre kritiske samfunnsfunksjoner slik at de kan legge forutsetningene til grunn for sin beredskapsplanlegging. FFI anbefaler at planforutsetningene utarbeides på bakgrunn av realistiske verstefallsscenarioer som er relevante for kraftforsyningen.

Det trengs bedre prosesser og metoder for vurdering av risiko
Kraftberedskapsforskriften med veileder spesifiserer ikke hvordan det skal skapes sammenhenger mellom risikovurderingene til de ulike KBO-enhetene. Dette gjør at viktige risikokilder kan bli utelatt. Manglende klassifisering av og sikringskrav til beredskapslagre er et eksempel på dette (se kapittel 8).[45] Videre kan det føre til mangelfull oversikt over risiko for kraftforsyningen som helhet, noe som igjen kan føre til at kilder til systemisk risiko[46] ikke avdekkes (strømbruddet på Den iberiske halvøy 28. april 2025 er et eksempel på dette; se boks 3.1). Det er også nødvendig å inkludere viktige leverandører og avhengigheter til andre kritiske samfunnsfunksjoner i risikovurderingene (se kapittel 5 og 8).

FFI anbefaler at NVE som beredskapsmyndighet og Statnett som systemansvarlig sammen videreutvikler prosesser og metoder som gir oversikt over risiko i kraftforsyningen som helhet. Som minimum er det behov for helhetlig oversikt over risiko til anlegg, systemer eller annet som omfattes av kraftberedskapsforskriften §§ 5-2 og 5-7. Slike prosesser bør inkludere vurderinger av systemisk risiko og hvordan de ulike risikoområdene påvirker hverandre, inkludert risiko forbundet med leverandørkjeder. Andre KBO-enheter bør inkluderes i dette arbeidet. Det bør også vurderes å inkludere viktige virksomheter i leverandørbransjen.

[40] Klepper og Lausund (2025).
[41] Sellevåg et al. (2022, s. 78).
[42] NOU 2023: 17 (s. 30).
[43] Meld. St. 9 (2024-2025) (s. 119).
[44] Høyere gradert FFI-rapport (under utarbeidelse).
[45] Klepper og Lausund (2025).
[46] Systemisk risiko kan føre til at enkelthendelser kan få store følgekonsekvenser for systemet som helhet, noe som igjen kan føre til systemkollaps (se Aven (2020) og International Risk Governance Council (2018) for nærmere beskrivelse).

Det trengs tillit til kraftforsyningen og motstandsdyktighet mot sammensatte trusler
I FFIs analyse av hvilke tilsiktede handlinger som kan true norsk kraftforsyning, ble det identifisert en rekke angrepsmål som en trusselaktør kan ramme for å oppnå målsettingene sine.[47] Gjennom fordekt bruk av ulike metoder og virkemidler rettet mot kraftsystemet, virksomheter i kraftsektoren, myndigheter eller befolkningen kan en fremmedstatlig trusselaktør forsøke å endre norsk energipolitikk, svekke norsk handlefrihet eller svekke tilliten i samfunnet. Trusler fra fremmedstatlige aktører kan derfor ramme bredere enn områdene som ivaretas gjennom kraftberedskapsforskriften. Videre indikerer forskning fra Sverige at høye strømpriser kan føre til økt oppslutning for høyreradikale partier som er mot det grønne skiftet.[48] Dette kan føre til økt politisk polarisering som fremmedstatlige trusselaktører kan utnytte.[49] Norske myndigheter, KBO-enheter og andre virksomheter som er av betydning for norsk kraftforsyning, må ta hensyn til dette.

FFI anbefaler at Energidepartementet sikrer at problemstillinger knyttet til sammensatte trusler og befolkningens tillit til kraftforsyningen inkluderes i utviklingen av norsk politikk for kraftforsyningen. Som et ledd i dette anbefaler FFI at Energidepartementet operasjonaliserer regjeringens strategi for å styrke motstandskraften mot desinformasjon[50] i egen sektor.

Det trengs sektorspesifikke trusselbilder for kraftforsyningen også fremover
KBO-enheter og andre virksomheter i kraftsektoren må være informert om hvilke trusler de kan stå overfor. Selv om Etterretningstjenesten, Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og KraftCERT utgir sine årlige trussel- og risikovurderinger, varierer det fortsatt hvor godt sentrale aktører i kraftsektoren er informert om mulige trusler.

Kraftutbygging er også store infrastrukturinvesteringer med lange tidshorisonter. Slike utbyggingsprosjekter krever tilgang på mer langsiktige trusselbilder. I 2024 tok NVE initiativ til å utarbeide et overordnet trusselbilde for kraftforsyningen som er ment å dekke den fulle bredden av trusler, uavhengig av den aktuelle situasjonen.[51] Dette er et godt initiativ som bør videreføres og videreutvikles.

FFI anbefaler at NVE viderefører arbeidet med å utvikle et overordnet trusselbilde for kraftforsyningen. Dette krever en kontinuerlig og langsiktig kunnskapsproduksjon om trusler som kan ramme norsk kraftforsyning, inkludert teknisk våpenutvikling knyttet til militære anslag.

KBO-enheter i viktige geografiske områder bør underlegges sikkerhetsloven
Utfordringer med deling av sikkerhetsgradert informasjon er velkjente.[52] En mer krevende sikkerhetspolitisk situasjon gjør at behovet for tilgang på sikkerhetsgradert informasjon har

[47] Sellevåg (2023, s. 32, 33).
[48] Brännlund og Peterson (2024).
[49] Buvarp og Sivertsen (2025).
[50] Kultur- og likestillingsdepartementet (2025).
[51] Rapporten ble utarbeidet av Thema Consulting Group og FFI på oppdrag for NVE (Norges vassdrags- og energidirektorat, 2025b).
[52] Endregard et al. (2019); Grunnan og Elstad (2018); NOU 2023: 17 (s. 117).

økt.[53] I 2025 vurderte PST det som sannsynlig at russisk etterretning vil forsøke å gjennomføre sabotasje mot mål i Norge.[54] For å redusere risikoen for sabotasje har NSM blant annet anbefalt å søke informasjon fra etterretnings- og sikkerhetstjenestene (EOS).[55] Behovet for sikkerhetsgradert informasjonsutveksling vil også øke ved sikkerhetspolitiske kriser og krig. Gitt kraftforsyningens betydning for nasjonale sikkerhetsinteresser vurderer FFI det som avgjørende at KBO-enhetene har nødvendig tilgang på sikkerhetsgradert trusselinformasjon. Det kan ikke legges som en forutsetning at etterretnings- og sikkerhetstjenestene kan nedgradere eller avgradere trusselinformasjon ved alvorlige sikkerhetspolitiske kriser eller krig.

Energidepartementet har utpekt nasjonal kraftforsyning som en grunnleggende nasjonal funksjon etter sikkerhetsloven.[56] I 2025 er det få KBO-enheter som er underlagt norsk sikkerhetslov. Dette betyr at det er få KBO-enheter som kan få tilgang til og håndtere sikkerhetsgradert informasjon. Enkelte informanter til FFIs oppdrag har vurdert at dagens krav gjennom kraftberedskapsforskriften er tilstrekkelige, og at det ikke fører til mer sikkerhet dersom en større del av kraftbransjen underlegges sikkerhetsloven. FFI mener at en slik vurdering ikke lenger er faglig forsvarlig.

For det første vil KBO-enhetene ha behov for tilgang på sikkerhetsgradert trusselinformasjon som nevnt ovenfor. I tillegg vil økt avhengighet mellom kraftforsyningen og elektroniske kommunikasjonstjenester føre til økt behov for sikker informasjonsutveksling mellom virksomheter i kraftsektoren og i ekomsektoren.[57] Alvorlige tilsiktede handlinger kan føre til svikt i kraftforsyningens transmisjonsnett.[58] I slike situasjoner hvor det er nødvendig å gå over til såkalt øydrift av kraftsystemet, blir rollen til distribusjonsnettoperatører og lokale kraftproduksjonsanlegg relativt sett viktigere. Dette gjelder særlig i geografiske områder som er av stor betydning for nasjonale sikkerhetsinteresser og forsvarsevne.[59]

FFI anbefaler til Energidepartementet at KBO-enheter i geografiske områder som er av stor betydning for nasjonale sikkerhetsinteresser og forsvarsevne, underlegges sikkerhetsloven. Hvilke KBO-enheter dette gjelder, må utledes fra behovet for forsyningssikkerhet i de gitte geografiske områdene.

[53] NOU 2023: 17 .
[54] Politiets sikkerhetstjeneste (2025, s. 12).
[55] Nasjonal sikkerhetsmyndighet (2025, s. 15).
[56] Nasjonal sikkerhetsmyndighet (u.å.).
[57] Ulshagen et al. (2023).
[58] Sellevåg (2023); Sellevåg og Ulshagen (2023).
[59] Høyere gradert FFI-rapport (under utarbeidelse).

Boks 3.1 – Strømbruddet på Den iberiske halvøy 28. april 2025

Den 28. april 2025 kl. 12:33 oppsto et fullstendig spenningsfall i kraftsystemet på Den iberiske halvøy. Dette førte til strømbrudd i store deler av Spania og Portugal. I tillegg ble deler av Frankrike berørt. Hendelsen er en av de mest alvorlige som har oppstått i det europeiske kraftsystemet i nyere tid hvis man ser bort fra angrepene mot Ukrainas kraftforsyning.

Den 17. juni 2025 presenterte spanske myndigheter (MITECO) hovedfunnene fra en spesialkomité som ble nedsatt for å finne årsaken og anbefale tiltak.[A] Etterforskningen viste at strømbruddet skyldtes en kombinasjon av tekniske og systemiske faktorer og ikke én enkelt feil. Hovedårsaken var en kjedereaksjon som ble utløst av overspenning, som igjen førte til at kraftverk koblet seg fra nettet. Dette forverret spenningsnivåene og førte til ytterligere frakoblinger.

Selve hendelsesforløpet ble delt inn i fem faser:

1. ustabil spenning i ukene og timene før hendelsen
2. systemiske svingninger i frekvens og spenning
3. tap av kraftproduksjon grunnet overspenning
4. full kollaps av spenning («blackout»)
5. gradvis gjenoppretting av kraftforsyningen (fullført 29. april kl. 14:36)

Den tekniske analysen avdekket flere faktorer som bidro til strømbruddet:

- *Utilstrekkelig spenningskontroll:* En kombinasjon av for få kraftverk med spenningsregulering i drift, manglende eller feil respons fra kraftverkene da spenningen steg, begrensede muligheter til å justere spenningen gradvis fra systemoperatørens side (REE) og at mange store forbrukere og distribusjonsselskaper ikke fulgte kravene til såkalt reaktiv effekt, bidro til ustabilitet da spenningen begynte å avvike fra det nominelle nivået.

- *Kraftige svingninger i systemet:* To store svingninger (kl. 12:03 og kl. 12:19) ble registrert i systemet før det kollapset. Den første var en svingning i frekvens på 0,6 Hz som trolig oppsto i Sør-Spania, og som ble forsterket av en solcellepark som viste svingende produksjon i takt med frekvensoscillasjonen. Den andre store svingningen var en kjent «øst-senter-vest»-svingning i det europeiske nettet som fikk ekstra stor amplitude i Spania på grunn av svake mellomlandsforbindelser og lite roterende masse i systemet («piskesnert-effekt»). De to svingningene bidro til å destabilisere nettet.

- *Feil og svakheter i kontrollsystemer:* Rapporten peker på flere feil og svakheter i kontrollsystemene. Viktige funn var manglende eller feilaktig regulering av reaktiv effekt (synkrone kraftverk leverte ikke reaktiv effekt som forventet), feiljusterte eller for følsomme spenningsvern (flere sol- og vindparker koblet seg ut ved spenninger som var innenfor tillatte grenser), langsom eller manglende respons i transformatorer (manuell eller treg automatisk regulering), utilstrekkelig synlighet og kontroll over distribuerte anlegg (systemoperatøren hadde begrenset oversikt over hva som skjedde i distribusjonsnettet), og manglende logging og segmentering i digitale systemer.

- *Svake mellomlandsforbindelser:* Den iberiske halvøy har svake mellomlandsforbindelser til resten av det europeiske kraftsystemet. Dette førte til at svingningen kl. 12:19 ble forsterket i Spania. I tillegg forsinket det gjenopprettingen etter kollapsen.

- *Markedsmekanismer og negative priser:* Midt på dagen da kollapsen skjedde, var det overproduksjon av fornybar energi (sol og vind). Høy produksjon, lav etterspørsel og begrenset eksportkapasitet (svake mellomlandsforbindelser) førte til negative priser ned mot −10 €/MWh i det intradaglige markedet. De negative strømprisene førte til at flere solcelleanlegg reduserte eller stanset produksjonen, som igjen førte til brå endringer i spenning og reaktiv effekt. Dette bidro til ustabilitet i nettet.

Hovedårsakene til strømbruddet var altså for lav kontroll over spenningen, kraftige svingninger i frekvens og kraftverk som koblet seg ut for tidlig. Det har blitt spekulert i at det var den høye andelen av fornybar, uregulerbar kraftproduksjon som forårsaket kollapsen. Spesialkomitéens undersøkelser viste at dette ikke var rotårsaken, men på grunn av blant annet mangelfulle kontrollsystemer og manglende etterlevelse av krav, bidro den høye fornybarproduksjonen til å gjøre kraftsystemet mer sårbart.

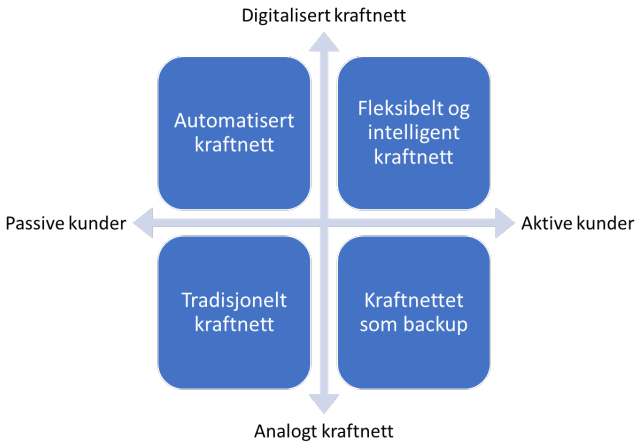
På bakgrunn av funnene foreslo spesialkomitéen en rekke tiltak. Noen av dem var å forbedre driftskontroll, bruke såkalt nettdannende teknologi, forbedre koordineringen mellom systemansvarlig, nettansvarlig og produsenter, ta tak i utfordringer med negative strømpriser, forsterke mellomlandsforbindelser og styrke kraftforsyningsberedskapen gjennom trening og øving.

[A] Ministerio Para La Transición Ecológica Y El Reto Demográfico (2025)

4 Digitalisering og digital sikkerhet

Elektrifiseringen av Norge krever økt kraftproduksjon fra fornybare energikilder, om vi skal oppfylle klimaforpliktelsene våre. Imidlertid er det dyrt og tidkrevende å bygge ut kraftnettet for å håndtere høyere strømforbruk og økte effekttopper. Kapasiteten til det eksisterende kraftnettet kan derfor bli en flaskehals for videre elektrifisering av samfunnet. Med økt uregulerbar kraftproduksjon fra sol- og vindkraft, kraftproduksjon som flyttes nærmere forbrukerne, og økte effekttopper er det nødvendig å utnytte det eksisterende kraftnettet bedre gjennom digitalisering og automatisering, nye markedsplattformer og nye konstellasjoner[60] av kraftprodusenter. Dette skal skje samtidig som krav til forsyningssikkerhet opprettholdes.

