FFI Forsvarets forskningsinstitutt

23/02425

FFI-RAPPORT

Tilsiktede handlinger som kan true norsk kraftforsyning

– en scenariobasert tilnærming

Stig Rune Sellevåg

Tilsiktede handlinger som kan true norsk kraftforsyning

– en scenariobasert tilnærming

Stig Rune Sellevåg

Forsvarets forskningsinstitutt (FFI) 15. desember 2023

Emneord
Kraftforsyning
Trusler
Scenarioer
Nasjonal sikkerhet
Samfunnssikkerhet

FFI-rapport
23/02425

Prosjektnummer
5953

Elektronisk ISBN
978-82-464-3506-0

Engelsk tittel
Malicious acts that can harm the Norwegian power system – a scenario-based approach

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 norsk sikkerhet. Norges posisjon som energinasjon i kombinasjon med vår geografiske nærhet til Russland gjør at vi kan bli utsatt for press og angrep. Energiomstilling gjør at det norske kraftsystemet vil spille en stadig viktigere rolle fremover i en tid med stormaktsrivalisering og krig i Europa.

Formålet med dette arbeidet har vært å belyse tilsiktede handlinger som kan true norsk kraftforsyning, og som det er nødvendig å ha beredskap for å håndtere. Dette er gjort gjennom en scenariobasert tilnærming.

Utfallsrommet for hvilke fremtidige tilsiktede handlinger det er som kan true norsk kraftforsyning, er stort og beheftet med stor usikkerhet. Funnene viser at norsk kraftforsyningsberedskap bør ta høyde for følgende kategorier av tilsiktede handlinger: (i) datakriminalitet, (ii) ekstremisme fra politisk motiverte ikke-statlige aktører, (iii) sammensatte trusler i form av maktposisjonering, fordekt tvang, sabotasje eller tvangsdiplomati fra fremmedstatlige aktører og (iv) væpnede angrep. Disse kategoriene kan benyttes for å utvikle konkrete scenarioer for tilsiktede handlinger som norsk kraftforsyningsberedskap må ta høyde for.

Det er også stor usikkerhet knyttet til samfunnsutviklingen mot lavutslippssamfunnet som er nødvendig for at Norge skal nå klimaforpliktelsene sine. Dette gjelder både omfanget av og tempoet på energiomstillingen og i hvilken grad tilliten i samfunnet opprettholdes. I dette arbeidet har vi beskrevet denne usikkerheten i form av fire fremtidsbilder: «På kjente stier», «Klimaspranget», «Spredning i laget» og «Bakpå».

Store samfunnsendringer vil være nødvendige for at Norge skal bli et lavutslippssamfunn. Hvorvidt en omfattende energiomstilling vil føre til at samfunnet går i retning av «Klimaspranget» eller «Spredning i laget», vil blant annet være avhengig av i hvilken grad Norge lykkes med slike omfattende samfunnsendringer på måter som gjør at tilliten i samfunnet opprettholdes.

Begrenset energiomstilling kombinert med svekket tillit i samfunnet («Bakpå») fremstår som den farligste utviklingsretningen fordi økt politisk polarisering og økt konflikt i samfunnet kan gjøre Norge mer sårbart overfor tilsiktede handlinger. I en slik sammenheng må det tas med i betraktningen at konsekvenser av klimaendringer kan fungere som en trusselmultiplikator.

Videreutviklingen av norsk kraftforsyningsberedskap må ta hensyn til både usikkerheten og ustabiliteten i den sikkerhetspolitiske situasjonen og energiomstillingen mot et lavutslippssamfunn. Strategier som fungerer godt over et bredt spektrum av mulige utfall, bør velges for å møte det fremtidige utfordringsbildet. I et slikt perspektiv bør norsk kraftforsyningsberedskap ta høyde for realistiske verstefallsscenarioer i hele konfliktspekteret. Slike verstefallsscenarioer må også inkludere krig.

Summary

Reliable power supply is of vital importance for economic growth, the welfare of the population and national security. Norway's position as an energy nation together with our geographical proximity to Russia makes Norway vulnerable to pressure and attacks. As a consequence of the clean energy transition, the Norwegian power system will play an increasingly important role going forward; this happens in a time with great power rivalry and war in Europe.

The purpose of this work has been to shed light on malicious acts that can harm the Norwegian power supply and that Norway needs to prepare for. This has been done through a scenario-based approach.

The range of outcomes for which future malicious acts could harm the Norwegian power system is large and fraught with great uncertainty. Our findings show that the Norwegian power supply preparedness should take into account the following categories of malicious acts: (i) cyber-crimes, (ii) extremism from politically motivated non-state actors, (iii) foreign state actors' hybrid interference activities in the form of priming, covert coercion, sabotage or coercive diplomacy, and (iv) armed attacks. These categories can be used to develop specific scenarios for malicious acts that the Norwegian power supply preparedness must include.

There is also significant uncertainty related to the transition towards the low-emission society that is necessary to meet Norway's climate commitments. This applies to both the extent and pace of the energy transition and to the degree to which trust in society is maintained. In our work, we describe this uncertainty in the form of four futures: 'On Familiar Paths', 'The Green Leap', 'Worlds Apart' and 'Falling Behind'.

Major changes will be necessary for Norway to become a low-carbon society. Whether an extensive energy transition will lead our society in the direction of 'The Green Leap' or in the direction of 'Worlds Apart' will depend, among other things, on the extent to which Norway is able to undertake such major societal changes while still maintaining a high level of trust in society.

Limited energy transition combined with weakened trust in society ('Falling Behind') appears as the most dangerous direction of development because increased political polarization and increased conflict in society can make Norway more vulnerable to malicious acts. In such a context, we must consider that consequences of climate change can act as a threat multiplier.

The further development of the Norwegian power supply preparedness must take into account both the uncertainty and instability in the security policy situation and the energy transition towards a low-carbon society. Strategies that work well across a wide range of possible outcomes should be chosen to meet future challenges. In such a perspective, the Norwegian power supply preparedness should include realistic worst-case scenarios in the entire conflict spectrum. Such worst-case scenarios must also include war.

Innhold

Forord

Denne rapporten er utarbeidet på oppdrag for Norges vassdrags- og energidirektorat (NVE) og Statnett. Rapporten er en del av FFI-oppdraget «Forsyningssikkerhet og beredskap i kraftforsyningen» som er finansiert av NVE og Statnett. Et gradert vedlegg til rapporten med konkrete scenarioer vil utarbeides som en del av oppdraget.

Ressurspersoner ved NVE, Statnett og FFI takkes for gode diskusjoner.