Forenklet kan endringene i kraftnettet forstås langs en nettakse og en kundeakse (figur 4.1). Dagens kraftnett (karakterisert som «tradisjonelt kraftnett») driftes med betydelige sikkerhetsmarginer på grunn av begrensede muligheter for automatisert overvåking og styring.[61] Digitalisering kan som nevnt øke fleksibiliteten og utnyttelsen av eksisterende nett, men kan også øke kompleksiteten til kraftnettet og introdusere nye sårbarheter.[62]



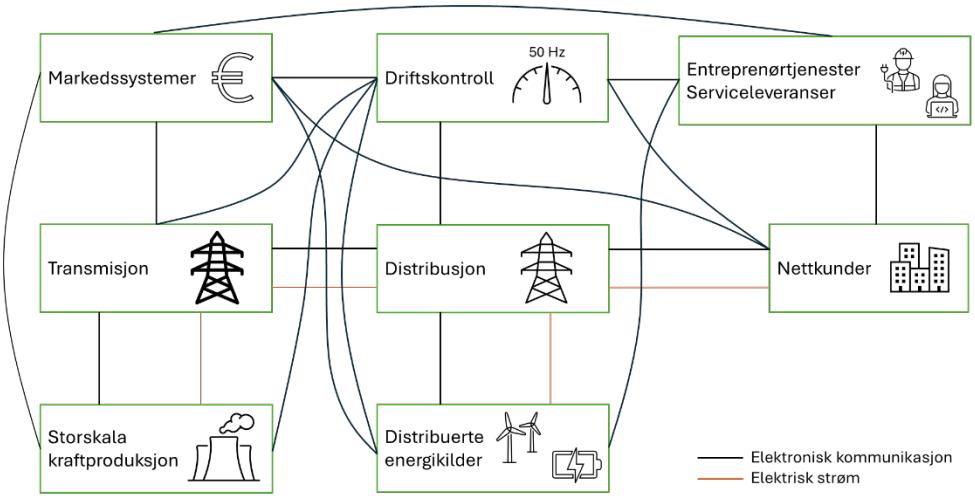
Figur 4.1 Utviklingsretninger for kraftnettet (basert på Holmstrøm og Gjerde (2024)).

Digitalisering vil føre til at kraftsystemets kontrollplan utvides. Kontrollplanet kan sees på som «intelligensen» i kraftsystemet. I tillegg til driftskontrollfunksjonen vil også Elhub[63], markedssystemer og smart styring av forbruk inngå. Dette sammen med økt avhengighet av elektronisk

[60] Produsenter av vind- og solkraft og bioenergi inngår av og til i et konsept som kalles *virtuelle kraftprodusenter*. Hensikten med dette er å samle små ressurser til større og mer forutsigbare enheter som kan tilby verdi for kraftforsyningen (Ulshagen et al., 2025, s. 16).
[61] Energi21 (2022, s. 43).
[62] Ulshagen et al. (2025).
[63] Elhub er den norske kraftbransjens IT-system for distribusjon av måleverdier og behandling av markedsprosesser (https://elhub.no/om-elhub).

kommunikasjon vil føre til økt kompleksitet i kraftsystemet (forenklet illustrert i figur 4.2 ved bruk av det europeiske smartgrid-konseptet som eksempel).

FFI har i en egen rapport sett nærmere på hvilke sårbarheter digitalisering av kraftsystemet kan føre med seg.[64] Områdene som er studert, er smart styring av strømforbruk, sensorsystemer for økt driftskontroll og overvåking, automatisering og beslutningsstøtte, nye markedsplattformer og nye konstellasjoner av kraftprodusenter. Se Ulshagen et al. (2025) for en mer detaljert diskusjon rundt mulige sårbarheter innenfor de nevnte områdene.



Figur 4.2 Forenklet illustrasjon av det europeiske smartgrid-konseptet og hvordan digitalisering fører til økt kompleksitet gjennom utvidet kontrollplan og økt avhengighet av elektronisk kommunikasjon.[65]

4.1 Konsekvenser av digitalisering

FFI har pekt på tre områder som kraftsektoren bør ha oppmerksomhet på når det gjelder digitalisering.[66]

Økt digital angrepsflate
For det første vil digitalisering av kraftsystemet øke den digitale angrepsflaten fordi hvert system som innføres, og kommunikasjonen mellom disse systemene, representerer et mulig angrepspunkt.[67] Økt bruk av tingenes internett (IoT) og industrielle tings internett (IIoT) i

[64] Ulshagen et al. (2025).
[65] Sand (2014).
[66] Ulshagen et al. (2025).
[67] Ulshagen et al. (2025).

kraftforsyningen,[68] i tillegg til tettere koblinger mellom IT-systemer og operasjonell teknologi (OT-systemer), fører til nye cybersikkerhetsutfordringer.[69] Blant annet har en doktorgrads-avhandling ved Universitetet i Oslo funnet at det fremdeles finnes utfordringer med å forbedre evnen til å detektere cybertrusler i kraftsystemer.[70] Utfordringene er knyttet til manglende automatisering i logganalyse, usikkerhet om hvilke data som er relevante, mangel på realistiske evalueringsmiljøer for deteksjonssystemer, mangel på ressurser, begrenset kompetanse og inkonsistente regulatoriske krav.

FFI har tidligere påpekt svakheter med håndteringen av alvorlige IKT-sikkerhetshendelser som kan få tverrsektorielle konsekvenser, [71] og NVE har selv pekt på svakheter i IKT-sikkerhetstilstanden i kraftforsyningen.[72] Siden trusselbildet i det digitale rom er svært dynamisk, må evnen til å detektere og håndtere hendelser stadig videreutvikles.

FFI anbefaler at NVE sammen med KraftCERT og NSM videreutvikler evnen til å detektere og håndtere IKT-sikkerhetshendelser i kraftsektoren. Dette bør inkludere å videreutvikle planverk, trening og øving (se kapittel 9). FFI anbefaler at NVE og KraftCERT holder seg oppdatert på forskningsfronten innen defensive cyberoperasjoner og vurderer hvordan utviklingen innen defensive cyberoperasjoner kan nyttiggjøres innen kraftsektoren.

FFI anbefaler at NVE ser nærmere på ordninger for å validere og sertifisere maskinvare som brukes i kraftforsyningen. NVE bør også vurdere om det skal stilles krav til at leverandører av programvare til kraftforsyningen må dokumentere hvilke programvarebiblioteker som blir benyttet. Dette kan gjøre det enklere å agere på sårbarhetsvarslinger.[73]

Økt kompleksitet i kraftsystemet

For det andre vil digitalisering føre til økt kompleksitet i kraftsystemet. Dette kan gi utslag på flere måter. Digitalisering vil føre til økt avhengighet av offentlige elektroniske kommunikasjonstjenester og globale navigasjonssatellittsystemer for tidsstempling av sanntidsdata. Svikt i elektronisk kommunikasjon kan føre til lignende utfordringer for kraftforsyningen som det som ble observert under uværet i Innlandet i 2021.[74] Høyere grad av sammenkobling mellom IT- og OT-systemer vil gi et mer fleksibelt og intelligent kraftnett,[75] men samtidig kan det gi en hel rekke utfordringer, som beskrevet av Netsecurity på oppdrag for NVE.[76]

[68] Røyksund og Valdal (2020); Ulshagen et al. (2025).
[69] Garimella (2018); Storm (2024).
[70] Storm (2024).
[71] Sellevåg et al. (2022, s. 63–66).
[72] Kvadsheim et al. (2023).
[73] Ulshagen et al. (2025).
[74] Lunde og Lunde (2022).
[75] Norges vassdrags- og energidirektorat (2024a).
[76] Norges vassdrags- og energidirektorat (2024a).

Digitalisering vil også føre til høyere endringstakt og større organisatorisk kompleksitet gjennom lengre og mer uoversiktlige leverandørkjeder. Risikoen for å bli rammet av digitale leverandørkjedeangrep kan derfor øke samtidig som nasjonal kontroll utfordres (se kapittel 5).[77]

FFI anbefaler at KBO-enhetene tar en proaktiv tilnærming til digital sikkerhet for å realisere gevinstene som digitalisering av kraftsystemet kan gi. FFI anbefaler at NVE sammen med KraftCERT skaper arenaer for erfaringslæring og deling av mønsterpraksis.

Økt sårbarhet for økonomisk virkemiddelbruk
For det tredje kan digitalisering føre til at sårbarheten for økonomisk virkemiddelbruk øker. FFI har i en tidligere rapport sett på hvordan utviklingen innen kunstig intelligens, 5G, skytjenester og IoT påvirker staters muligheter til å drive såkalt økonomisk statshåndverk.[78] Dette er teknologier som er viktige for digitaliseringen av kraftforsyningen. Fremmedstatlige aktører som er dominerende innenfor disse teknologiområdene, kan utnytte sin posisjon til å akkumulere og utøve makt gjennom økonomisk statshåndverk.

Gjennom «Global Energy Interconnection»-iniativet (GEI) som ble lansert i 2015, viser Kina at de har globale ambisjoner innen fornybar energi.[79] Avhengig av hvordan GEI utvikler seg, kan dette gi lignende sikkerhetsutfordringer som man har sett for det kinesiske Belte-vei-initiativet.[80] Vi omtaler problematikk knyttet til nasjonal kontroll over leverandørkjeder nærmere i kapittel 5.

Kravene i kraftberedskapsforskriften til sikkerhet i digitale informasjonssystemer ble sist oppdatert i 2019, og NVE har utarbeidet en veileder for risikovurdering av IT og OT.[81] NVE har også strammet inn reglene for kraftsensitiv informasjon. NVE har derfor tatt grep for å legge til rette for en mer enhetlig tilnærming til digital sikkerhet i kraftsektoren. Dette arbeidet bør videreføres og videreutvikles.

FFI anbefaler at Statnett utvikler en helhetlig handlingsplan for forsvarlig digitalisering av kraftnettet, med utgangspunkt i Statnetts «Strategisk plan teknologi»[82] og slik at gevinster realiseres og krav til forsyningssikkerhet og digital sikkerhet opprettholdes. En slik handlingsplan bør utvikles i samarbeid med nettselskapene. Se rådet om helhetlig tilnærming til risiko i kapittel 3.

4.2 Lovverk og praksis for digital sikkerhet i kraftforsyningen

Digital sikkerhet i kraftforsyningen vil også berøres av lov om digital sikkerhet (digitalsikkerhetsloven). Digitalsikkerhetsloven ble vedtatt av Stortinget 12. desember 2023, og den trådte i kraft 1. oktober 2025 gjennom digitalsikkerhetsforskriften. Loven er en gjennomføring av NIS-

[77] Ulshagen et al. (2025).
[78] Waage og Lindgren (2022).
[79] Wang et al. (2018).
[80] Quimbre et al. (2023).
[81] Norges vassdrags- og energidirektorat (2024b).
[82] Statnett (2025b).

direktivet i norsk rett og vil blant annet gjelde for KBO-enheter og virksomheter som ved enkeltvedtak helt eller delvis er underlagt kraftberedskapsforskriften § 1-3 andre ledd. Det er med andre ord noe overlapp mellom digitalsikkerhetsforskriften og kraftberedskapsforskriften. Det er imidlertid godt kjent at NIS-direktivet har en rekke svakheter som rettes opp gjennom NIS2-direktivet. Sett i forhold til NIS-direktivet har NIS2-direktivet blant annet et utvidet omfang, strengere sikkerhetskrav og rapporteringsplikter, en mer enhetlig tilnærming til cybersikkerhet og økt vektlegging av tilsyn.[83] Samtidig er det usikkert om EUs arbeid med digital sikkerhet i NIS- og NIS2-direktivene har hatt tilstrekkelig oppmerksomhet på sikkerhet i OT.[84]

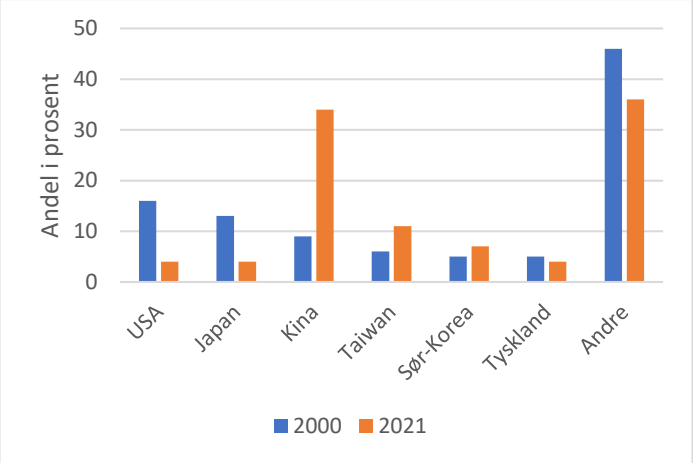
FFI anbefaler at kraftberedskapsforskriftens krav til digital sikkerhet som minimum tilfredsstiller kravene som stilles gjennom NIS2-direktivet. Videre anbefaler FFI at NIS2-krav gjøres gjeldende for områder som ikke dekkes av kraftberedskapsforskriften. FFI anbefaler at dette gjøres som en del av regjeringens lovarbeid knyttet til implementering av NIS2 i norsk rett.[85] FFI anbefaler at NVE utreder nærmere om NIS2-direktivet i tilstrekkelig grad tilfredsstiller krav til sikkerhet i OT.

[83] Per oktober 2025 pågår det et lovarbeid i regjeringen som ser på implementering av NIS2-direktivet i norsk rett (Regjeringen, 2023).
[84] Toftegaard (2024).
[85] Regjeringen (2023).

5 Sikkerhet i anskaffelser og leverandørkjeder

– Ikke noe land har satt seg i en bedre posisjon enn Kina til å bli en supermakt innen fornybar energi (International Renewable Energy Agency, 2019, s. 40)

Krigen i Ukraina og stormaktsrivalisering mellom USA og Kina har trukket oppmerksomheten mot styrket reparasjonsberedskap, økt lagerbeholdning av kritiske komponenter og utfordringer med lengre leveringstider for kritiske komponenter. Imidlertid dominerer Kina produksjonen av svært mange kritiske råmaterialer og elektroniske komponenter (figur 5.1).



Figur 5.1 Endringen i andel av eksport av elektronikk fra år 2000 til 2021 for utvalgte land. Kilde: Lu (2023).

Kina har globale ambisjoner innen fornybarenergiområdet. Det såkalte «Global Energy Interconnection» (GEI), som ble lansert av State Grid Corporation of China (SGCC) i 2015, er et kinesisk initiativ som har som ambisjon å utvikle et globalt strømnett som kan akselerere det grønne skiftet gjennom å utnytte kraftlinjer med ultrahøyspenning (UHV) og smarte teknologier.[86] Selv om initiativet kan føre til reduserte klimagassutslipp og økt kraftforsyningssikkerhet, kan det også gi sikkerhetsutfordringer ved at initiativet kan legge til rette for Beijings strategiske interesser. Hvorvidt Kina vil lykkes med sine ambisjoner, er usikkert, men GEI gjør det mulig for Kina å utvide sin globale rekkevidde gjennom å sikre langsiktig tilgang til kritiske energikorridorer, eksport av tekniske standarder for overføring av ultrahøyspenningskraft og integrasjon av kinesiske selskaper i kraftforsyningen til partnerland. I tillegg vil Kinas narrativer innen grønn utvikling bidra til å styrke Kinas myke makt.[87]

Selv om det er usikkert om Kina vil lykkes med sine ambisjoner, og selv om det er lite trolig at Norge blir direkte koblet til GEI, kan Kinas ambisjoner og posisjon innen fornybarenergiområdet likevel ha sikkerhetsimplikasjoner for Norge. Ettersom Kina dominerer ressurser som er avgjørende for den grønne omstillingen, kan Norge få økt avhengighet til Kina for å sikre utvikling, vedlikehold og modernisering av kraftinfrastrukturen og fornybar energiteknologi.

[86] Loen og Gusdal (2025).
[87] Loen og Gusdal (2025).

Denne avhengigheten kan forsterke Kinas mulighet til å utøve påvirkning og tvang gjennom eksklusjon eller gjennom informasjonskontroll.[88]

Langsiktige sikkerhetsvurderinger bør prioriteres i anskaffelser
FFI erfarer at kraftbransjen har varierende grad av modenhet når det gjelder sikkerhetsstrategier og protokoller for å ha kontroll på produksjonsland for utstyr og komponenter i utstyr.[89] Vurderinger rundt produksjonsland henger i større grad sammen med risikofaktorer knyttet til bærekraftkriterier, inkludert menneskerettigheter og arbeidsforhold. Med tanke på sikkerhet velges det en mer praktisk og tillitsbasert tilnærming der man benytter noen få leverandører fra godkjente land og har tillit til at disse vil opprettholde kontroll og kvalitet for å oppnå langvarige samarbeidsforhold. For fysiske komponenter følger man i tillegg opp med fabrikkbesøk og ulike tester eller godkjenninger underveis i produksjonsprosessen. Dette er dog vanskeligere med elektroniske komponenter og IT-systemer.

Fra intervjuer med aktører i kraftbransjen erfarer FFI at likeverdighetsprinsipper og regelverk for offentlige anskaffelser bidrar til at kinesiske leverandører må inkluderes i anskaffelsesprosessene.[90] Gitt Kinas dominans innen fornybarenergiområdet er det svært vanskelig å holde kinesiske leverandører utenfor, og på en del områder er det nærmest umulig. Dette gjør at Norge kan få økt sårbarhet overfor sikkerhetsutfordringene som trekkes frem av Loen og Gusdal (2025).

FFI anbefaler at selskapene i kraftsektoren legger vekt på og prioriterer langsiktige sikkerhetsvurderinger når de skal tildele oppdrag. Sikkerhet i anskaffelser og leverandørkjeder bør inkluderes i selskapenes strategier, på lik linje med strategier for eksempelvis bærekraft. FFI anbefaler at NVE i samarbeid med NSM videreutvikler veiledere for sikkerhet i anskaffelser og leverandørkjeder for kraftsektoren.

FFI anbefaler at Energidepartementet i samarbeid med Nærings- og fiskeridepartementet ser nærmere på mulighetene for å etablere produksjon av kritiske komponenter for kraftforsyningen både i Norge og gjennom nordisk samarbeid. Betydningen av geopolitiske forhold for forsyningssikkerheten kan dermed reduseres.

Kravene for anskaffelser bør skjerpes
I kraftberedskapsforskriften stilles det krav til at KBO-enhetene skal følge opp sine leverandører. Imidlertid knyttes ikke dette direkte opp mot sikkerhetsmyndighetenes trussel- og risikovurderinger, og det gis dermed heller ikke spesifiseringer. Det geografiske kravet i kraftberedskapsforskriften (§ 7-14 k) gjelder kun driftskontrollsystemer i anlegg av klasse 2 og 3. Klasse 1-anlegg er derfor utelatt. Det fremtidige kraftsystemet vil ha større andel av sol- og vindkraft i energimiksen, men de er i 2025 ikke omfattet av kraftberedskapsforskriften § 7-14 k. I tillegg vil et digitalisert kraftsystem føre til økt bruk av sensorikk som i mange tilfeller vil ha

[88] Loen og Gusdal (2025)
[89] Klepper og Gakkestad (2025).
[90] Klepper og Gakkestad (2025).

kinesiskproduserte komponenter (se kapittel 4). Klasse 1-anlegg kan også få en viktig betydning i alvorlige kriser og krig fordi det kan bli nødvendig å operere kraftsystemet i øydrift.[91] Det bør derfor vurderes om de geografiske kravene i kraftberedskapsforskriften § 7-14 k bør utvides til å gjelde for alle anleggsklassene.

Det er også nødvendig å stille spørsmål om hvorvidt man skal skille mellom utstyr som brukes i administrative IT-nett, kontra systemer og komponenter som brukes i OT. Hva som må ligge til rette for at skadevare kan spre seg fra et administrativt IT-system og over til et OT-system, kan være vanskelig å vurdere. Imidlertid kan skadevare spres fra IT-systemet til OT-systemet dersom det kun er en brannmur mellom de to systemene, og dersom brannmuren har vært utsatt for tukling.[92] Tukling i en datamaskin eller en brannmur kan være svært vanskelig å oppdage. Det er også slik at ikke all maskinvare behøver å være tuklet med; noe kan være helt i orden, mens andre deler kan være kompromitterte. Det gjør arbeidet med å finne ut om et utstyr er kompromittert eller ikke, er ekstra vanskelig. Dette er en av hovedgrunnene til at vi anbefaler å følge et føre-var-prinsipp med tanke på innkjøp av elektronikk til bruk i kraftsystemet.

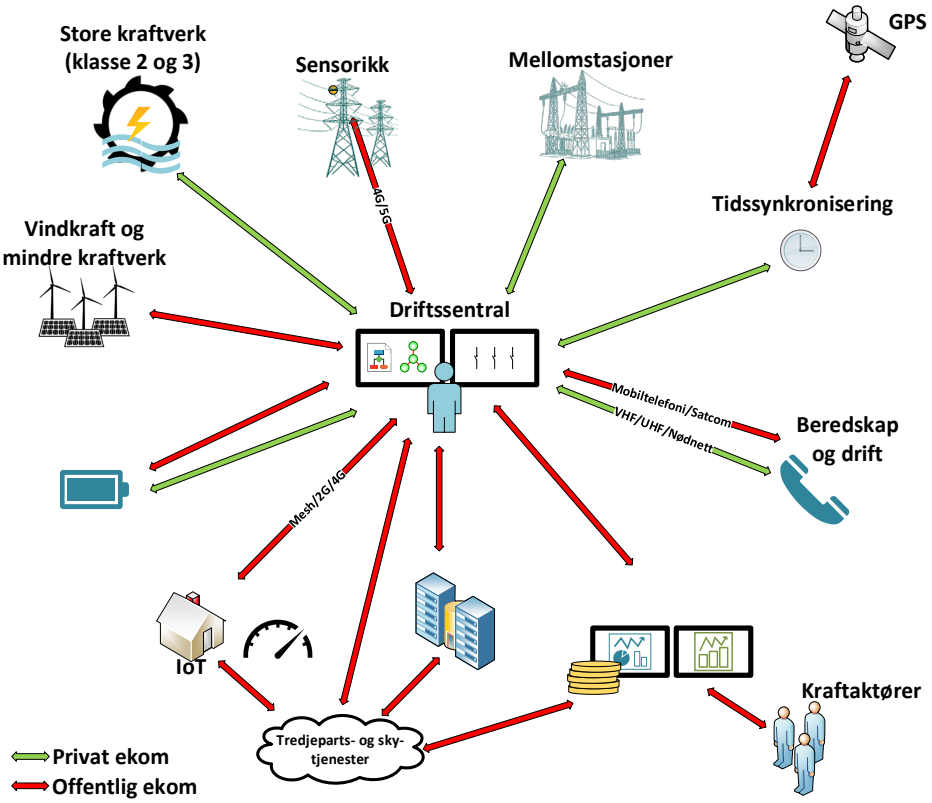
FFI anbefaler at NVE skjerper regelverket for anskaffelser av utstyr til klassifiserte anlegg i alle tre klassene. Dette kan gjøres ved at kraftberedskapsforskriften § 7-14 k gjøres gjeldende for et større omfang av driftskontrollsystemer enn dagens krav. FFI anbefaler at dette også gjøres gjeldende for anskaffelser av utstyr til IT-nett som benyttes i slike anlegg.

[91] Høyere gradert FFI-rapport (under utarbeidelse).
[92] Tukling med elektronikk eller programvare fører til brudd i integritetsegenskaper. Tukling i for eksempel et kretskort eller en krets betyr i denne sammenhengen at en trusselaktør endrer egenskapene til enheten slik at den enten ikke virker, virker med redusert ytelse, lekker informasjon eller stopper å virke på kommando eller et gitt tidspunkt.

6 Krav til driftsradio og samband i driftskontrollsystemer

Figur 6.1 viser en forenklet skisse over bruken av elektronisk kommunikasjon (ekom) i kraftforsyningen. Sentralt i systemet er driftssentralene som ved hjelp av ekom regulerer produksjon og distribusjon av kraft. I tillegg er mobile radionett (driftsradioen) viktig for daglig drift og ikke minst i en beredskapssituasjon. Med økende digitalisering vil kraftsystemets avhengighet av ekom øke (se kapittel 4).[93]

Kraftberedskapsforskriften setter krav til ekom i driftskontrollsystemer og til driftsradioen. For driftskontrollsystemer i klasse 2 og 3 er det satt som krav at ekom skal fungere uavhengig av funksjonssvikt i offentlige ekomtjenester (§ 7-14). Driftsradioen skal kunne fungere uavhengig av funksjonssvikt i offentlig ekomtjenester og ha reservestrøm med minimum 48 timer selvstendig driftstid (§ 7-17).



Figur 6.1 Forenklet illustrasjon over bruken av elektronisk kommunikasjon til driftskontroll og samband for beredskap og drift (driftsradio) i kraftforsyningen. [94]

[93] Pham et al. (2024).
[94] Pham (2025).

Kravene til elektronisk kommunikasjon for driftskontrollfunksjonen bør opprettholdes
Kravene til ekom og driftsradio i kraftberedskapsforskriften har gjort at KBO-enheter over tid har bygd ut og benyttet privat eller dedikert ekominfrastruktur for å etterleve kravene. Å etablere dedikert infrastruktur medfører store investeringskostnader og behov for personell og kompetanse for å drifte ekomnettet. Samtidig har norske myndigheter gjennomført store tiltak for å styrke robustheten til offentlige ekomtjenester.[95] Dersom kraftsektorens egen ekominfrastruktur kan erstattes med offentlig ekom, vil dette spare samfunnet for betydelige kostnader.

Transportnettet til offentlige ekomtjenester er det eneste mulige alternativet for driftskontrollfunksjonen. FFIs kartlegging viser imidlertid at selv om transportnettet er godt utbygd mange steder i landet, er det fremdeles variasjoner, og robustheten er svakere i mindre tettbygde områder og regioner.[96] Både Lyse Tele og GlobalConnect har riktignok landsdekkende fibernett, men Telenors infrastruktur er i en særstilling. I 2025 har andre ekomtilbydere fremdeles store avhengigheter til Telenor. Telenors transportnett er robust og godt sikret,[97] men alvorlig svikt i Telenors transportnett kan likevel ikke utelukkes (se også boks 6.1).[98]

Boks 6.1 – Cyberangrepet mot Kyivstar i 2023[A]

Den 12. desember 2023 ble Kyivstar, Ukrainas største teleoperatør, utsatt for et av de mest alvorlige cyberangrepene i landets historie. Over 24 millioner brukere mistet tilgang til mobil- og internettjenester, og luftvernsirener i mer enn 75 tettsteder rundt Kyiv ble satt ut av spill. Bank- og betalingssystemer ble også rammet.

Ifølge Ukrainas sikkerhetstjeneste (SBU) sto «Sandworm» bak angrepet. Dette er en gruppe som er tilknyttet den russiske etterretningsorganisasjonen GRU. Etterforskningen viste at angriperne hadde infiltrert Kyivstars systemer allerede i november 2023, og muligens så tidlig som i mai samme år. Fordi gruppen fikk full tilgang til selskapets nettverk, ble det mulig å forberede et svært målrettet og ødeleggende angrep. Selve angrepet ble gjennomført ved at angriperne slettet data og ødela kjernenettet, noe som førte til at omtrent 40 % av Kyivstars infrastruktur ble deaktivert. Kyivstar ble tvunget til å stenge ned hele nettverket for å hindre ytterligere skade.

[A] NTT Security (2024).

[95] Nasjonal kommunikasjonsmyndighet (2022).
[96] Pham (2025).
[97] Kiran et al. (2023).
[98] Direktoratet for samfunnssikkerhet og beredskap (2019, s. 204).

Basert på kartleggingen mener FFI at ingen offentlige ekomnett i tilstrekkelig grad oppfyller kravene til dekning, redundans og robusthet som er nødvendig for å ivareta driftskontroll-funksjonen.[99] Bruk av offentlige ekomnett kan likevel bidra til styrket robusthet og redundans.

FFI anbefaler at kraftberedskapsforskriftens krav om at ekom til driftskontrollfunksjonen skal fungere uavhengig av funksjonssvikt i offentlige ekomtjenester (§ 7-14), opprettholdes. NVE bør utrede kost-nytteeffekten ved at offentlige ekomnett benyttes for å styrke robustheten og redundansen til ekom for driftskontrollfunksjonen

Kravene til driftsradio bør opprettholdes, og satkom bør vurderes
Når det gjelder driftsradio, har FFI vurdert nødnett, mobilnett og satellittbasert kommunikasjon (satkom). Dagens nødnett er relativt godt utbygd med god redundans og robusthet, men reserve-strømkapasiteten tilfredsstiller ikke kravet i kraftberedskapsforskriften. Mobilnettet har ikke tilstrekkelig reservestrømkapasitet, og det vil være svært kostbart å oppgradere mobilnettets basestasjoner til å oppfylle kravet til reservestrøm. I tillegg kan dekningsgraden til mobilnettet være utilstrekkelig i områder hvor det ikke bor folk, men som er viktige for kraftforsyningen. Satkom er uavhengig av lokal kraftforsyning, men mangler innendørsdekning, har krav til frisikt og tilstrekkelig åpningsvinkel, krever større brukerterminaler for bredbåndstjenester og har noe høyere kostnader. Dette gjør det usikkert om satkom er egnet som driftsradio. Imidlertid kan satkom være en svært nyttig reservesambandsløsning.[100]

FFI anbefaler at kraftberedskapsforskriftens krav om at driftsradio skal fungere uavhengig av funksjonssvikt i offentlige ekomtjenester (§ 7-17), opprettholdes. NVE bør utrede kost-nytte-effekten ved å benytte satellittbasert kommunikasjon som reserveløsning for driftsradio.

Kravene til reservestrøm for driftsradioen bør skjerpes
Kraftberedskapsforskriften setter i dag krav til 48 timers reservestrøm for driftsradioen. I en ekstraordinær situasjon hvor det ikke er mulig å fjernstyre kraftsystemet, er driftsradioen avgjørende for å kunne opprettholde fortsatt drift på en sikker og trygg måte. Den fremtidige sikkerhetspolitiske utviklingen peker i retning av fortsatt stormaktsrivalisering, ustabilitet og usikkerhet. I tillegg forventes mer ekstremvær som følge av klimaendringer. Hyppigheten og alvorlighetsgraden til driftsforstyrrelser kan derfor øke. Kravene til reservestrøm bør derfor skjerpes i geografiske områder som er viktige for nasjonale sikkerhetsinteresser og forsvarsevne, og i områder som er særlig utsatt for ekstremvær og hvor de samfunnssikkerhets-messige konsekvensene kan bli store.

FFI anbefaler at NVE får skjerpet kravet til reservestrøm for driftsradioen til 72 timer i områder som er viktige for nasjonale sikkerhetsinteresser og forsvarsevne, og i områder som er særlig utsatt for ekstremvær, og hvor de samfunnssikkerhetsmessige konsekvensene kan bli store. NVE bør utrede hvilke områder dette gjelder.