Kjeller, 15. desember 2023
Stig Rune Sellevåg

1 Innledning

Kraftforsyning er grunnleggende for vår velferd, for kritiske samfunnsfunksjoner og for vår forsvarsevne. I «World Energy Outlook 2022» advarte det internasjonale energibyrået (IEA) om at verden kan stå overfor en global energikrise, utløst av Russlands invasjon av Ukraina 24. februar 2022 (IEA, 2022b). Energikrisen og behovet for energiomstilling for å redusere konsekvenser av klimaendringer, har aktualisert betydningen av forsyningssikkerhet for strøm i Norge. Regjeringen har derfor i 2022 og 2023 fått gjennomført to utredninger – Strømnettutvalget og Energikommisjonen – av fremtidige energibehov og hvordan energiproduksjon og strømnettet bør utvikles i tiden fremover. Energikommisjonen fastslår at når samfunnet skal elektrifiseres i høy fart mot 2050, blir forsyningssikkerhet tilsvarende viktigere og samtidig mer krevende å opprettholde (NOU 2023: 3, s. 148).

Forsyningssikkerhet for strøm er beskrevet som «kraftsystemets evne til å kontinuerlig levere strøm av en gitt kvalitet til sluttbrukere, og omfatter både energisikkerhet, effektsikkerhet og driftssikkerhet/leveringspålitelighet» (NOU 2023: 3, s. 148-149):

- 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 på antall avbrudd i strømforsyningen og avbruddenes varighet»

Denne beskrivelsen gir imidlertid få svar på følgende spørsmål som ethvert sikkerhetskonsept bør adressere (Baldwin, 1997):

1. Sikkerhet for hvem?
2. Sikkerhet for hvilke verdier?
3. Sikkerhet mot hvilke farer og trusler?
4. Hvor mye sikkerhet er nødvendig?
5. Sikkerhet med hvilke virkemidler?
6. Sikkerhet til hvilken kostnad?
7. Sikkerhet over hvilken tidsperiode?

Dette arbeidet er avgrenset til de tre første spørsmålene.

Når det gjelder de to første spørsmålene, er pålitelig kraftforsyning av vital betydning for verdiskaping og befolkningens velferd (NOU 2023: 3, s. 148). Kraftforsyning er også av vital betydning for norske myndigheter og virksomheters evne til å ivareta samfunnssikkerheten og nasjonale sikkerhetsinteresser (DSB, 2016; NATO, 2022b; NSM, 2021). Opprettholdelse av kraftforsyning er derfor nødvendig i hele krisespekteret, også i krig, jf. energiloven § 9-1. Det er valgt å avgrense analysen til forhold som kan påvirke samfunnssikkerheten og nasjonale sikkerhetsinteresser.

Formålet med dette arbeidet er å belyse det tredje spørsmålet; altså hva kan true norsk kraftforsyning og som det er nødvendig å ha beredskap for å håndtere. Analysen er avgrenset til tilsiktede handlinger. Det henvises til DSB (2019) for analyse av scenarioer for naturhendelser som kan påvirke norsk kraftforsyning.

Hvilke fremtidige tilsiktede handlinger som kan true norsk kraftforsyning er nødvendigvis beheftet med stor usikkerhet og utfallsrommet er stort. For å håndtere denne usikkerheten, kan scenarioer benyttes. Et scenario er en beskrivelse av en mulig situasjon som er relevant med hensyn til planlegging og forebygging av fremtidige utfordringer (Amer *et al.*, 2013).

Følgende metodiske tilnærming er benyttet for scenarioutviklingen: Først beskrives utviklingstrekk som er av betydning for utfallsrommet for hvilke tilsiktede handlinger som kan skje (kapittel 2). Valgt tidshorisont for analysen er frem til 2030. Dernest benyttes morfologisk analyse (Ritchey, 2013a, 2013b; Zwicky, 1969) for å strukturere kompleksiteten i utfallsrommet (kapittel 3). På bakgrunn av den morfologiske analysen beskrives kategorier av tilsiktede handlinger som kan true norsk kraftforsyning (kapittel 3.2). Ulike fremtidsbilder som kan oppstå som følge av samfunnsendringer, belyses i kapittel 5. Til slutt trekkes konklusjoner i kapittel 6. Utfyllende informasjon fra den morfologiske analysen er gitt i vedlegg A.

2 Utviklingstrekk frem mot 2030

Dette kapittelet oppsummerer utviklingstrekk som er av betydning for norsk kraftforsyning. Utviklingstrekkene som diskuteres er klimaendringer, teknologisk utvikling, kriminalitetsutvikling i det digitale rom, terrorisme i Vest-Europa og trusler fra fremmedstatlige aktører. Tidsperspektivet er frem mot 2030. Der hvor ikke annet er oppgitt, er oppsummeringen basert på Beadle *et al.* (2019), Sellevåg *et al.* (2020), Sellevåg *et al.* (2021), Klepper *et al.* (2022) og Skjelland *et al.* (2023).

2.1 Klimaendringer

Klimaendringer er en av de største samfunnsutfordringene vi står overfor, og effekter av klimaendringer kan påvirke vår samfunnssikkerhet og våre nasjonale sikkerhetsinteresser. Dette skyldes ikke bare de direkte effektene av klimaendringer, men også fordi klimaendringer kan forsterke andre, eksisterende sikkerhetsutfordringer (NATO, 2022a).

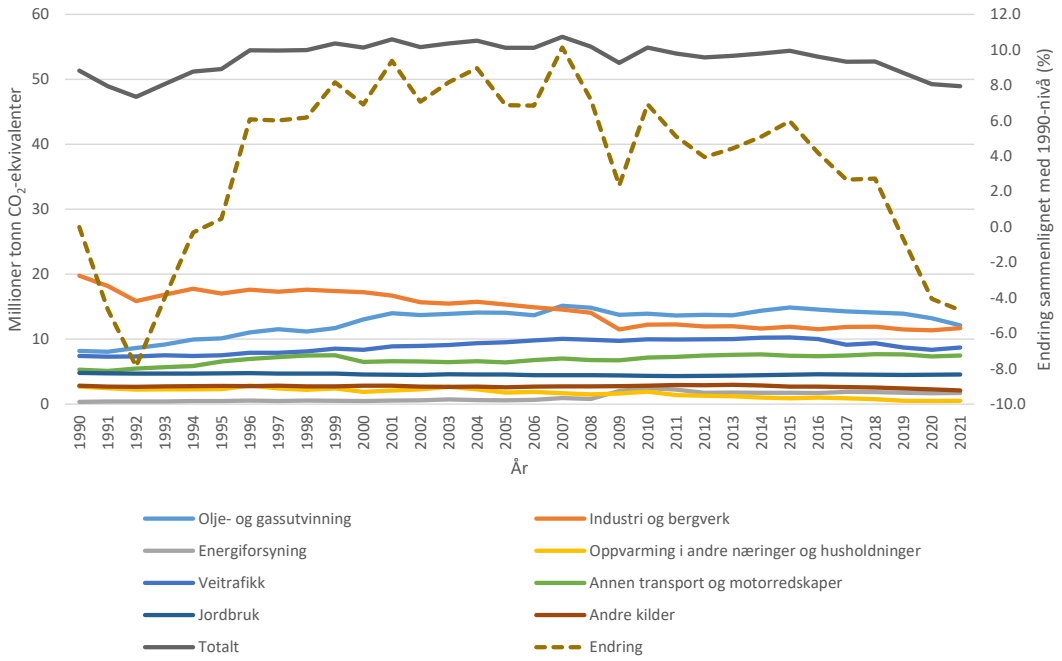
Det er bred vitenskapelig konsensus knyttet til at menneskelig påvirkning er den viktigste driveren av mange observerte klimaendringer (IPCC, 2021). FNs klimapanel fastslår i sin sjette hovedrapport at vi kan komme til å oppleve år med 1,5-graders global oppvarming allerede på 2030-tallet. Det er også et etablert faktum at menneskeskapte klimaendringer har ført til at episoder med ekstremvær, og særlig hetebølger, har blitt mer intense og opptrer hyppigere.