[99] Pham (2025).
[100] Pham (2025).

7 Sikring mot luftleverte våpen

Erfaringer fra Ukraina viser at omfattende militære angrep mot kraftforsyningen kan få svært alvorlige følger for et lands motstandsdyktighet og forsvarsevne (se boks 7.1). Generelt sett er det fem hovedtyper av situasjoner som kan gi konsekvenser for kraftforsyningen i krig:

- tap av anlegg som følge av okkupasjon eller krigsutflytting (altså at kraft- eller nettselskapet ikke lenger kan operere anlegget)
- angrep med luftleverte langtrekkende våpen (missiler, droner, flybomber og langtrekkende artilleri)
- angrep som gir skadelig elektromagnetisk puls (EMP) (for eksempel fra kjernefysisk detonasjon)
- fysisk sabotasje utført av spesialstyrker eller stedfortredere («proxyaktører»)
- utilsiktede skader og ødeleggelser som følge av kamphandlinger nær kraftinstallasjoner

I tillegg kommer destruktive cyberangrep, men slike angrep vil først og fremst føre til drifts-forstyrrelser snarere enn store ødeleggelser sammenlignet med skader fra luftleverte langt-rekkende våpen, angrep med elektromagnetisk puls eller fysiske sabotasjeaksjoner.

Hvilke konsekvenser militære anslag kan få for kraftforsyningen, vil være avhengig av flere faktorer. Viktige faktorer er kraftsystemets oppbygging og redundans, fysisk sikring av kritiske anlegg, kraftforsyningens reparasjonsberedskap og militære styrkers evne til å beskytte kraftforsyningen eller nøytralisere trusselen.

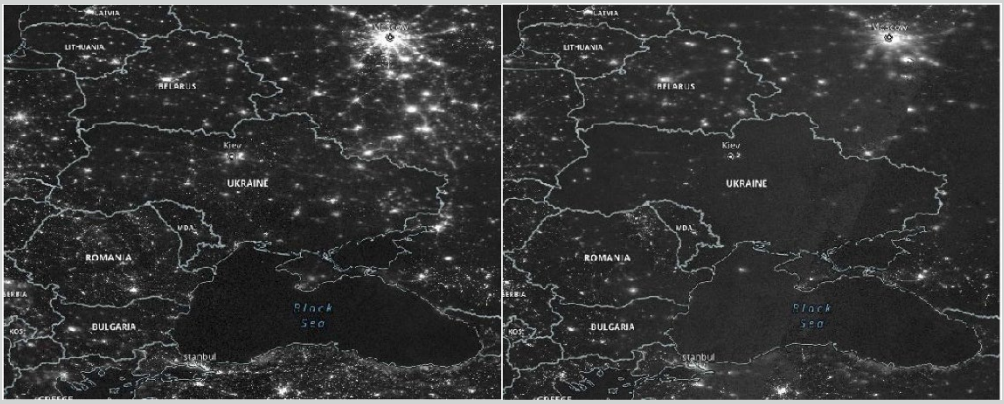
Det norske kraftsystemet kjennetegnes av god distribusjon av produksjonskapasitet. Mange kraftstasjoner er konstruert og testet for å kunne starte fra spenningsløs stasjon (såkalt svart-start). Dette gjør lokal strømforsyning («øydrift») mulig hvis tilknytningen til transmisjonsnettet skulle svikte. I tillegg har Norge et stort antall vannkraftverk med turbiner plassert i fjell, noe som gjør dem beskyttet mot avstandsleverte militære våpen. Gjennom damsikkerhetsforskriften er det også satt krav til at vassdragsanlegg i konsekvensklasse 3 og 4 skal «dimensjoneres og kontrolleres for laster fra tilsiktede aksjoner i fred, under beredskap og i krig» (§ 5-3). Vind- og solkraft bidrar også til desentralisert kraftproduksjon. I Norge er det derfor først og fremst kraftnettet, altså transmisjonen og distribusjonen av strøm, som kan være sårbart for fysisk sabotasje eller militære anslag.

I *Forsvarsanalysen 2024* advarte FFI om at hele kraftnettet i Norge kan angripes med missiler og droner fra russisk territorium, og at slike angrep kan utføres med svært kort varslingstid.[101] Russland kan derfor ramme kraftnettet i en tidlig fase av et væpnet angrep. Dette kan skape store og langvarige konsekvenser for en rekke andre kritiske samfunnsfunksjoner, inkludert Forsvaret, hvis angrepene lykkes.[102,103]

[101] Skjelland et al. (2024, s. 44).
[102] Sellevåg og Ulshagen (2023).
[103] Høyere gradert FFI-rapport (under utarbeidelse).

Boks 7.1 – Russiske militære angrep mot kraftforsyningen i Ukraina

Erfaringer fra Ukraina viser at Russland angriper kraftforsyningen på en målrettet og metodisk måte med luftleverte og langtrekkende våpen. Dette er gjort for å påvirke Ukrainas motstandskraft og forsvarsevne. I november 2022 var nattehimmelen over nær sagt hele Ukraina nesten like mørk som over Svartehavet som følge av Russlands angrep (Figur 7.1).



Figur 7.1 Satellittfoto fra NASA som viser nattehimmelen over Ukraina før (venstre) og etter (høyre: november 2022) Russlands fullskala invasjon i 2022. Kilde: https://worldview.earthdata.nasa.gov/.

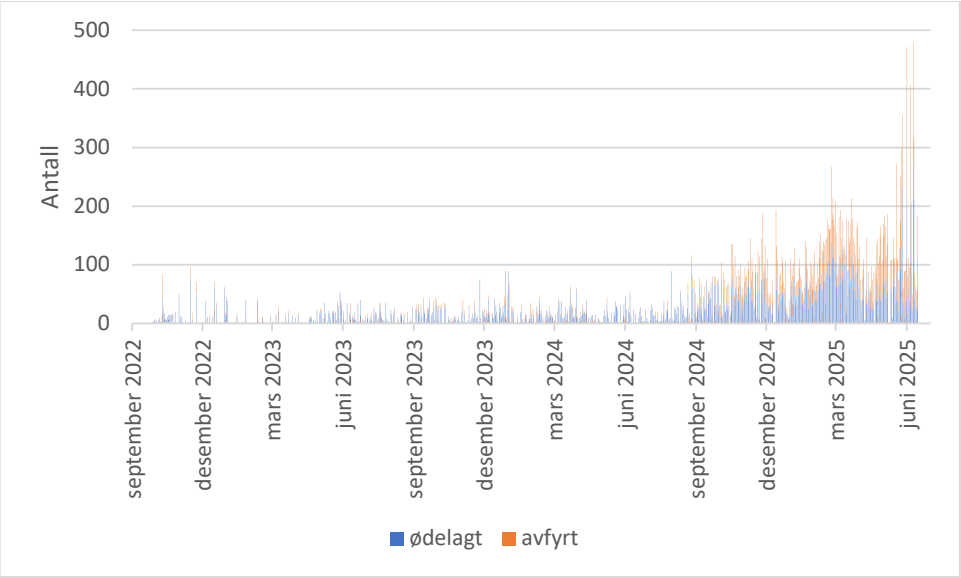
Tidslinje over situasjonen for ukrainsk kraftforsyning (2022–2024):[A]

- Før fullskalainvasjonen var ukrainsk kraftproduksjonskapasitet 44 GW, mens forbruket på vinterstid var 26 GW.
- I oktober 2022 startet Russland målrettede angrep mot Ukrainas kraftforsyning. Fra oktober 2022 til februar 2023 gjennomførte Russland minst 13 angrepsbølger med kryssermissiler og ballistiske missiler i 19 av 24 regioner av Ukraina, inkludert Kyiv.
- I april 2023 hadde Ukraina mistet nesten halvparten av produksjonskapasiteten sin som følge av okkupasjon og missilangrep.
- Vinteren 2023/2024 kunne Ukraina bare produsere rundt 17,8 GW, mens kraftforbruket var opp mot 18,5 GW. Kraftunderskuddet ble dekket opp av import.
- 26. august 2024 gjennomførte Russland et av sine største luftangrep med mer enn 100 missiler og 100 droner. Angrepene var hovedsakelig rettet mot kraftforsyningen og annen infrastruktur.

[A] UN Human Rights Monitoring Mission in Ukraine (2024).

Russland utsetter Ukraina for massive missil- og droneangrep. Figur 7.2 viser at angrepene har økt i intensitet i løpet av krigens gang. Angrepene er også rettet mot ukrainsk kraftforsyning, hvor kritiske anlegg for kraftoverføring, eksempelvis transformatorstasjoner, utsettes for målrettede angrep med missiler og droner.[104] Russland endrer også taktikk når det er nødvendig for å oppnå målsettingene om å ødelegge Ukrainas kraftforsyning.[105] Selv om Ukraina har fått mye luftvern som vestlig støtte, har Russland likevel fortsatt angrepene mot kraftsystemet. Det internasjonale energibyrået (IEA) har derfor blant annet anbefalt at reparasjon og gjenoppbygging av Ukrainas kraftsystem må gjøres slik at det er bedre fysisk sikret mot nye militære angrep.[106]

Russland vil ha en langvarig evne til brutal adferd.[107] Det er derfor nødvendig å avskrekke Russland fra både et lynangrep og en langvarig krig.[108] For å bidra til å styrke den nasjonale motstandsdyktigheten i en væpnet konflikt er det behov for å forsterke sikringen av kraftnettet.[109,110]



Figur 7.2 Antall russiske missiler og droner som det ukrainske forsvaret har rapportert offentlig at er avfyrt mot Ukraina. Kilde: Ivaniuk (2025) (tilgjengeliggjort under en CC BY-NC-SA 4.0-lisens)

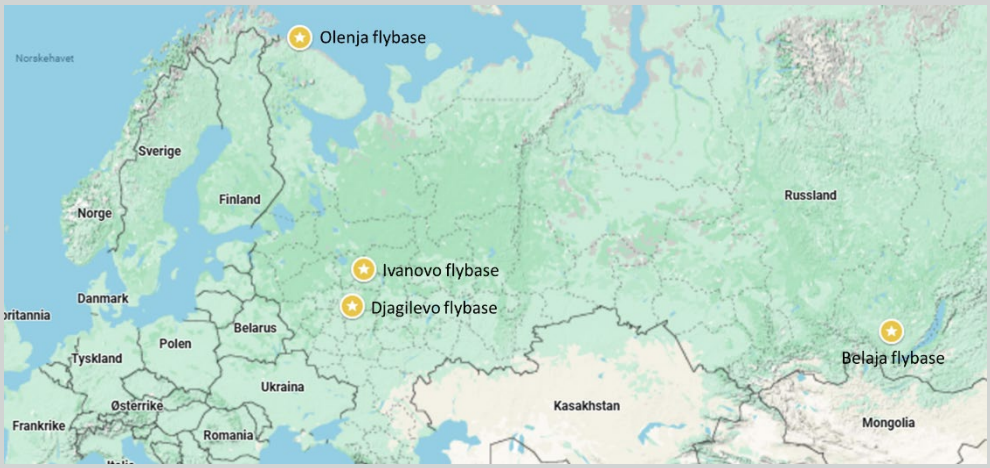
[104] Brunbaum et al. (2022); Cobham og Butler (2024); Lister et al. (2022); Sabonis-Helf (2025).
[105] Edwards et al. (2024).
[106] International Energy Agency (2024, s. 8).
[107] Skjelland et al. (2025, s. 17–21).
[108] Diesen et al. (2024).
[109] Lausund og Dullum (2025).
[110] Høyere gradert FFI-rapport (under utarbeidelse).

Boks 7.2 – Operasjon Spider's Web[A]

Den 1. juni 2025 gjennomførte Ukraina en spektakulær droneoperasjon mot Russland. Rundt 150 små og presise FPV-droner[A] ble skjult i containere som ble fraktet på lastebiler og smuglet inn i Russland. Opplysninger tilsier at angrepet gjorde at Ukraina kunne ramme over 40 fly fordelt på fire ulike flybaser dypt inne på russisk territorium (Figur 7.3).[B] Flytypene som ble rammet, var blant annet de strategiske bombeflyene Tupolev Tu-95MS, Tupolev Tu-22M3 og Tupolev Tu-160, og dessuten overvåkingsflyet Beriev A-50. Angrepet mot en femte flybase var ikke vellykket.

Ukraina benyttet det russiske mobilnettet til å fjernstyre FPV-dronene etter at de var ført inn i Russland. Dette gjorde det mulig å kommunisere over lange avstander uten satellittkommunikasjon eller spesialiserte militære nettverk. Videre førte det til lavere risiko for oppdagelse siden signalene inngikk i den vanlige mobiltrafikken. Resultatet var at Ukraina kunne fjernstyre dronene i sanntid selv når de var tusenvis av kilometer fra Ukraina.

Operasjonen viste hvordan billig teknologi, utnyttelse av kunstig intelligens og god planlegging kan få strategiske effekter.



Figur 7.3 Russiske flybaser som ble angrepet av Ukraina i operasjon Spider's Web (kart fra Google Maps)

[A] FPV er en forkortelse for «*first person view*», eller «førstepersonsperspektiv», som betyr at droneoperatøren kan se gjennom kameraer på dronen ved hjelp av videobriller når hen styrer den.
[B] Bondar (2025).

Viktige kraftanlegg bør sikres mot angrep

Å sikre det norske kraftnettet mot militære angrep må sees i sammenheng med Forsvarets operative evne. FFIs forsvarsanalyse for 2025 viste at Forsvaret vil ha vesentlige gap i 2028.[111] Dette er knyttet til lagdelt luftvern, anti-ubåtoperasjoner og langtrekkende ild. Forsvaret har også for lav beredskap til å håndtere militære anslag med korte varslingstider. Mot 2036 dekkes de fleste gapene, men med lagdelt luftvern som viktigste unntak. Foreløpige analyser tyder også blant annet på at Forsvaret har mangler innen elektromagnetisk krigføring.

Videre er Forsvarets operative evne først og fremst dimensjonert ut fra militære behov og oppgaver. I faktiske situasjoner må Forsvaret gjøre en operativ vurdering av hvordan de militære kapasitetene skal benyttes. Dette gjelder også hvilke områder og objekter som skal beskyttes mot lufttrusler.[112] Samtidighetsutfordringen for Forsvaret vil trolig være størst i en nasjonal eller nordisk fase av en væpnet konflikt inntil allierte utenfor Norden kommer. Det kan derfor ikke forutsettes at Forsvaret vil ha tilstrekkelig kapasitet til å forsvare kraftsystemet mot luftleverte våpen. Dermed er det nødvendig å se på hvilke tiltak kraftsektoren selv kan ta.

Basert på erfaringer fra Ukraina og en analyse av den våpentekniske utviklingen har FFI vurdert mulige tiltak for forsterket sikring av klassifiserte anlegg i kraftnettet mot luftleverte våpen.[113] Mot kryssermissiler som er konstruert for å trenge gjennom vegger av betong, vil fjellanlegg med tilstrekkelig overhøyde være nødvendig for å gi fysisk sikring. Eksempelvis vil et treff med et kryssermissil mot en åpen transformatorsjakt fullstendig ødelegge det som befinner seg i sjakten. Tilgrensende sjakter kan også bli skadet, men ikke nødvendigvis totalskadd. Ødeleggelse av store transformatorer kan få omfattende og langvarige konsekvenser. Samtidig er dette utstyr som det kan ta lang tid å erstatte hvis man ikke har tilstrekkelige beredskapslagre (se kapittel 8). For å opprettholde forsyningssikkerhet til særlig kritiske samfunnsfunksjoner eller industri, kan det være nødvendig å sikre klassifiserte kraftanlegg i fjellanlegg. Hvilke kraftanlegg dette kan gjelde, må komme frem av en risiko- eller scenarioanalyse (se rådet om helhetlig tilnærming til risiko i kapittel 3). Slike vurderinger må inkluderes i konsesjonsbehandlingen av klassifiserte kraftanlegg.

FFI anbefaler at NVE sørger for at regjeringens strategiske hovedprioriteringer[114] i nasjonal sikkerhetsstrategi inkluderes i konsesjonsbehandlingen av klassifiserte kraftanlegg. NVE bør se nærmere på om dette fører til behov for å tydeliggjøre eller endre gjeldende regelverk.

Detonasjon av små[115] sprengladninger kan være tilstrekkelig for å forårsake skade og brann på en transformator ved direktetreff. Hendelsen på Sunndalsøra[116] i 2016 og hendelsen på

[111] Skjelland et al. (2025).
[112] Diesen (2025).
[113] (Lausund & Dullum, 2025).
[114] De strategiske hovedprioriteringene i den nasjonale sikkerhetsstrategien er: (1) raskt styrke forsvarsevnen, (2) gjøre samfunnet mer motstandsdyktig og (3) styrke vår økonomiske sikkerhet (Statsministerens kontor, 2025).
[115] Hva som vurderes som en mindre sprengladning i denne sammenhengen, er informasjon som er unntatt offentlighet i tråd med offentleglova § 21. Detaljer er gitt i Lausund og Dullum (2025).
[116] Heggstad (2016); Korsnes (2016).

Heathrow[117] lufthavn i 2025 er eksempler på hvilke konsekvenser som kan oppstå ved brann i transformatorstasjoner. FFI har identifisert tiltak som kan sikre eksisterende transformatorstasjoner mot små luftleverte sprengladninger på en kostnadseffektiv måte,[118] men dette må utredes nærmere.

FFI anbefaler at Energidepartementet innfører et forbud mot uautorisert bruk av droner over kraftanleggene som NVE vurderer som mest kritiske.

FFI anbefaler anlegg som NVE vurderer som mest kritiske etablerer fysisk sikring mot små luftleverte sprengladninger. FFI anbefaler at Forsvarsbygg får i oppdrag å utrede fysisk sikringsløsning mot små luftleverte sprengladninger for eksisterende anlegg.

FFI anbefaler at nye anlegg, eller utskiftning av eksisterende anlegg, som NVE vurderer som mest kritiske, og som vil ha lang teknisk levetid, sikres i fjellanlegg. Dette tiltaket bør sees i sammenheng med behov for å sikre kritiske anlegg mot naturfarer som ras og jordskred.

FFI anbefaler at NVE i samråd med relevante sektorer holder politiet og Forsvaret løpende oppdatert om hvilke anlegg som vurderes som mest kritiske for kraftforsyningen, og hvor svikt kan gi store konsekvenser for samfunnssikkerheten eller nasjonale sikkerhetsinteresser, slik at politiet og Forsvaret kan gjøre nødvendige objektsikringstiltak. FFI anbefaler at NVE følger opp politiet og Forsvaret med tanke på status for objektsikringstiltakene.

FFI anbefaler at det for anlegg som vurderes som mest kritiske og som ikke kan sikres i fjellanlegg, forberedes tiltak for rask gjenoppretting av kraftforsyningen dersom slike anlegg utsettes for sabotasje eller krigshandlinger.[119]

[117] Schwebs et al. (2025).
[118] Lausund og Dullum (2025).
[119] For kritisk viktige transformatorstasjoner kan slike tiltak inkludere forberedte løsninger for forbikobling («omlooping») av transformatorstasjonen.

8 Reparasjonsberedskap

Kraftberedskapsforskriften stiller krav til reparasjonsberedskap. I henhold til forskriftens § 4-1, skal reparasjonsberedskapen «dimensjoneres etter stedlige forhold og anleggenes tilstand og klasse. Så langt som det er samfunnsmessig rasjonelt, skal hensynet til liv og helse og annen samfunnskritisk virksomhet prioriteres ved gjenoppretting av funksjon». Likevel opplever vi at det mangler kriterier for kravoppnåelse. Dette skaper uklarheter knyttet til hvorvidt man i realiteten har tilstrekkelig reparasjonsevne. Dette gjelder særlig for alvorlige tilsiktede handlinger og krig. Vi har observert flere kritiske mangler som tilsier at reparasjonsevnen ikke oppfyller kravene i kraftberedskapsforskriften.[120]

Leveringstiden for kritiske komponenter har de siste årene økt betydelig og ført til at det er kritisk risiko knyttet til viktig materiell. Bransjen er i stor grad avhengig av komponenter som leveres av leverandørselskaper utenfor norsk kontroll. Samtidig er kraftbransjen helt avhengig av leverandørbransjen når det gjelder reparasjonsevne og eventuelle produksjonsfasiliteter for kritiske komponenter. Det er få leverandører som gjennomfører reparasjonstjenester, noe som kan føre til kapasitetsmangel ved større kriser og krig. Vi ser også utfordringer knyttet til leverandørbransjen, særlig i den øvre delen av konfliktspekteret, fordi den norske delen av selskapene er helt avhengig av samarbeid med utenlandske deler av selskapene.

Det er behov for flere beredskapslagre, og det bør stilles krav til klassifisering og sikring
Kraftberedskapsforskriften stiller ikke krav til klassifisering av beredskapslagre. Dermed stilles det heller ikke særskilte krav til sikring av slike lagre. Sikring av lagre er kun basert på KBO-enhetenes egen vurdering. Dette fører til en sårbarhet ettersom viktige beredskapslagre med lavt sikringsnivå vil kunne være lette sabotasjemål for å redusere reparasjonsberedskap og gjenoppretningsevne i sikkerhetspolitiske kriser og krig. Geografisk tilgjengelighet til lagrene vil i en krise- eller krigssituasjon være av stor betydning for reparasjonsevnen og utholdenheten. På tross av at det finnes gode planer for transport av tunge komponenter, har FFI fått opplyst at det likevel kan oppstå problemer som følge av mangelfullt vedlikehold eller uannonserte endringer av transportinfrastrukturen. I krisesituasjoner eller krig kan dette få konsekvenser for samfunnssikkerheten eller totalforsvarsevnen.

FFI anbefaler at KBO-enhetene etablerer større og flere regionalt spredte beredskapslagre for å øke reparasjonsevnen og utholdenheten i en krise- eller krigssituasjon. Slike beredskapslagre må også inkludere elektroniske komponenter som er kritisk viktige for forsyningssikkerheten.

FFI anbefaler at NVE utvider kraftberedskapsforskriften til å sette krav til klassifisering og sikring av beredskapslagre.

[120] Klepper og Lausund (2025).

FFI anbefaler at Energidepartementet og Samferdselsdepartementet tar initiativ til en gjennomgang av transportplanleggingen for å avdekke om endringer i transportinfrastrukturen kan ha betydning for kraftforsyningsberedskapen.

KBO-enhetenes tilgang til drifts- og reparasjonskompetanse bør sikres

KBO-enhetene har prioriteringsavtaler med leverandører som skal sørge for at de prioriteres ved behov for assistanse med reparasjon. Dette fungerer så lenge det er snakk om enkelthendelser og andre kriser ikke legger beslag på personell hos leverandørene. Imidlertid vil flere samtidige hendelser utfordre kapasiteten til leverandørene. Dette gjør at KBO-enhetenes prioriteringsavtaler kan bli vanskelig å opprettholde i alvorlige kriser og krig.[121] I tillegg kan det medføre utfordringer dersom kritisk personell for drift og gjenoppretting av kraftforsyningen innkalles til militær- eller sivilforsvarstjeneste i krise eller krig.

Personell med lokalkunnskap og kunnskap om manuell drift nærmer seg pensjonsalder. Dette kan være avgjørende for gjenopprettingsevnen i en krise og kan forverre situasjonen og konsekvensene ved et strømutfall. I tillegg utdannes det for få personer med nødvendig spesialkompetanse. Dette kan føre til en sårbarhet for fremtidig kraftforsyningsberedskap.

FFI anbefaler at KBO-enhetene går gjennom leverandøravtalene sine for å sikre tilstrekkelig reparasjonsevne i hele konfliktspekteret.

FFI anbefaler at KBO-enhetene øker sin egen reparasjonsevne med tanke på materiell og tilgjengelig personell og kompetanse for å redusere avhengigheten av eksterne leverandører. Dette inkluderer å legge vekt på systematisk kunnskapsoverføring om gamle systemer og manuell drift og gjennomføre målrettede øvelser (se også kapittel 9).

FFI anbefaler at NVE går i dialog med Forsvaret og med Sivilforsvaret når det gjelder fritaksordninger fra militær- eller sivilforsvarstjeneste og fritak for forhåndsrekvirering av transportmidler for å sikre at KBO-enhetene har tilstrekkelig personell og materiell for drift og gjenoppretting av kraftforsyningen i krise og krig.

FFI anbefaler at Kunnskapsdepartementet sammen med Energidepartementet vurderer hvordan fagutdanninger innen elkraft kan styrkes for å øke rekrutteringen til kraftsektoren.

[121] Klepper og Lausund (2025).

9 Samarbeid, trening og øving

Organisering og ledelse av kraftforsyningens beredskapsorganisasjon (KBO) er godt regulert gjennom energiloven og kraftberedskapsforskriften med tilhørende veileder. Imidlertid er operasjonaliseringen av regelverket mangelfullt på noen områder. Dette bør følges opp gjennom planprosesser og tilsyn.

Planverket bør gjennomgås, og det bør øves mer

Energidepartementet kan i særskilte nasjonale kriser og krig legge hele kraftforsyningen inn under KBO. Kraftberedskapsforskriften § 3-3 sier at kraftforsyningens sentrale ledelse (KSL) overtar ledelsen av KBO i slike situasjoner. Videre sier § 3-3: «Statnett SF skal i slike situasjoner være KSLs utøvende organ for regulering av produksjon, omforming, overføring, omsetning og fordeling av elektrisk energi». KSL består av NVE som beredskapsmyndighet, og med deltagelse fra Statnett. Flere respondenter gir uttrykk for at KSL er lite aktivt, og at det er behov for en styrket operasjonalisering av KSL.[122] Det stilles også spørsmål ved om planverket som ligger til grunn for denne funksjonen, er tilstrekkelig og vil fungere.

Det er et behov for styrket trening og øving av KBO. Dette gjelder særlig håndtering av sikkerhetspolitiske kriser og krig (se også boks 9.1). Det er avgjørende at det gjennomføres jevnlige, konkrete og tverrsektorielle øvelser. Slike øvelser må inkludere hele kraftsystemet, også leverandører av kritiske tjenester, sektorer som er kritisk avhengige av kraftforsyning, og aktører som har viktige sikringsoppgaver (dette gjelder særlig politiet og Forsvaret). Det bør også gjennomføres regelmessig stresstesting av systemene for å avdekke mulige ekstreme utfall.

FFI anbefaler at Energidepartementet og NVE går gjennom planverket som ligger til grunn for KBO, og sørger for at KBO-enhetene, kraftforsyningens distriktssjefer (KDS) og KSL regelmessig trener og øver. Det er behov for både sektorspesifikke og tverrsektorielle øvelser.

FFI anbefaler at NVE styrker oppfølgingen og kontrollen med etterlevelse av kraftberedskapsforskriften § 2-7. FFI anbefaler at NVE videreutvikler veilederne sine for planlegging og gjennomføring av øvelser til også å inkludere øvelser på sammensatte trusler og krigsscenarioer.

Kritiske leverandører bør inngå i kraftforsyningens beredskapsorganisasjon

Kraftforsyningen er svært avhengig av noen få leverandører for å oppgradere, vedlikeholde og reparere særdeles viktig utstyr, inkludert store transformatorer. Ingen av disse selskapene er, så langt FFI har brakt på det rene, en del av KBO. Flere respondenter peker på at en utvidelse av KBO til også å inkludere særdeles viktige selskaper i leverandørbransjen vil kunne styrke sektorens beredskap generelt og reparasjonsberedskap spesielt.[123]

[122] Klepper og Lausund (2025).
[123] Klepper og Lausund (2025).

Flere sentrale beredskapsoppgaver håndteres av en leverandørbransje som ikke er en del av KBO, og som ikke er definert som samfunnskritisk. Dette kan føre til forsinkelser med tanke på reparasjoner i en krise- eller krigssituasjon.

FFI anbefaler at kraftforsyningens beredskapsorganisasjon utvides til å inkludere særlig viktige bedrifter i leverandørbransjen. I tillegg bør personell med særlig kompetanse i andre leverandørbedrifter defineres som samfunnskritisk personell.

Kraftsektorene i de nordiske landene bør samarbeide tettere

Beredskapssamarbeid mellom systemoperatørene i Norden fungerer godt på et overordnet nivå, og det er utveksling av informasjon om hendelser og av materiell i en krisesituasjon. Dette gjelder særlig mellom Norge og Sverige. Likevel pekes det på at det vil være behov for et mer inngående samarbeid når det gjelder reparasjonsberedskap og beredskapslagre – ikke bare i Norden, men også på europeisk nivå.[124] Så langt FFI kjenner til, er det heller ikke etablert felles beredskapsordninger mellom de nordiske landene for personell med kritisk kompetanse. Ulik lovgivning i de nordiske landene fører til utfordringer når det gjelder både utveksling av informasjon og muligheter for å utveksle personell. Dette har ført til at selskapene først og fremst har et nasjonalt fokus for å løse eventuelle kompetanse- og personellutfordringer og henter eventuelt inn kompetanse fra leverandørselskaper på lengre kontrakter.

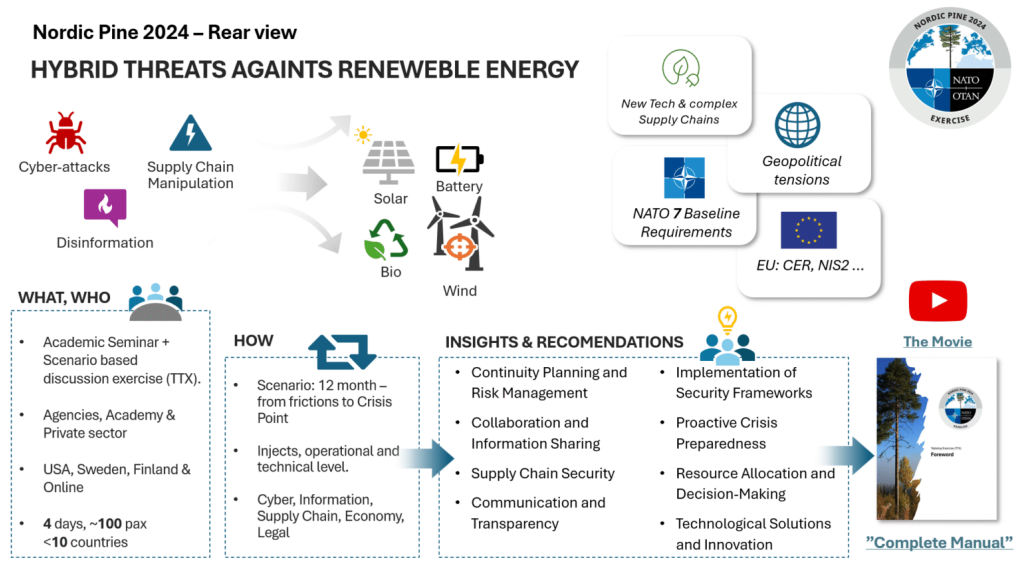
FFI anbefaler at norske KBO-enheter videreutvikler sikkerhets- og beredskapssamarbeidet med nordiske kraft- og nettselskaper. Kraftsektorene i de nordiske landene bør øve mer på å håndtere hendelser som går på tvers av landegrenser. Slike øvelser bør inkludere tverrsektorielle aspekter og utveksling av informasjon, materiell og personell i krise- og krigsscenarioer.