Verdenssamfunnet er langt unna å nå klimamålene i Parisavtalen. FNs klimapanel vurderer at det ikke vil være mulig å redusere global oppvarming under 2 °C uten raske og omfattende reduksjoner i utslipp fra energisystemet (IPCC, 2022). Noen klimaendringer lar seg ikke reversere, men det er fremdeles mulig å hindre de mest alvorlige konsekvensene fordi teknologien som kreves er tilgjengelig. De klimapolitiske valgene som tas det neste tiåret er derfor avgjørende for å hindre katastrofale følger.

2.1.1 Norges klimaforpliktelser og fremtidig kraftbehov

For å redusere konsekvenser av klimaendringer er det nødvendig med omfattende endringer i energisystemet og det må skje raskt. FNs klimapanel peker på redusert bruk av fossile brensler, økt bruk av energikilder med null eller lite utslipp, økt elektrifisering, karbonfangst og -lagring, redusert energiforbruk og økt energieffektivitet som nødvendige tiltak (IPCC, 2022).

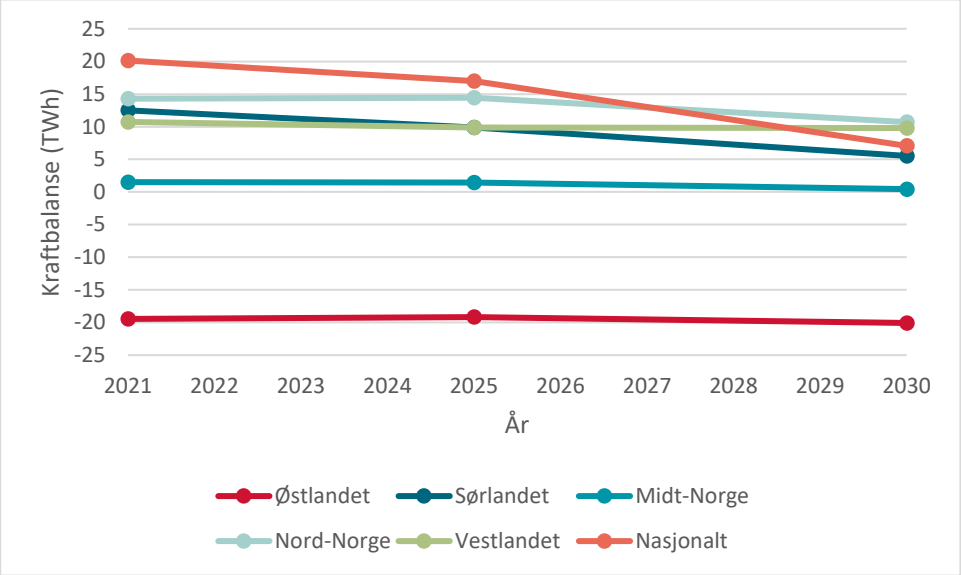
Gjennom regjeringens klimaplan for 2021–2030 har Norge forpliktet seg til å redusere utslippet av klimagasser med 55 % sammenlignet med 1990-nivå innen 2030 (Meld. St. 13 (2020-2021)). I tillegg har Norge forpliktet seg til å nå et karbonnøytralt lavutslippssamfunn innen 2050 ved å redusere utslippene med 90–95 %. Per 2021 var norske klimagassutslipp redusert med –4,7 % sammenlignet med 1990-nivå (Figur 2.1). Dette setter Norge på en kurs mot 20 % utslippskutt innen 2030 ifølge OECD (2022).



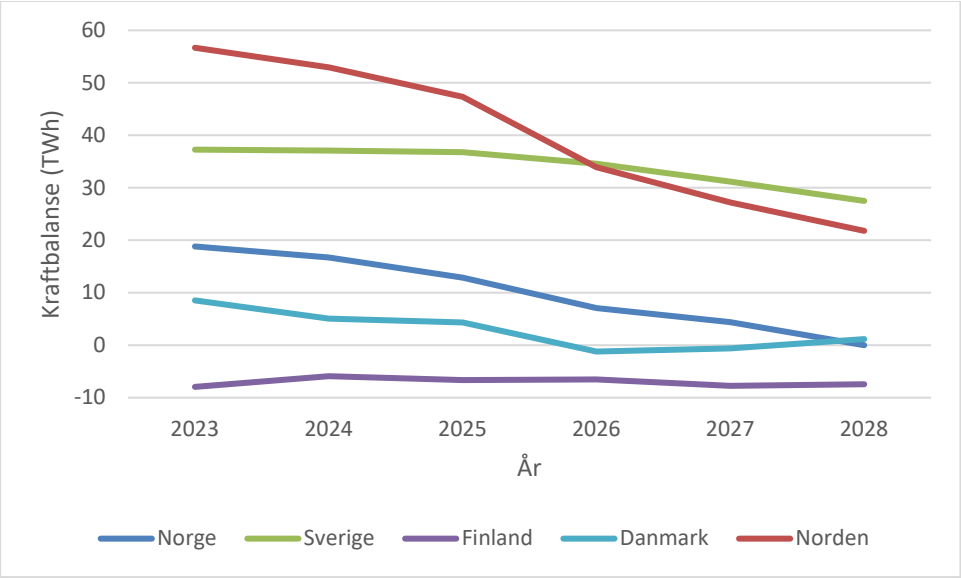
Figur 2.1 *Norske utslipp av klimagasser per hovedkilde 1990-2021 i millioner tonn CO_2-ekvivalenter, samt endring i prosent sammenlignet med 1990-nivå. Kilde: Utslipp til luft, Statistisk sentralbyrå*

Energikommisjonen skriver i sin utredning at massive behov for mer fornybar kraft er nødvendig for at klimamålene skal nås (NOU 2023: 3, s. 9). Dette må til når landtransport skal elektrifiseres, sjøtransport skal over på utslippsfritt drivstoff basert på fornybar kraft, dagens industri basert på fossilt brensel skal gjennom det grønne skiftet og ny grønn industri skal etableres.

Frem mot 2030 forventes det en vekst i kraftbruk på mellom 21 og 35 TWh, kanskje helt opp mot 75 TWh, avhengig av hva som antas om ny grønn industrietablering (NOU 2023: 3, s. 10). Uten et taktskifte i kraftutbyggingen, kan det bli vanskelig å opprettholde kraftoverskudd i normalår. Forventet fremtidig utvikling for kraftbalansen er derfor viktig for vurderinger av hvordan forsyningssikkerheten vil utvikle seg. I basisscenarioet vurderer NVE (2021) at kraftoverskuddet nasjonalt reduseres frem mot 2030, med betydelige forskjeller mellom kraftprisområdene (Figur 2.2). Statnett (2023) estimerer at Norges kraftbalanse går mot null i 2028 (Figur 2.3). Ser man Norden under ett, er kraftoverskuddet rundt 57 TWh i 2023. Statnett (2023) estimerer at dette reduseres til rundt 22 TWh i 2028. Energikommisjonen fremhever at et tørrår i 2030 kan bli krevende å håndtere uten import, flerårsmagasiner og forbrukerfleksibilitet på vårparten (NOU 2023: 3, s. 154-158). Import blir særlig viktig hvis vi får flere tørrår år på rad, mens flerårsmagasiner er viktig for forsyningssikkerheten når mer uregulerbar kraft fases inn.



Figur 2.2 Forventet kraftbalanse for Norge og i norske prisområder (basisscenario). Kilde: NVE (2021)



Figur 2.3 Forventet kraftbalanse for Norge og Norden (basisscenario). Kilde: Statnett (2023)

Energikommisjonen foreslår flere tiltak for å møte situasjonen (NOU 2023: 3, s. 9-25):

- Mer effektiv og fleksibel energibruk på alle områder
- Utnytte alle kilder til mer fornybar kraft (vannkraft, vindkraft på land og til havs og sol-kraft, samt tiltak for fjernvarme bioenergi og varmepumper)
- Raskere saksbehandling for ny kraftproduksjon
- Mer nettkapasitet (jf. tiltakene foreslått i NOU 2022: 6)

Når det gjelder kjernekraft, vurderer flertallet i kommisjonen at dette er ikke en løsning for Norge nå (NOU 2023: 3, s. 18). Energikommisjonen advarer også om at kraftutbygging kan stoppe opp av ulike grunner:

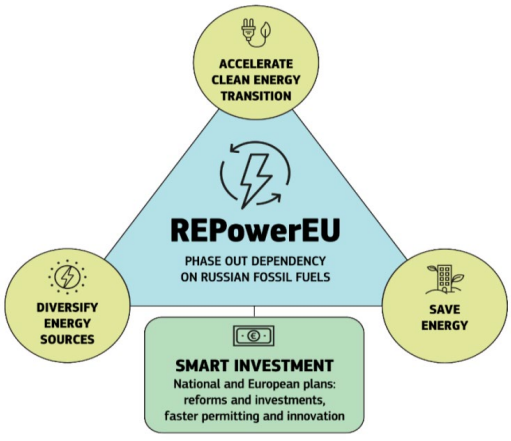
- Naturhensyn
- Folkelig motstand
- Høye kostnader

Dersom økt kraftutbygging ikke lykkes i tempoet som er nødvendig, kan politikerne bli stilt overfor en situasjon hvor de må ta stilling til følgende alternativer (NOU 2023: 3, s. 24):

- Å godta en overgangsperiode med stram eller negativ kraftbalanse. I en slik situasjon kan Norge bli avhengig av betydelig import fra Norden og Europa for øvrig hvis det blir tørrår.
- Utsette elektrifiseringsprosjekter, men hvor en da står i fare for å ikke nå klimamålene for 2030.
- Begrense tilknytningen av ny kraftintensiv industri.

2.1.2 Energisystemet i Europa: Storstilt omstilling og tett integrasjon

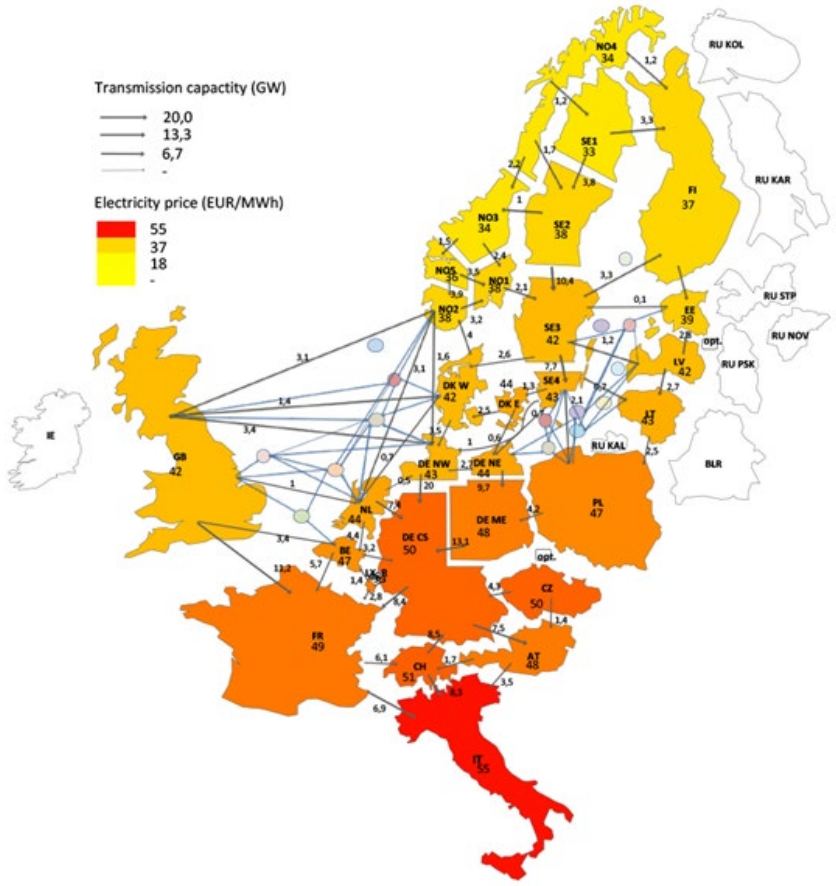
I tillegg gjennomgår den europeiske kraftsektoren en storstilt omstilling, både som følge av klimaforpliktelser òg som følge av behovet for å redusere avhengigheten av russisk naturgass. EUs plan *REPowerEU* skal bidra til dette gjennom energieffektivisering, akselerert produksjon av og overgang til ren energi, diversifisering av energiforsyningen og smarte investeringer (European Commission, 2022) (Figur 2.4).



Figur 2.4 EUs REPowerEU-plan. Kilde: European Commission (2022)

Økt overføringskapasitet mellom land er avgjørende for at Europa skal nå sine klimamål (ENTSO-E, 2022). Videre viser scenarioer fra ENTSO-E (2022) at det et

fullt integrert energisystem for strøm, naturgass og hydrogen kan muliggjøre karbonnøytral energiproduksjon i Europa før 2050. Det forventes store avhengigheter mellom Norden, og spesielt Norge, og resten av Europa i et slikt system (Figur 2.5). Under energikrisen i 2022 med høye strømpriser i Norge, ble det mye debatt rundt Norges mellomlandsforbindelser og hvorvidt de styrker eller svekker norsk forsyningssikkerhet (Kampevoll & Lorch-Falch, 2022).