[124] Klepper og Lausund (2025).

Boks 9.1 – NATO-øvelsen «Nordic Pine»[A]

NATO-øvelsen «Nordic Pine» ble arrangert av den svenske Totalförsvars-stiftelsen og NATO Science & Technology Organization (STO) i 2024 og 2025. Øvelsen har som formål å styrke motstandsdyktigheten til fornybare energi-systemer mot sammensatte trusler, inkludert cyberangrep, påvirknings-operasjoner og utnyttelse av verdikjeder som våpen.

Øvelsen ble avholdt i Sverige og Finland. I 2025 deltok det aktører fra Sverige, Finland, USA, Tyskland, Danmark og Sveits.



[A] Informasjon om øvelsen: https://nordicpine.org.

10 Konklusjoner

Rimelig og sikker tilgang på fornybar elektrisk kraft har vært et konkurransefortrinn for Norge. Pålitelig kraftforsyning er derfor avgjørende for verdiskaping, befolkningens velferd og norsk sikkerhet.

Norge står i 2025 overfor en alvorlig sikkerhetspolitisk situasjon. Krigen i Ukraina, Russlands militære utvikling, stormaktsrivalisering mellom USA og Kina, Kinas dominans innen fornybar energi og behovet for en rask og omfattende energiomstilling for å møte klimautfordringene vil få avgjørende betydning for sikkerheten og beredskapen til Norges kraftforsyning i årene fremover.

FFI har på oppdrag for NVE og Statnett utredet hvordan forsyningssikkerhet og beredskap i kraftforsyningen kan styrkes. Basert på funnene og vurderingene våre har vi gitt følgende overordnede råd til hvordan forsyningssikkerheten og beredskapen i kraftforsyningen kan styrkes:

1. Kraftsektoren må ha en helhetlig tilnærming til risiko i hele konfliktspekteret. Dette inkluderer blant annet å bruke realistiske verstefallsscenarioer, utvikle planforutsetninger for dimensjonering av kraftforsyningsberedskapen i krig og at en større del av kraftsektoren underlegges sikkerhetsloven.

2. Kraftsektoren må ha en proaktiv tilnærming til digital sikkerhet for å realisere gevinstene som digitalisering av kraftsystemet kan gi. Dette inkluderer blant annet å utvikle en helhetlig handlingsplan for forsvarlig digitalisering av kraftsystemet slik at gevinster realiseres og krav til forsyningssikkerhet og digital sikkerhet opprettholdes.

3. Kraftsektoren må styrke sikkerheten i anskaffelser og leverandørkjeder. Dette inkluderer å vektlegge langsiktige sikkerhetsvurderinger, utvide kraftberedskapsforskriften § 7-14 k og utforske muligheter for nasjonal produksjon av kritiske komponenter til kraftforsyningen.

4. Dagens krav i kraftberedskapsforskriften til driftsradio og samband i driftskontrollsystemet (§§ 7-14 og 7-17) må videreføres. Samtidig bør kravet til reservestrøm for driftsradioen skjerpes til 72 timer i særskilt viktige eller utsatte geografiske områder.

5. Kraftsektoren må etablere sikringstiltak mot luftleverte våpen. Dette inkluderer blant annet fysiske sikringstiltak mot små luftleverte sprengladninger for eksisterende kritiske kraftanlegg. I tillegg bør anlegg som NVE vurderer som mest kritiske, og som har lang teknisk levetid, sikres i fjellanlegg.

6. Kraftsektoren må etablere en reparasjonsberedskap som er dimensjonert for krigsscenarioer. Dette inkluderer blant annet å etablere større og flere regionalt spredte beredskapslagre for å øke reparasjonsevnen og utholdenheten i en krise- eller

krigssituasjon, etablere beredskapslagre for elektroniske komponenter som er kritisk viktige for forsyningssikkerheten, etablere sikringskrav til beredskapslagre og styrke nasjonal egenevne og kompetanse.

7. Kraftforsyningens beredskapsorganisasjon (KBO) må trenes og øves, og det nordiske beredskapssamarbeidet innen kraftforsyning må styrkes. Dette inkluderer blant annet at KBO må ha oppdatert planverk, og at KBO-enhetene, kraftforsyningens distriktssjefer (KDS) og kraftforsyningens sentrale ledelse (KSL) regelmessig øver på å håndtere ekstraordinære situasjoner og krigsscenarioer. I tillegg bør KBO utvides til å inkludere særlig viktige bedrifter i leverandørbransjen.

Disse rådene er utdypet i 36 konkrete tiltak. Vi anbefaler at tiltakene inkluderes i kunnskaps-grunnlaget som Stortinget har bedt regjeringen om når det gjelder planer for styrket beredskap i kraftsystemet.[125]

Fortsatt kraftutbygging og styrking av forsyningssikkerheten og kraftforsyningsberedskapen vil føre til betydelige kostnader. For norske politikere og myndigheter blir det avgjørende å skape aksept for prioriteringene som må gjøres, og at gode løsninger identifiseres og iverksettes raskt. Forskning, utvikling og innovasjon bør tas i bruk for å sikre at Norge fortsatt har rikelig tilgang på rimelig, sikker og fornybar elektrisk kraft i en verden som preges av ustabilitet og usikkerhet.

[125] Innst. 242 S (2024-2025) .

Vedlegg

A Metodisk tilnærming

A.1 Forskningshypoteser og datagrunnlag

Følgende forskningshypoteser har ligget til grunn for arbeidet:[126]

- Digitalisering av kraftsystemet fører til endringer som påvirker forsyningssikkerheten. Dagens regelverk er ikke utformet for å håndtere endringene som følger av nye forretningsmodeller. Regelverket må moderniseres for å håndtere de større konsekvensene av digitaliseringen.

- Bedre koordinering av investeringer i infrastruktur mellom sektoren for elektronisk kommunikasjon («ekomsektoren») og kraftsektoren kan styrke kraftforsyningsberedskapen. Samarbeid og informasjonsdeling mellom ekomsektoren og kraftsektoren reduserer risikoen for utfall av ekom til driften av kraftforsyningen. Forberedte prosesser for prioritering av kraft og ekom kan redusere utilsiktede konsekvenser for driften av kraftsystemet og for samfunnet ved kraftmangel.

- Tilgangen på materiell og ressurser til reparasjonsberedskap har blitt redusert. Leveringstiden har økt på grunn av økt etterspørsel etter deler og råvarer og transportutfordringer globalt.

- Det er behov for å revurdere kraftforsyningsberedskapen nasjonalt for å bedre forsyningssikkerheten i Norge, som følge av krigen i Ukraina og Russlands konflikt med Vesten. Risikostyringsprosesser må styrkes for å oppnå bedre kraftforsyningsberedskap i KBO-enhetene.

Følgende datagrunnlag er lagt til grunn for vurderingene:

- rapporter og notater fra delutredningene
- FFI-rapporter knyttet til tilstøtende problemstillinger
- NVE og Statnett sine egne rapporter og analyser
- fagfellevurderte vitenskapelige publikasjoner og doktorgradsavhandlinger
- Norges offentlige utredninger
- stortingsmeldinger, innstillinger og proposisjoner

[126] Bestemt av oppdragsgiverne NVE og Statnett i dialog med FFI. Forskningshypotesene er utredet i egne delutredninger med tilhørende leveranser.

- nyhetsartikler fra redaktørstyrte medier
- annen offentlig informasjon

Snøballmetoden ble benyttet for litteratursøk (bruk av referanselister og siteringssøk). Kunstig intelligens (Microsoft Copilot) ble brukt til oversetting.

A.2 Vurdering av risiko

Forståelsen og beskrivelsen av risiko som er lagt til grunn for arbeidet, er basert på moderne risikoteori.[127] Her er risiko forstått som fremtidige konsekvenser av en hendelse og usikkerhet, hvor konsekvensene er relatert til dagens tilstand. Siden det er usikkert hva konsensene vil bli dersom hendelsen inntreffer, står vi overfor risiko.[128] Dette kan uttrykkes som

$$\text{Risiko} = \text{Konsekvenser (C)} + \text{Usikkerhet (U)} = (C, U), \qquad (A.1)$$

hvor konsekvensen er relatert til en gitt referanse (for eksempel dagens tilstand). Usikkerheten er knyttet til sannsynligheten for at hendelsen gir de spesifiserte konsekvensene, og styrken på kunnskapen som vurderingen bygger på. I tillegg tas det høyde for at det kan skje overraskelser i forhold til kunnskapen vi har i dag.

På grunn av usikkerhetene som er involvert når det gjelder å vurdere tilsiktede handlinger som kan true norsk kraftforsyning, har vi brukt en scenariobasert tilnærming. Vurderingene av sannsynligheten for at en tilsiktet handling gir bestemte konsekvenser, er derfor avgrenset til en vurdering av om det er plausibelt at scenarioet kan inntreffe (ikke-kvantifisert vurdering av sannsynlighet). Dette er beskrevet i en egen rapport.[129] Vurderingene av konsekvenser er relatert til i hvilken grad samfunnssikkerheten eller nasjonale sikkerhetsinteresser påvirkes negativt ved at trusselaktøren lykkes med målsettingene sine gjennom å ramme verdier relatert til norsk kraftforsyning. Dette er gjort gjennom sårbarhetsvurderinger som er utført i de ulike delutredningene.

Vurderingen av risiko i dette arbeidet er derfor knyttet til spørsmålet:

> *Dersom scenario X inntreffer, er sikkerhets- og beredskapsnivået i kraftforsyningen i 2025 tilstrekkelig, gitt forventet utvikling av kraftforsyningen frem mot 2036?*

På bakgrunn av en risikobasert vurdering av om dagens sikkerhet og beredskap er tilstrekkelig sett opp mot scenarioet, foreslår vi eventuelle risikoreduserende tiltak. Utvalgte tiltak har deretter blitt gjenstand for en effekt-kostnadsvurdering (vedlegg A.3) som gir prioriteringer av tiltakene.

[127] Aven (2016); Aven (2017).
[128] Pluss («+») leses som «og». Risiko uttrykkes altså som konsekvenser og usikkerhet.
[129] Sellevåg (2023).

A.3 Effekt-kostnadsvurdering

Metoden for å vurdere virkninger av anbefalingene har tatt utgangspunkt i Direktoratet for forvaltning og økonomistyring (DFØ) sin veileder i samfunnsøkonomiske analyser.[130] Metoden som FFI har benyttet, er basert på DFØs anbefalte metode for kvalitativ vurdering av ikke-prissatte virkninger (verdimatrisemetoden).[131]

I dette arbeidet er *virkningen* av tiltaket beskrevet som hvilken *ikke-prissatt effektvirkning* tiltaket har som risikoreduserende tiltak for kraftforsyningen. FFIs vurdering av effektvirkning er altså *ikke* en vurdering av samfunnsøkonomisk nytte. Følgende skala er benyttet for å vurdere effektvirkninger:

- meget stor positiv effekt
- stor positiv effekt
- middels positiv effekt
- liten eller ingen positiv effekt

Regler for vurdering av effektvirkninger er gitt i tabell A.1.

Tabell A.1 Regler for vurdering av effektvirkninger.

Effektvirkning	Regel
Meget stor positiv effekt	Tiltak som kan relateres direkte til forbedret sikkerhet og beredskap i kraftsystemet, og som har langvarig virkning
Stor positiv effekt	Tiltak som kan relateres direkte til forbedret sikkerhet og beredskap i kraftsystemet
Middels positiv effekt	Alle andre tiltak
Liten eller ingen positiv effekt	Ekskluderes og omtales ikke fordi de har utilfredsstillende virkning som risikoreduserende tiltak

Vurdering av kostnadsvirkninger er en kvalitativ og samlet vurdering av enhetsverdi, påvirkning på hver berørte og antall berørte (ikke-prissatt vurdering). Dette er fremstilt i figur A.1. For å vurdere kvantumet, er følgende skala benyttet:

- stort negativt kvantum
- middels negativt kvantum
- lite negativt kvantum

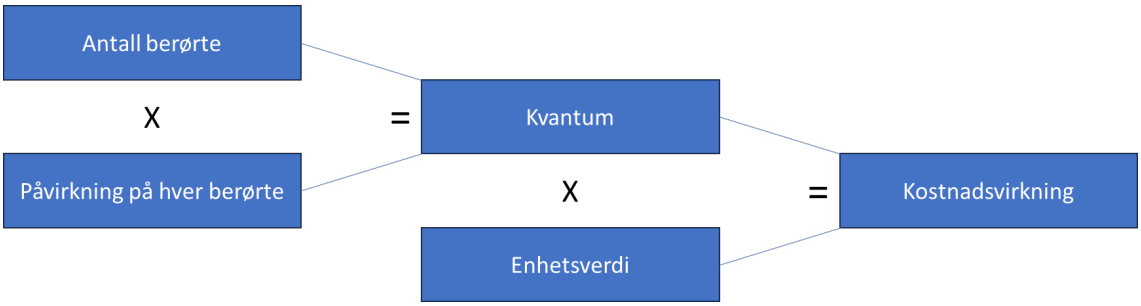
[130] Direktoratet for forvaltning og økonomistyring (u.å.).
[131] Direktoratet for forvaltning og økonomistyring (u.å., kap. 3.4.5).

- verken negativt eller positivt kvantum

Enhetsverdien er vurdert på følgende skala:

- liten enhetsverdi
- middels enhetsverdi
- høy enhetsverdi
- svært høy enhetsverdi

Verdimatrisen for kvalitativ vurdering av kostnadsvirkninger er gitt i tabell A.2. Regler for vurdering av kvantum og enhetsverdi er gitt i henholdsvis tabell A.3 og tabell A.4. Positive kostnadsvirkninger er ikke vurdert.



Figur A.1 Kvalitativ metode for vurdering av kostnadsvirkninger.

Tabell A.2 Verdimatrise for kvalitativ vurdering av kostnadsvirkninger.