Figur 2.5 Fremtidig handel og transmisjonskapasitet i Europa i 2050 som beregnet i Nordic Clean Energy Scenarios. Kilde: Wråke et al. (2021).

2.2 Teknologisk utvikling

Teknologiutviklingen i dag kjennetegnes ved at både utviklingen og kunnskapsspredningen går svært raskt. Utviklingen drives frem av kommersielle interesser, behov for næringsutvikling og verdiskaping, samt behov for å fornye offentlig sektor. Samtidig er teknologiutvikling også avgjørende for å lykkes med det grønne skiftet. Sentrale teknologiområder knyttet til energiomstilling er digitaliserte og integrerte energisystemer, vannkraft, vindkraft på land og til havs, solenergi, batterier, hydrogen og CO_2-håndtering (Energi21, 2022). I det følgende diskuteres utvalgte faktorer knyttet til fremvoksende og banebrytende teknologier, digitaliserte og integrerte energisystemer, samt tilgang på kritiske råvarer for viktige teknologier knyttet til energiomstillingen.

2.2.1 Fremvoksende og banebrytende teknologier

Fremvoksende og banebrytende teknologier som kommunikasjonsteknologi (5G), informasjonsteknologi og skybaserte tjenester, kunstig intelligens og stordata, tingenes internett, robotisering og autonome systemer, romteknologi, kvanteteknologier og syntetisk biologi er eksempler på teknologiområder som er av stor betydning for verdiskaping i samfunnet. Dette er teknologier som kan gi oss store muligheter for verdiskaping, men som også har militære anvendelser og som kan utnyttes av kriminelle (Andås, 2020; Klepper *et al.*, 2022; NATO Science and Technology Organization, 2023; Sellevåg *et al.*, 2021; Sellevåg *et al.*, 2020).

Felles for mange av de fremvoksende og banebrytende teknologiene er at de er sentrale for den digitale transformasjonen av samfunnet. Den digitale transformasjonen drives frem gjennom utnyttelse og analyse av data, hvor fire generelle utviklingstrekk er karakteristiske for utviklingen (Klepper *et al.*, 2022):

- Intelligent
- Sammenkoblet
- Distribuert
- Digitalt

Tilgang til internett blir derfor nærmest grunnleggende for all næringsvirksomhet, hvor informasjons- og kommunikasjonsteknologi (IKT) blir en integrator for moderne verdiskaping.

Et annet karakteristisk for teknologiutviklingen er at det skapes synergier mellom ulike teknologiområder og at ulike teknologier konvergerer og smelter sammen. Datadrevne beslutninger er et eksempel i så måte hvor dette muliggjøres gjennom å utnytte synergier mellom innsamling av store datamengder, bruk av kunstig intelligens og IKT. Denne utviklingen vil forsterkes ved å utnytte nye sensorteknologier og kvantedatamaskiner. Utnyttelse av data og nye beregningsmetoder forventes også å gjøre det lettere å utvikle nye materialer, for eksempel for energilagring eller for elektronikk som ikke er basert på bruk av silisium-brikker (NATO Science and Technology Organization, 2023).

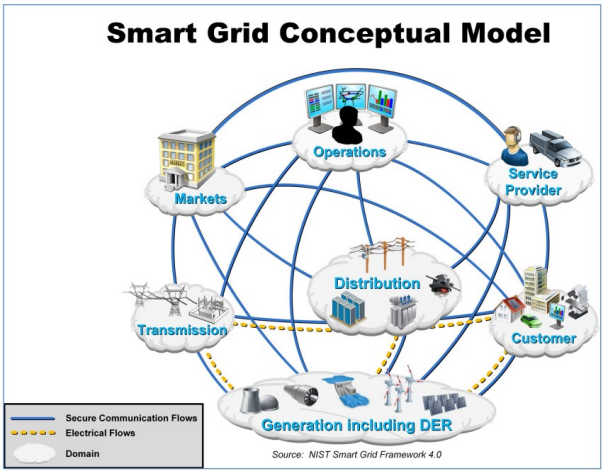
Utviklingen som forventes innen IKT kan gjøre sikkerhetsarbeidet mer krevende. Tette koblinger og dynamiske avhengigheter, lange verdikjeder og rask innføring av ny teknologi øker kompleksiteten i IKT-systemene. I tillegg øker angrepsflaten for trusler i det digitale rom (Farsund *et al.*, 2022) og for sikkerhetstruende økonomisk virkemiddelbruk (Waage & Lindgren, 2022).

2.2.2 Digitaliserte og integrerte kraftsystemer («smartgrids»)

I tillegg til økt kraftproduksjon, fremheves økt fleksibilitet på produksjons- og etterspørselssiden som avgjørende for å lykkes med elektrifiseringen av Norge på en samfunnsøkonomisk effektiv måte og for å ivareta forsyningssikkerheten (NOU 2023: 3). Dette skyldes at det er dyrt og tidkrevende å bygge ut kraftnettet for å håndtere høyere strømforbruk og økte effekttopper.

Store deler av dagens kraftsystem kjøres med betydelig sikkerhetsmargin på grunn av mangelfulle muligheter for automatisert overvåking og styring (Energi21, 2022, s. 43). Med økt uregulerbar kraftproduksjon, kraftproduksjon som flyttes nærmere forbrukerne («distribuert produksjon») og økte effekttopper, er det helt nødvendig å ta i bruk teknologi som bidrar til økt utnyttelse av det eksisterende kraftnettet samtidig som krav til forsyningssikkerhet opprettholdes. For å oppnå dette må IKT og andre digitale teknologier integreres tett med kraftsystemet. En annen suksessfaktor er økt digital samhandling mellom nettselskaper og andre aktører i kraftbransjen.

Slike digitaliserte og integrerte kraftsystemer omtales gjerne som «smartgrids» og dette vil være såkalte cyber-fysiske systemer.[1] En konseptuell modell for smartgrids er vist i Figur 2.6. Et karakteristisk trekk ved modellen er forskjellen i kompleksitet mellom flyten av strøm og flyten av informasjon i systemet. Det er også grunn til å forvente at antall aktører i systemet øker (lengre verdikjeder).



Figur 2.6 Konseptuell modell for smartgrid (DER er forkortelse for distribuert energiproduksjon). Kilde: Reprodusert fra Gopstein et al. (2021)

Den økte kompleksiteten i systemet øker risikoen for at feil kan oppstå. Samtidig kan konsekvensene av uønskede hendelser bli større. Det har lenge vært kjent at store kaskadefeil kan oppstå i komplekse nettverk, hvor feil i en liten andel av kritiske noder i nettverket kan føre til fullstendig sammenbrudd i systemet (Buldyrev *et al.*, 2010). Smartgrid kan også være sårbare overfor cyberangrep hvor falske

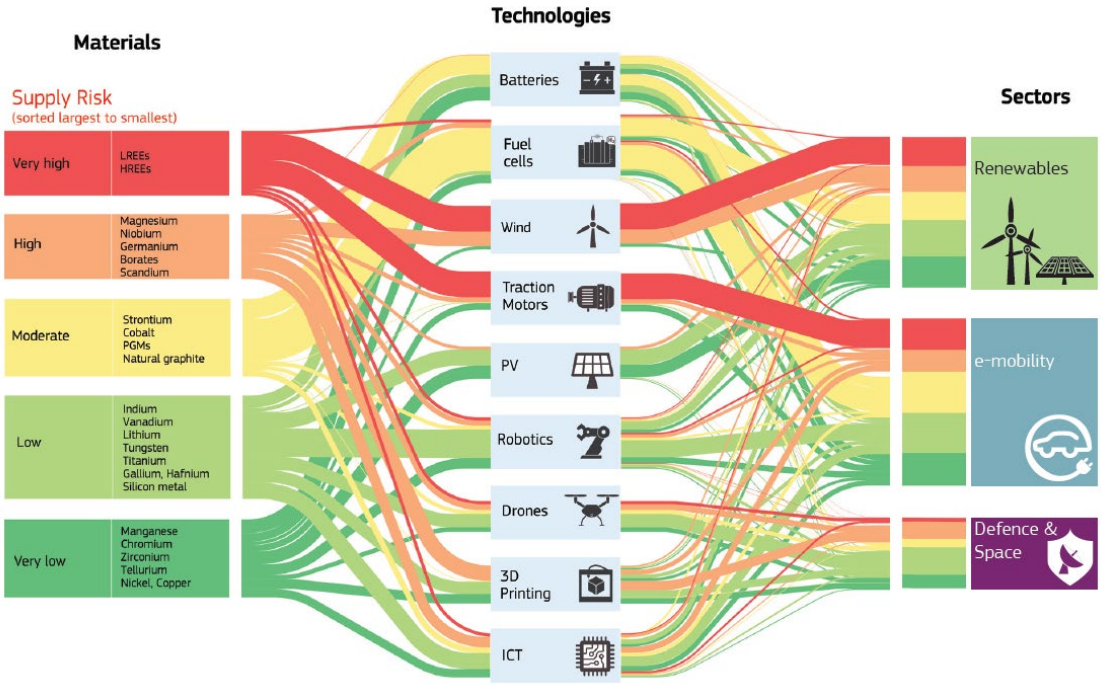
[1] For en beskrivelse av cyber-fysiske systemer, se for eksempel Griffor (2017).

data injiseres for å lure sensorene i systemet (Chen *et al.*, 2016; Liu *et al.*, 2011) eller cyber-angrep hvor lasten i systemet manipuleres (Amini *et al.*, 2018; Cardenas, 2021; Huang *et al.*, 2019; Soltan *et al.*, 2018). Sikker styring og kontroll av smartgrids blir derfor sentralt for å opprettholde forsyningssikkerheten.

2.2.3 Tilgang til kritiske råmaterialer

Tilgang på kritiske råmaterialer er avgjørende for utvikling av teknologier. EU har utarbeidet en liste over kritiske råmaterialer for strategisk viktige teknologiområder som elektronikk, fornybar energi og digitale teknologier (Tabell 2.1). Oversikten viser at Kina dominerer produksjonen av svært mange av dem. Dette gjelder særlig sjeldne jordarter hvor EU er fullstendig avhengig av import. Andre eksempler er DR Kongo som har størsteparten av koboltressursene i verden, mens Sør-Afrika er største produsent av platinametaller. I tillegg har også Russland store forekomster av kritiske råmaterialer (særlig palladium, titan og vanadium) (European Commission, 2020b).

Koronapandemien som brøt ut i 2019–2020 viste hvor sårbare globale forsyningskjeder er for forstyrrelser. For eksempel kan politisk ustabilitet i land som har store ressurser av råmaterialer, føre til forstyrrelser eller svikt i forsyninger. I tillegg kan land med dominerende markedsmakt utnytte denne posisjonen til maktutøvelse (Waage & Lindgren, 2022, s. 44). Det er derfor viktig å ha oversikt over risikoen knyttet til tilgang til kritiske råmaterialer. I en studie gjennomført av EU, vurderes risikoen for forsyningssvikt å være størst for sjeldne jordarter (Figur 2.7).



Figur 2.7 Risiko for forsyningssvikt av kritiske råmaterialer til ni strategiske teknologier og tre sektorer i EU. Kilde: Reprodusert fra European Commission (2020a)

Tabell 2.1 Liste over kritiske råmateriale i EU innen ulike teknologiområder, samt hvilket land som er største produsent globalt. Kilde: European Commission (2020b)

Kritisk råmateriale	Teknologiområde			Største produsent globalt (andel i prosent)	EUs import-avhengighet (i prosent)[a]
	Elektronikk	Fornybar energi	Digitale teknologier		
Bauxitt	x	x	x	Australia (20 %)	87 %
Beryllium	x	x	x	USA (88 %)	n/a
Bismut	x		x	Kina (85 %)	100 %
Borat	x	x	x	Tyrkia (42 %)	100 %
Kobolt	x	x	x	DR Kongo (59 %)	86 %
Kokskull		x		Kina (55 %)	62 %
Gallium	x	x	x	Kina (80 %)	31 %
Germanium	x	x		Kina (80 %)	31 %
Hafnium	x	x	x	Frankrike (49 %)	0 %
Indium	x	x	x	Kina (48 %)	0 %
Litium	x	x	x	Chile (44 %)	100 %
Magnesium	x		x	Kina (80 %)	100 %
Naturlig grafitt	x	x	x	Kina (69 %)	98 %
Scandium		x		Kina (66 %)	100 %
Silisium	x	x		Kina (66 %)	63 %
Strontium	x			Spania (31 %)	0 %
Tantal	x	x	x	DR Kongo (33 %)	99 %
Titan	x			Kina (45 %)	100 %
Wolfram	x			Kina (69 %)	n/a
Vanadium		x		Kina (55 %)	n/a
Platinametaller	x	x		Sør-Afrika (84 %)	100 %
Tunge, sjeldne jordarter	x	x		Kina (86 %)	100 %
Lette, sjeldne jordarter	x	x		Kina (86 %)	100 %

[a] n/a betyr at importavhengigheten ikke kan beregnes; se European Commission (2020b) for detaljer