Enhetsverdi / Kvantum	Liten	Middels	Høy	Svært høy
Stort negativt	Middels negativ	Stor negativ	Meget stor negativ	Svært stor negativ
Middels negativt	Liten negativ	Middels negativ	Stor negativ	Meget stor negativ
Lite negativt	Ubetydelig/ ingen	Liten negativ	Middels negativ	Stor negativ
Verken negativt eller positivt	Ubetydelig/ ingen	Ubetydelig/ ingen	Ubetydelig/ ingen	Ubetydelig/ ingen

Tabell A.3 Regler for vurdering av kvantum

Kvantum	Regel
Stort negativt	Tiltak som berører store deler av kraftsektoren eller hele kraftsystemet
Middels negativt	Tiltak som berører en delmengde av KBO-enhetene eller deler av kraftsystemet
Lite negativt	Tiltak som berører et fåtall aktører eller KBO-enheter, en liten del av kraftsystemet eller få kraftanlegg, eller som påvirker hver enkelt KBO-enhet i liten grad
Verken negativt eller positivt	Alle andre tiltak

Tabell A.4 Regler for vurdering av enhetsverdi

Enhetsverdi	Regel
Svært høy	Dette kan være tiltak som medfører svært store investeringskostnader, eksempelvis etablering av nye og sikrede beredskapslagre eller bygging av transformatorstasjoner i fjellanlegg
Høy	Dette kan være tiltak som medfører store investeringskostnader (eksempelvis forbedret sikring av eksisterende anlegg) eller betydelige prosess- eller organisasjonsendringer (eksempelvis at KBO-enheter blir underlagt sikkerhetsloven)
Middels	Dette kan være tiltak som medfører økt trenings- og øvingsaktivitet, forbedret digital grunnsikring, forbedrede prosesser osv.
Liten	Alle andre tiltak

B Effekt-kostnadsvurdering av anbefalte tiltak

Tabell B.1 Ikke-prissatt effekt-kostnadsvurdering av anbefalte tiltak

Tiltak	Kvantum	Enhetsverdi	Kostnadsvirkning	Effektvirkning	Merknad
Videreutvikle veiledere for risikovurderinger og styring av risiko	Verken negativt eller positivt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Gi KBO-enheter økt kunnskap om hvordan de kan utnytte scenarioanalyser	Lite negativt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Etablere planforutsetninger for dimensjonering av kraftforsyningsberedskapen i krig	Lite negativt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Videreutvikle prosesser og metoder som gir oversikt over risiko i kraftforsyningen som helhet	Lite negativt	Middels	Liten negativ	Stor positiv	Lavthengende frukt
Operasjonalisere regjeringens strategi for å styrke motstandskraften mot desinformasjon i kraftsektoren	Lite negativt	Liten	Ubetydelig/ingen	Stor positiv	Lavthengende frukt
Videreføre arbeidet med å utvikle et overordnet trusselbilde for kraftforsyningen	Lite negativt	Liten	Liten negativ	Middels positiv	Lavthengende frukt
Gjøre sikkerhetsloven gjeldende for KBO-enheter i geografiske områder som er av stor betydning for nasjonale sikkerhetsinteresser og forsvarsevne	Middels negativt	Høy	Stor negativ	Meget stor positiv	Ressurs- og tidkrevende
Videreutvikle evne til å detektere og håndtere IKT-sikkerhetshendelser	Middels negativt	Middels	Middels negativ	Stor positiv	
Innføre ordninger for å validere og sertifisere maskinvare som benyttes i kraftforsyningen	Stort negativt	Middels	Stor negativ	Stor positiv	Bør utredes nærmere
Innføre dokumentasjonskrav til leverandører av programvare til kraftforsyningen	Stort negativt	Liten	Middels negativ	Middels positiv	Bør utredes nærmere
Sørge for at krav gjennom NIS2-direktivet danner et minimumsnivå for digital sikkerhet	Stort negativt	Liten	Middels negativ	Stor positiv	
Skape arenaer for erfaringslæring og deling av mønsterpraksis innen digital sikkerhet	Lite negativt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Utvikle en helhetlig handlingsplan for forsvarlig digitalisering av kraftnettet	Middels negativt	Middels	Middels negativ	Stor positiv	
Videreutvikle veiledere for sikkerhet i anskaffelser og leverandørkjeder for kraftsektoren	Lite negativt	Liten	Ubetydelig/ingen	Stor positiv	Lavthengende frukt

Tiltak	Kvantum	Enhetsverdi	Kostnadsvirkning	Effektvirkning	Merknad
Skjerpe regelverket for anskaffelser av utstyr til klassifiserte anlegg	Stort negativt	Liten	Middels negativ	Meget stor positiv	
Vurdere muligheter for produksjon av kritiske komponenter for kraftforsyningen både i Norge og gjennom nordisk samarbeid	Verken negativt eller positivt	Middels	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Opprettholde kravet i kraftberedskapsforskriften om at ekom til driftskontrollfunksjonen skal fungere uavhengig av funksjonssvikt i offentlige ekomtjenester	Middels negativt	Høy	Stor negativ	Meget stor positiv	
Opprettholde kravet i kraftberedskapsforskriften om at driftsradio skal fungere uavhengig av funksjonssvikt i offentlige ekomtjenester	Stort negativt	Middels	Stor negativ	Meget stor positiv	
Skjerpe kravet til reservestrøm for driftsradioen til 72 timer i områder som er viktige for nasjonale sikkerhetsinteresser og forsvarsevne	Middels negativt	Middels	Middels negativ	Meget stor positiv	
Inkludere strategiske hovedprioriteringer i nasjonal sikkerhetsstrategi i konsesjonsbehandlingen av klassifiserte kraftanlegg	Verken negativt eller positivt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Forby uautorisert droneflyging over kraftanleggene som NVE vurderer som mest kritiske	Verken negativt eller positivt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Etablere fysisk sikring mot små luftleverte sprengladninger for eksisterende anlegg som NVE vurderer som mest kritiske	Lite negativt	Høy	Middels negativ	Meget stor positiv	Ressurs- og tidkrevende
Sikre kritiske anlegg i fjellanlegg ved nyetablering eller utskifting av eksisterende anlegg	Lite negativt	Svært høy	Stor negativ	Meget stor positiv	Ressurs- og tidkrevende
Holde politiet og Forsvaret oppdatert om hvilke anlegg som vurderes som mest kritiske for kraftforsyningen	Verken negativt eller positivt	Liten	Ubetydelig/ingen	Stor positiv effekt	Lavthengende frukt
Forberede tiltak for rask gjenoppretting dersom kritiske anlegg som ikke er sikret i fjellanlegg, skades eller ødelegges	Lite negativt	Høy	Middels negativ	Meget stor positiv	
Etablere større og flere regionalt spredte beredskapslagre for å øke reparasjonsevnen og utholdenheten i en krise- eller krigssituasjon	Middels negativt	Svært høy	Meget stor negativ	Meget stor positiv	Ressurs- og tidkrevende
Utvide kraftberedskapsforskriften til å sette krav til klassifisering og sikring av beredskapslagre	Middels negativt	Høy	Stor negativ	Meget stor positiv	Ressurs- og tidkrevende
Gjennomgå transportplanleggingen for å avdekke om endringer i transportinfrastrukturen kan ha betydning for kraftforsyningsberedskapen	Lite negativt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt

Tiltak	Kvantum	Enhetsverdi	Kostnadsvirkning	Effektvirkning	Merknad
Få KBO-enhetene til å gjennomgå leverandøravtalene sine for å sikre tilstrekkelig reparasjonsevne i hele konfliktspekteret	Lite negativt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Få KBO-enhetene til å øke sin egen reparasjonsevne med tanke på materiell og tilgjengelig kompetanse, for å redusere avhengigheten av eksterne leverandører	Stort negativt	Middels	Stor negativ	Stor positiv	Ressurs- og tidkrevende
Vurdere hvordan fagutdanninger innen elkraft kan styrkes for å øke rekrutteringen til kraftsektoren.	Lite negativt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Gjennomgå planverk og trene og øve KBO	Lite negativt	Middels	Liten negativ	Stor positiv	Lavthengende frukt
Utvide KBO til å inkludere særlig viktige bedrifter i leverandørbransjen	Middels negativt	Middels	Middels negativ	Stor positiv	
Starte dialog mellom NVE, Forsvaret og Sivilforsvaret med tanke på fritaksordninger fra militær- eller sivilforsvars-tjeneste og fritaksordninger for materiell i krise eller krig	Lite negativt	Liten	Ubetydelig/ingen	Middels positiv	Lavthengende frukt
Styrke oppfølgingen og kontrollen med kraftberedskaps-forskriften §2-7 og videreutvikle veiledere for øvelser	Stort negativt	Liten	Middels negativ	Meget stor positiv	
Få norske KBO-enheter til å videreutvikle sikkerhets- og beredskapssamarbeidet med nordiske kraft- og nettselskaper	Middels negativt	Liten	Liten negativ	Stor positiv	Lavthengende frukt

Referanser

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal for Operational Research*, *253*, 1–13.

Aven, T. (2017). Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. *Reliability Engineering & System Safety*, *167*, 42–48. https://doi.org/10.1016/j.ress.2017.05.006

Aven, T. (2020). How to determine the largest global and national risks: Review and discussion. *Reliability Engineering & System Safety*, *199*, 106905. https://doi.org/10.1016/j.ress.2020.106905

Aven, T., Ben-Haim, Y., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., Kröger, W., Renn, O., Thompson, K. M. & Zio, E. (2018). *Society for Risk Analysis Glossary*. Society for Risk Analysis. https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Ben-Haim, Y. (2019). Info-Gap Decision Theory (IG). I V. A. W. J. Marchau, W. E. Walker, P. J. T. M. Bloemen & S. W. Popper (Red.), *Decision Making under Deep Uncertainty. From Theory to Practice* (s. 93–115). Springer.

Bondar, K. (2025, 2. juni). *How Ukraine's Operation "Spider's Web" Redefines Asymmetric Warfare*. Center for Strategic & International Studies. Hentet 17. juni 2025 fra https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

Brunbaum, M., Stern, D. L. & Rauhala, E. (2022, 25. oktober). *Russia's methodical attacks exploit frailty of Ukrainian power system*. The Washington Post. Hentet 8. mars 2023 fra https://www.washingtonpost.com/world/2022/10/25/russias-methodical-attacks-exploit-frailty-ukrainian-power-system/

Brännlund, A. & Peterson, L. (2024). Power politics: How electric grievances shape election outcomes. *Ecological Economics*, *217*, 108077. https://doi.org/https://doi.org/10.1016/j.ecolecon.2023.108077

Buvarp, P. M. H. & Sivertsen, E. G. (2025). *Valgpåvirkning i 2023 og 2024 - en trendstudie* (FFI-rapport 25/003). Forsvarets forskningsinstitutt.

Cobham, T. & Butler, A. (2024, 29. november). *Why is Russia targeting Ukraine's energy grid with missile attacks*. Independent. Hentet 16. juni 2025 fra https://www.independent.co.uk/news/world/europe/ukraine-russia-war-putin-oreshnik-missile-energy-power-attack-b2655757.html

Diesen, S. (2025, 27. juni). *Hva skal norsk luftvern beskytte?* DN. Hentet 1. juli 2025 fra https://www.dn.no/globalt/luftvern/langtidsplanen/nato/hva-skal-norsk-luftvern-beskytte/2-1-1838524

Diesen, S., Karlsen, G., Kosiander, A., Løvik, A. & Nyhamar, T. (2024). *Erfaringer fra krigen i Ukraina - læringspunkter etter tusen dager med krig* (FFI-rapport 24/01299). Forsvarets forskningsinstitutt.

Direktoratet for forvaltning og økonomistyring. (u.å.). *Veileder i samfunnsøkonomiske analyser*. Hentet 26. juni 2025 fra https://dfo.no/fagomrader/utredning-og-analyse-av-statlige-tiltak/samfunnsokonomiske-analyser/veileder-i-samfunnsokonomiske-analyser

Direktoratet for samfunnssikkerhet og beredskap. (2019). *Analyser av krisescenarioer 2019*. https://www.dsb.no/rapporter-og-evalueringer/analyser-av-krisescenarioer-2019/

Edwards, C., Butenko, V., Voitovych, O. & Vlasova, S. (2024, 14. april). *'Their tactics have changed': Russia's bid to blow apart Ukraine's power grid*. CNN. Hentet 16. juni 2025 fra https://edition.cnn.com/2024/04/14/europe/russia-tactics-ukraine-energy-power-strikes-intl/index.html

Endregard, M., Elstad, A.-K., Siedler, R. E., Tønsager, J., Brattekås, K. & Åtland, K. (2019). *Vurdering av Trident Juncture 2018* (FFI-rapport 19/01791; BEGRENSET). Forsvarets forskningsinstitutt.

Energi21. (2022). *Strategi 2022. Nasjonal strategi for forskning, utvikling, demonstrasjon og kommersialisering av ny klimavennlig energiteknologi*. https://www.energi21.no/contentassets/2ec5d9578a134adc930a0d9ecea1bf64/energi21_2022_webversjon-1.pdf

Energidepartementet. (2025, 27. juni). *Høring - Forslag fra Energidepartementet om endringer i energiloven om prioritert nettilknytning av hensyn til nasjonale sikkerhetsinteresser*. Hentet 1. juli 2025 fra https://www.regjeringen.no/no/dokumenter/horing-forslag-fra-energidepartementet-om-endringer-i-energiloven-om-prioritert-nettilknytning-av-hensyn-til-nasjonale-sikkerhetsinteresser/id3113120/?expand=horingsnotater

Etterretningstjenesten. (2025, 5. februar). *Fokus 2025. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Hentet 1. juli 2025 fra https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus2025_innhold

European Commission. (2022). *REPowerEU Plan* (COM(2022) 230 final). https://eur-lex.europa.eu/resource.html?uri=cellar:fc930f14-d7ae-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF

Forsvarets forskningsinstitutt. (2025). *Russland i krig* (Viten 1. 2025). https://www.ffi.no/publikasjoner/arkiv/russland-i-krig

Garimella, P. K. (2018, 25–27 Oct. 2018). IT-OT Integration Challenges in Utilities. 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), https://doi.org/10.1109/CCCS.2018.8586807

Grunnan, T. & Elstad, A.-K. (2018). *Observasjoner og betraktninger fra øvelse Trident Javelin/Polaris/Gram 2017 – Sivilt-militært samarbeid og erfaringslæring* (FFI-rapport 2018/01169; BEGRENSET). Forsvarets forskningsinstitutt.

Heggstad, Ø. J. (2016, 23. mars). *Må fjerne transformatoren etter storbrann*. NRK. Hentet 19. juni 2025 fra https://www.nrk.no/mr/ma-fjerne-hele-transformatoren-1.12868829

Holmstrøm, S. & Gjerde, O. (2024, 11. desember). *Digitalisering og automatisering i strømnettet*. SINTEFblogg. Hentet 22. juni 2025 fra https://blogg.sintef.no/energi/digitalisering-og-automatisering-i-stromnettet/

Innst. 224 S (2024-2025). *Innstilling fra kommunal- og forvaltningskomiteen om representantforslag om å fjerne byråkrati og sikre gjennomføringskraft i Forsvaret*. https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Innstillinger/Stortinget/2024-2025/inns-202425-224s/

Innst. 242 S (2024-2025). *Innstilling fra justiskomiteen om Totalberedskapsmeldingen - Forberedt på kriser og krig*. https://www.stortinget.no/globalassets/pdf/innstillinger/stortinget/2024-2025/inns-202425-242s.pdf

International Energy Agency. (2022). *World Energy Outlook 2022*. https://www.iea.org/reports/world-energy-outlook-2022

International Energy Agency. (2024). *Ukraine's Energy Security and the Coming Winter*. https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter

International Renewable Energy Agency. (2019). *A New World. The Geopolitics of the Energy Transformation*. Global Commission on the Geopolitics of Energy Transformation. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Jan/Global_commission_geopolitics_new_world_2019.pdf

International Risk Governance Council. (2018). *Guidelines for the Governance of Systemic Risks*.

Ivaniuk, P. (2025). *Massive Missile Attacks on Ukraine*. Kaggle. Hentet 15. juni 2025 fra https://www.kaggle.com/datasets/piterfm/massive-missile-attacks-on-ukraine

Kippe, H. (2025). *Sikkerhetsaspekter ved kjernekraft i Norge* (FFI-rapport 25/017). Forsvarets forskningsinstitutt.

Kiran, J. H., Lausund, R. & Arnesen, O. H. (2023). *Oppdatert behovsanalyse av fortifikatoriske anlegg for elektronisk kommunikasjon* (FFI-rapport 23/01896, BEGRENSET). Forsvarets forskningsinstitutt.

Klepper, K. B. & Gakkestad, J. (2025). *Avhengighet av utenlandske forsyningskjeder* (Eksternnotat under ferdigstillelse). Forsvarets forskningsinstitutt.