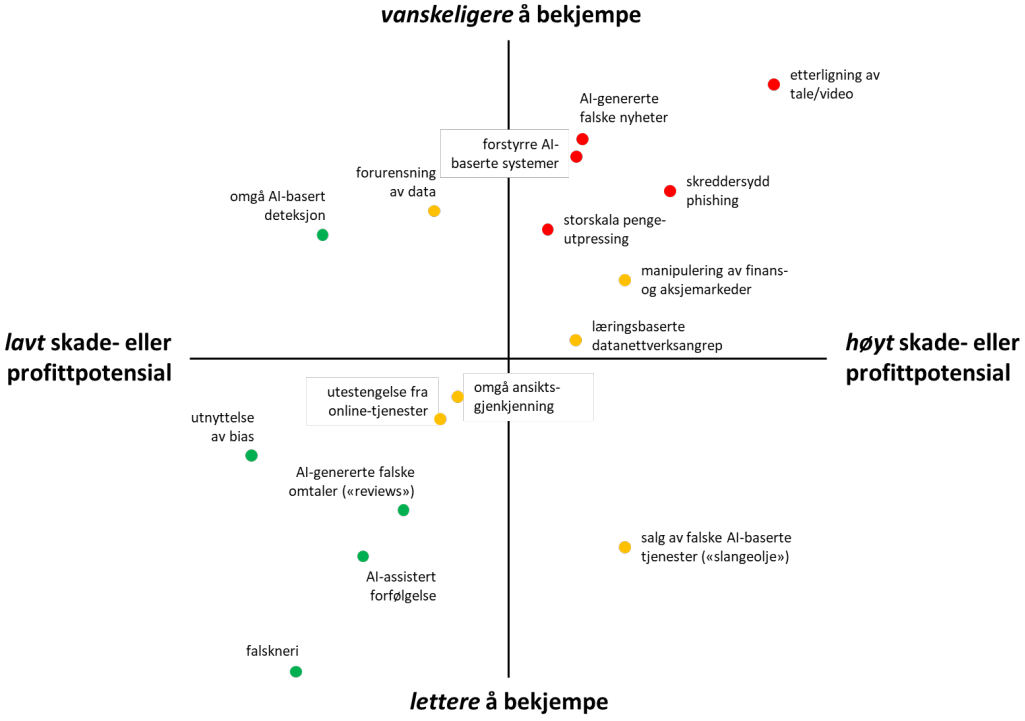
2.3 Kriminalitetsutvikling i det digitale rom

Teknologi, næringslivets selskapsstrukturer og den geopolitiske konteksten er viktige drivere for fremtidig utvikling innen organisert og annen alvorlig kriminalitet (Europol, 2017; Kripos, 2019; Sellevåg *et al.*, 2021, s. 84). Europol (2017) erfarer at spesielt organiserte kriminelle er raske med å ta i bruk ny teknologi, enten gjennom å endre *modus operandi* eller gjennom å endre deres «forretningsmodell».

Dette kommer særlig til uttrykk når det gjelder kriminalitet i det digitale rom, hvor teknologiutviklingen har vært sterkt drivende. Ikke minst gjelder dette fremvekst av såkalt «Crime-as-a-Service» (CaaS), hvor ulike nettverk tilbyr sine tjenester på det mørke nettet for å fasilitere annen kriminalitet gjennom utnyttelse av det digitale rom (Europol, 2020b; Kripos, 2023).

Kriminalitet i det digitale rom ansees som en global trend som har kommet for å bli (Maimon & Louderback, 2019). Kriminalitetsformen er kompleks av natur, noe som gjør den vanskelig å etterforske og straffeforfølge. I tillegg forsterkes utviklingen av kriminelles bruk av kryptovaluta og konfidensialitets- og anonymitetsløsninger for å opprettholde høy operasjonssikkerhet. Det digitale rom derfor et område hvor profesjonelle kriminelle kan operere med stor bevegelses- og handlefrihet (Sellevåg *et al.*, 2021, s. 86).

Bruken av løsepengevirus for å presse bedrifter for penger har utpekt seg som en økende trend de siste årene (Europol, 2020b, s. 32), og det vurderes som meget sannsynlig virksomheter med tilknytning til samfunnskritiske funksjoner vil rammes (Kripos, 2023, s. 48). Samtidig forventes det at kriminalitetsutviklingen i det digitale rom vil ta nye former, spesielt gjennom utnyttelse av kunstig intelligens. Bruk av kunstig intelligens for å etterligne tale/video, gjennomføre skreddersydd phishing og storskala pengeutpressing og laging av falske nyheter er kriminalitetsformer som er vurdert som både vanskelige å bekjempe og som har høyt skade- eller profittpotensial (Figur 2.8). Eksempelvis har Europol (2023) advart om at store språkmodeller som *ChatGPT* kan utnyttes av kriminelle.



Figur 2.8 Kvalitativ vurdering av vanskelighet med å bekjempe versus skade-/profittpotensialet til ulike former for kriminalitet basert på eller fasilitert av bruk av kunstig intelligens (AI). Kriminalitetsformer med høyest og lavest farepotensial er markert med henholdsvis rødt og grønt. Kilde: Caldwell et al. (2020).

2.4 Terrorisme i Vest-Europa

Boks 2.1 – Ulike former for voldelig ekstremisme (Europol, 2020a)

Jihadistisk terrorisme er en voldelig retning innen islamisme tuftet på væpnet kamp i form av hellig krig.

Høyreekstrem terrorisme er en voldelig retning med utspring i svært ytterliggående holdninger på den politiske høyresiden. Varianter innen høyreekstremisme er nynazisme, nyfascisme og ultranasjonalistiske grupperinger. Til forskjell fra høyreradikale som mener at demokratiet skal opprettholdes, mener høyreekstremister at demokratiet skal avvikles, universelle menneskerettigheter gjelder ikke og vold mot fiender av folkefellesskapet er legitimt (Bjørgo, 2018, s. 16-17).

Venstreekstrem terrorisme er en voldelig retning med utspring i politisk radikalisme som har utspring i ideologier som ligger til venstre for den parlamentariske sosialismen, ofte marxisme-leninisme.

Anarkistisk terrorisme er et samlebegrep for å beskrive terrorhandlinger begått av aktører med ulik anarkistisk ideologi og som fremmer en revolusjonær, antikapitalistisk og/eller antiautoritær agenda.

Etnonasjonalistisk og separatistisk terrorisme er et samlebegrep for aktører hvis voldshandlinger motiveres ut fra nasjonalisme, etnisitet og/eller religion. Grupperinger som den irske republikanske armé (IRA) og ETA – «Baskerland og frihet» hører innunder denne kategorien.

Ensaksterrorisme er et samlebegrep for aktører som benytter vold for å endre en spesifikk politikk eller praksis. Aktører innen denne kategorien har til nå gjerne vært voldelige dyrerettighetsekstremister, miljøekstremister eller antiabortekstremister.