Klepper, K. B. & Lausund, R. (2025). *Forsyningssikkerhet og beredskap i kraftforsyningen. Beredskapsstrategier og reparasjonsberedskap* (FFI-rapport til publisering (BEGRENSET)). Forsvarets forskningsinstitutt.

Klinke, A. & Renn, O. (2012). Adaptive and integrative governance on risk and uncertainty. *Journal of Risk Research*, *15*(3), 273–292. https://doi.org/10.1080/13669877.2011.636838

Korsnes, M. K. (2016, 20. mars). *Vurderer om ein skal la oljen brenne ut*. NRK. Hentet 19. juni 2025 fra https://www.nrk.no/mr/kraftig-brann-i-trafostasjon-i-sunndal-1.12864763

Kultur- og likestillingsdepartementet. (2025). *Strategi for å styrkje motstandskrafta mot desinformasjon (2025–2030)*. https://www.regjeringen.no/no/dokumenter/strategi-for-a-styrkje-motstandskrafta-mot-desinformasjon-2025-2030/id3109255/

Kvadsheim, H. D., Øvergaard, B. N. & Barstad, L. (2023). *IKT-sikkerhetstilstanden i kraftforsyningen 2023* (NVE Rapport nr. 27/2023). Norges vassdrags- og energidirektorat. https://publikasjoner.nve.no/rapport/2023/rapport2023_27.pdf

Lausund, R. & Dullum, O. (2025). *Fysisk sikring av anlegg i kraftsektoren. Sikring mot militære trusler* (Eksternnotat under publisering (unntatt offentlighet)). Forsvarets forskningsinstitutt.

Lempert, R. J., Schlesinger, M. E. & Bankes, S. C. (1996). When we don't know the costs or the benefits: Adaptive strategies for abating climate change. *Climatic Change*, *33*(2), 235–274. https://doi.org/10.1007/BF00140248

Lister, T., Voitovych, O. & Butenko, V. (2022, 10. desember). *Ukraine keeps patching up its power grid. But Russia's barrage could force more Ukrainians to flee as winter bites*. CNN. Hentet 8. mars 2023 fra https://edition.cnn.com/2022/12/10/europe/ukraine-energy-russian-missiles-intl-cmd/index.html

Loen, U. P. & Gusdal, I. H. (2025). *A Global Energy Interconnection? Exploring China's Strategic Ambitions and Security Implications for Norway* (FFI-rapport til godkjenning). F. forskningsinstitutt.

Lu, M. (2023, 3. desember). *Ranked: The World's Top 10 Electronics Exporters (2000-2021)*. Visual Capitalist. Hentet 3. september 2025 fra https://www.visualcapitalist.com/top-10-electronics-exporters-in-the-world/

Lunde, M. & Lunde, A. (2022). *Evaluering etter uvær i Innlandet november 2021* (Rapport nr. 11/2022). S. i. Innlandet. https://www.statsforvalteren.no/siteassets/fm-innlandet/000-annet/publikasjoner/fmin-rapportserie/evaluering-etter-uvar-i-innlandet-november-2021.pdf

Meld. St. 9 (2024-2025). *Totalberedskapsmeldingen. Forberedt på kriser og krig*. Justis- og beredskapsdepartementet. https://www.regjeringen.no/contentassets/c24e6978185f4a49a7d2689a4741a9b1/no/pdfs/stm202420250009000dddpdfs.pdf

Ministerio Para La Transición Ecológica Y El Reto Demográfico. (2025, 17. juni). *The report of the Committee for the Analysis of the Electricity Crisis of April 28 is presented*. Hentet 20. juni 2025 fra https://www.miteco.gob.es/en/prensa/ultimas-noticias/2025/junio/se-presenta-el-informe-del-comite-de-analisis-de-la-crisis-elect.html

Nasjonal kommunikasjonsmyndighet. (2022). *Robuste transmisjonsnett for Norge mot 2030. Målbilder og virkemidler*.

Nasjonal sikkerhetsmyndighet. (2025, 5. februar). *Risiko 2025*. Hentet 1. juli 2025 fra https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2025

Nasjonal sikkerhetsmyndighet. (u.å.). *Oversikt over innmeldte grunnleggende nasjonale funksjoner*. Hentet 14. juni 2025 fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/grunnleggende-nasjonale-funksjoner/oversikt-over-innmeldte-grunnleggende-nasjonale-funksjoner/

NATO. (2024, 15. juli). *Washington Summit Declaration*. Hentet 25. juni 2025 fra https://www.nato.int/cps/en/natohq/official_texts_227678.htm?selectedLocale=en

NATO. (2025, 25. juni). *The Hague Summit Declaration*. Hentet 25. juni 2025 fra https://www.nato.int/cps/en/natohq/official_texts_236705.htm

Norges vassdrags- og energidirektorat. (2024a). *Gjensidige avhengigheter av IT og OT i kraftforsyningen* (NVE Ekstern rapport nr. 17/2024). https://publikasjoner.nve.no/eksternrapport/2024/eksternrapport2024_17.pdf

Norges vassdrags- og energidirektorat. (2024b). *Veiledning for risikovurdering av IT og OT* (NVE Veileder nr. 2/2024). https://publikasjoner.nve.no/veileder/2024/veileder2024_02.pdf

Norges vassdrags- og energidirektorat. (2025a). *Tilstanden i kraftsystemet 2025. Kraftåret 2024 og utviklingen fram mot 2029*. https://publikasjoner.nve.no/rapport/2025/rapport2025_10.pdf

Norges vassdrags- og energidirektorat. (2025b). *Trusselbildet i kraftforsyningen* (NVE Ekstern rapport nr. 3/2025). https://publikasjoner.nve.no/eksternrapport/2025/eksternrapport2025_03.pdf

NOU 2023: 3. *Mer av alt - raskere. Energikommisjonens rapport*. Olje- og energidepartementet.

NOU 2023: 17. *Nå er det alvor. Rustet for en usikker fremtid*. Justis- og beredskapsdepartementet.

NTT Security. (2024, 21. februar). *Russian hacker claims responsibility for massive cyberattack in Ukraine*. Hentet 15. juni 2025 fra https://se.security.ntt/en/russian-hacker-claims-responsibility-for-massive-cyberattack-in-ukraine/

Pham, V. (2025). *Bruk av offentlig elektronisk kommunikasjon i kraftforsyningen* (FFI-rapport 25/00889, unntatt offentlighet). Forsvarets forskningsinstitutt.

Pham, V., Farsund, B. & Ulshagen, A. (2024). *Digitalisering av kraftforsyningen - et første blikk på trusler og sårbarheter* (Eksternnotat 24/00123, unntatt offentlighet). Forsvarets forskningsinstitutt.

Politiets sikkerhetstjeneste. (2025, 5. februar). *Nasjonal trusselvurdering 2025*. Hentet 5. februar 2025 fra https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2025/

Prop. 87 S (2023-2024). *Forsvarsløftet - for Norges trygghet. Langtidsplan for forsvarssektoren 2025-2036*. Forsvarsdepartementet. https://www.regjeringen.no/contentassets/27e00e5acc014c5ba741aacfff235d99/no/pdfs/prp202320240087000dddpdfs.pdf

Quimbre, F., Arciniegas Rueda, I., van Soest, H., Schmid, J., Shatz, H. J., Heath, T. R., Meidan, M., Wullner, A., Deane, P., Glynn, J. & Regan, L. (2023). *China's Global Energy Interconnection: Exploring the Security Implications of a Power Grid Developed and Governed by China*. RAND Corporation. https://doi.org/10.7249/RRA2490-1

Regjeringen. (2023, 23. august). *NIS2-direktivet*. Hentet 26. oktober 2025 fra https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/

Rosenhead, J., Elton, M. & Gupta, S. K. (1972). Robustness and Optimality as Criteria for Strategic Decisions. *Journal of the Operational Research Society*, *23*(4), 413–431. https://doi.org/10.1057/jors.1972.72

Røyksund, M. & Valdal, A.-K. (2020). *Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning* (Ekstern rapport nr. 2/2020). Norges vassdrags- og energidirektorat. https://publikasjoner.nve.no/eksternrapport/2020/eksternrapport2020_02.pdf

Sabonis-Helf, T. (2025, 3. februar). *The Electricity Front of Russia's War against Ukraine*. War on the Rocks. Hentet 16. juni 2025 fra https://warontherocks.com/2025/02/the-electricity-front-of-russias-war-against-ukraine/

Sand, K. (2014). *Smart grid referansearkitektur og use cases* (TR A7415 - Åpen). S. E. AS. https://hdl.handle.net/11250/2492626

Schwebs, I., Bugge, S., Aase, K. A. & NTB. (2025, 21. mars). *Brannen ved Heathrow: Starter opp igjen flyginger*. VG. Hentet 19. juni 2025 fra https://www.vg.no/nyheter/i/OoB4rq/heathrow-stengt-etter-stor-brann-i-elektrisitetsstasjon

Sellevåg, S. R. (2023). *Tilsiktede handlinger som kan true norsk kraftforsyning - en scenariobasert tilnærming* (FFI-rapport 23/02425). Forsvarets forskningsinstitutt.

Sellevåg, S. R., Birkemo, G. A., Breivik, H., Endregard, M., Enemo, G., Grunnan, T., Johnsen, A., Lausund, R., Sendstad, O. J. & Thuv, A. (2022). *Styrker og svakheter ved dagens totalforsvar - rapport til Totalberedskapskommisjonen* (FFI-rapport 22/02620). Forsvarets forskningsinstitutt.

Sellevåg, S. R. & Ulshagen, A. (2023). *Bortfall av kritisk infrastruktur i Troms og Finnmark i fredstid – modellering av kaskadekonsekvenser* (FFI-rapport 23/utkast, BEGRENSET). Forsvarets forskningsinstitutt.

Skjelland, E., Glærum, S., Nyhamar, T., Sendstad, C., Arnfinnsson, B., Bentstuen, O. I., Betten, S. I., Birkemo, G. A., Diesen, S., Guttelvik, M. S., Hodnesdal, S. A., Presterud, A. O., Rustad, S., Sellevåg, S. R., Strand, K. R. & Tansem, I. (2025). *Forsvarsanalysen 2025* (FFI-rapport 25/006). Forsvarets forskningsinstitutt.

Skjelland, E., Glærum, S., Nyhamar, T., Sendstad, C., Arnfinnsson, B., Fauske, M. F., Gjørven, E., Klausen, R. A., Køber, P. K., Lammersdorf, A. B., Lausund, K. B., Olsen, K. E., Olsen, R., Reitan, J., Sellevåg, S. R. & Waage, K. (2024). *Forsvarsanalysen 2024* (FFI-rapport 24/00298). Forsvarets forskningsinstitutt.

Statnett. (2024, 2. september). *Kortsiktig Markedsanalyse 2024-2029*. Hentet 25. juni 2025 fra https://www.statnett.no/om-statnett/nyheter-og-pressemeldinger/nyhetsarkiv-2024/behov-for-a-styrke-stromnettet-og-stor-verdi-av-nettiltak--kortsiktig-markedsanalyse-2024-2029/

Statnett. (2025a). *Langsiktig markedsanalyse Norge, Norden og Europa 2024-2050*. https://www.statnett.no/globalassets/for-aktorer-i-kraftsystemet/planer-og-analyser/lma/langsiktig-markedsanalyse-2024-50.pdf

Statnett. (2025b). *Strategisk plan teknologi*. Hentet 24. juni 2025 fra https://www.statnett.no/globalassets/om-statnett/forskning-og-utvikling/strategisk-plan-teknologi.pdf

Statsministerens kontor. (2025). *Nasjonal sikkerhetsstrategi*. https://www.regjeringen.no/no/dokumenter/nasjonal-sikkerhetsstrategi/id3099304/

Storm, J.-M. (2024). *Intrusion Detection in Industrial Control Systems. Challenges in Implementation and Verification* [University of Oslo]. https://www.duo.uio.no/handle/10852/115408

Toftegaard, Ø. A. A. (2024). *Regulatory Strategies for a Resilient Smart Grid. Cybersecurity Compliance in the Electric Energy Sector* [Norwegian University of Science and Technology]. https://hdl.handle.net/11250/3154787

Ulshagen, A., Farsund, B. H. & Pham, V. (2025). *Digitalisering av kraftforsyningen – hvordan vil dette påvirke risikoen knyttet til tilsiktede uønskede handlinger?* (Eksternnotat 25/00981). Forsvarets forskningsinstitutt.

Ulshagen, A., Pham, V., Klepper, K. B. & Farsund, B. (2023). *Beredskap og samarbeid i ekombransjen og kraftforsyningen - identifiserte læringspunkter og prioriterte kunnskapsbehov* (Eksternnotat 23/01092). Forsvarets forskningsinstitutt.

UN Human Rights Monitoring Mission in Ukraine. (2024, 19. september). *Attacks on Ukraine's Energy Infrastructure: Harm to the Civilian Population*. Hentet 25. juni 2025 fra https://ukraine.un.org/en/278992-attacks-ukraine%E2%80%99s-energy-infrastructure-harm-civilian-population

Wang, M., Kang, W., Chen, Z., Zhang, Y., Liu, C. & Yang, F. (2018). Global Energy Interconnection: an innovative solution for implementing the Paris Agreement—the significance and pathway of integrating GEI into global climate governance. *Global Energy Interconnection*, *1*(4), 467–476. https://www.sciencedirect.com/science/article/pii/S2096511718300677

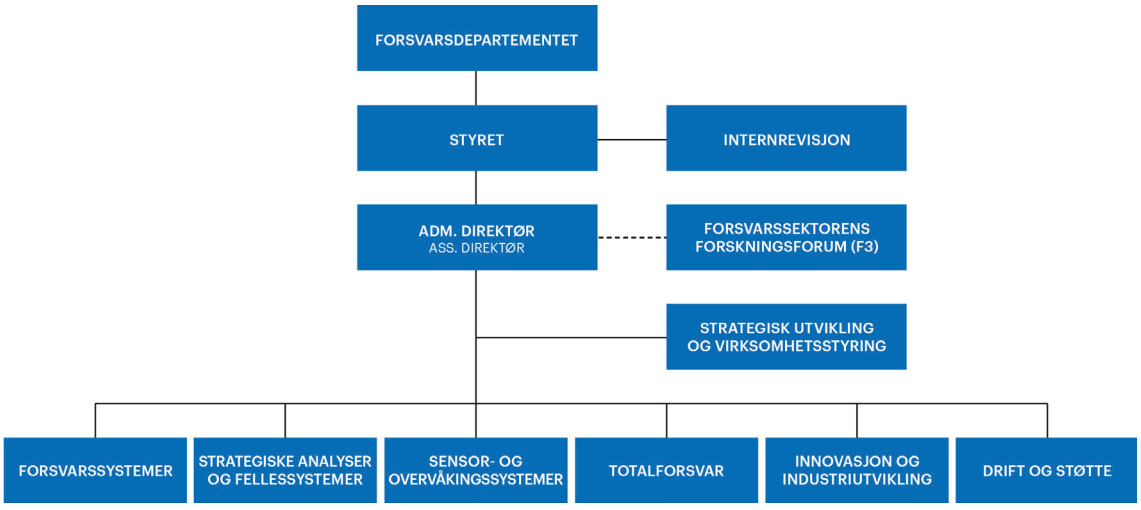
Waage, K. & Lindgren, P. Y. (2022). *Økonomisk statshåndverk, teknologisk utvikling og implikasjoner for norsk sikkerhet - en forstudie* (FFI-rapport 22/01758). Forsvarets forskningsinstitutt.

Om FFI
Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs formål
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

FFIs visjon
FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs verdier
Skapende, drivende, vidsynt og ansvarlig.



Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en