2.4.1 Terrorisme i et historisk perspektiv

Fire overordnede utviklingstrekk knyttet til terrorisme i Vest-Europa siden 1970-tallet fremstår som tydelige (Johansen & Gråtrud, 2018, s. 24):

- Klar nedgang i statsstøttet terrorisme
- Religiøst motivert terrorisme har dominert trusselbildet de siste tjue årene
- Terrortrusselen har blitt mer transnasjonal

- Internasjonal terrorisme har blitt mer dødelig, spesielt jihadistisk terrorisme

Samtidig preges terroristers valg av angrepsmål og - i høy grad av kontinuitet (Johansen & Gråtrud, 2018; Sellevåg *et al.*, 2021). Sikkerhetsstyrker, sivilbefolkningen og nærings- eller myndighetsmål har vært de vanligste angrepsmålene, mens bombeangrep, bruk av skytevåpen eller bruk av hugg-/stikkvåpen har vært de mest brukte angrepsmetodene. Det har svært få hendelser med bruk av kjemiske, biologiske eller radioaktive stoffer i nyere tid i Vest-Europa. Storparten av terrorangrep skjer på land, mens det har vært en nedgang i antall terrorplott mot luftfarten de siste ti årene. Terrorangrep mot maritime mål er svært sjelden i Vest-Europa. Imidlertid har det vært en dreining fra sentralstyrte og komplekse terrorangrep med flere utøvere, til terrorangrep hvor det kun er én utøver under angrepet. Det har også vært en dreining mot bruk av kjøretøy og enkle hugg-/stikkvåpen.

2.4.2 Forventet fremtidig utvikling

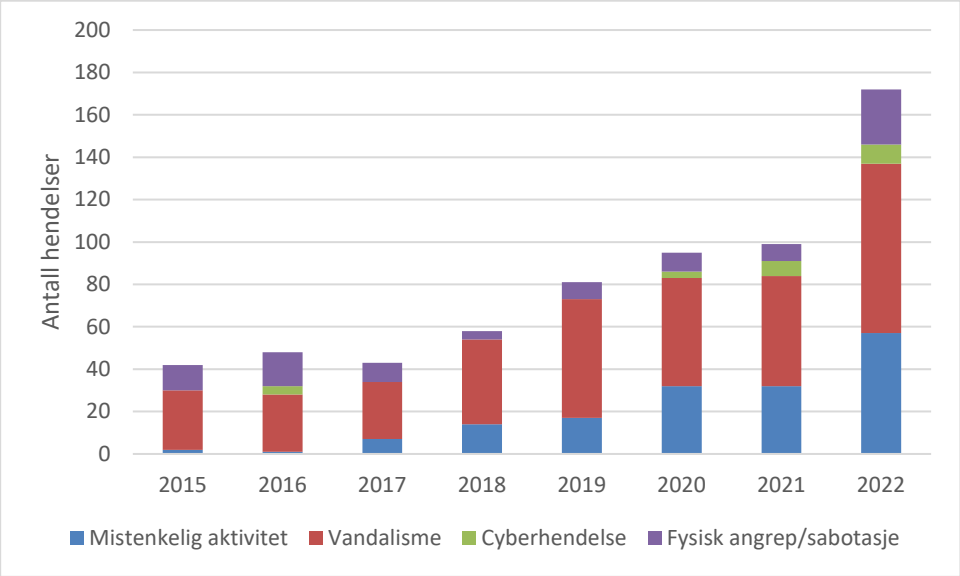
Historisk utvikling tilsier en betydelig grad av konsistens og stabilitet i terroraktørers angrepsmål og -metoder. Likevel er det stor usikkerhet knyttet til forventet fremtidig utvikling. Fremtidig konfliktutvikling, terroraktørers bruk av teknologi og internett, samt myndighetenes mottiltak mot terrorisme er viktige drivkrefter som kan påvirke utviklingen (Europol, 2020a; Johansen & Gråtrud, 2018; Nesser & Stenersen, 2014; Nesser *et al.*, 2016; Sellevåg *et al.*, 2021; Stenersen, 2017; Tønnessen, 2017).

Konflikter kan føre til radikalisering og bli en arena for trening og fremmedkrigervirksomhet. Oppslutningen om jihadistiske terrornettverk forventes å fortsette i regioner hvor konflikter vedvarer, Dette gjelder særlig i Midtøsten, Nord-Afrika og Sør-Asia. I tillegg har uttrekkingen av vestlige styrker ført til en mer usikker situasjon i Afghanistan. En negativ utvikling i disse regionene kan påvirke terrortrusselen mot Europa. Det forventes derfor at trusselen fra ekstreme islamister vil vedvare i tiden frem mot 2030 (Sellevåg *et al.*, 2021, s. 123). Ifølge PST (2023, s. 29) kan opplevde provokasjoner, krenkelser eller undertrykkelse av islam bidra til radikalisering og i verste fall motivere til terrorhandlinger i Norge.

Utviklingen innen høyreekstremisme har i økende grad blitt transnasjonal. Dette skyldes særlig spredning av konspirasjonsteorier og alternative virkelighetsoppfatninger på internett om at «den hvite rasen» er truet. Angrepet mot den amerikanske kongressbygningen 6. januar 2021 ansees av flere høyreekstreme i Europa som en forsmak på den kommende vestlige rasekrigen. På kort sikt knyttes det spesielt bekymring til høyreekstremister som eksplisitt oppfordrer til fysisk kamp og som tar til orde for å fremskynde en total kollaps av samfunnet ved hjelp av terror, såkalt akselerasjonisme (Sellevåg *et al.*, 2021, s. 124; se også boks 2.2). Økning i høyreekstremisme kan føre til fremvekst av venstreekstremisme. I sin nasjonale trusselvurdering for 2023 vurderer PST (2023, s. 34) at fiendebildet til norske høyreekstremister fremdeles særlig vil omfatte minoritetsgrupper og norske myndigheter fordi de mener at disse truer nasjonen, kulturen eller «rasens» overlevelse. Økofascisme inngår også i høyreekstremt tankegods (Campion, 2022; Kaati *et al.*, 2020).

Boks 2.3 – Vandalisme og angrep mot amerikansk kraftforsyning

De siste fem årene har amerikanske myndigheter sett en økning i vandalisme og fysiske angrep rettet mot kraftforsyningen (Figur 2.9). For mange av tilfellene er det så langt uklart hvem som står bak, men amerikanske myndigheter frykter at innenlands ekstremister i økende grad skal angripe kraftforsyningen (Bergenggruen, 2023). Nylig avdekket FBI at nynazister skal ha planlagt å ødelegge kraftnettet i Baltimore. En av personene som ble arrestert, dannet Atomwaffen Division som senere byttet navn til National Socialist Resistance Front. En del av denne gruppens strategi er å bruke terrorisme og vold for å fremskynde samfunnskollaps (Kagge, 2023).



Figur 2.9 Oversikt over utvalgte tilsiktede handlinger som har påvirket amerikansk kraftforsyning. Kilde: U. S. Department of Energy (u.å.)

Antistatlig ekstremisme er en overordnet beskrivelse for ideer og konspirasjonspregede teorier som inneholder et voldselement og hvor mistillit til styresmaktene er en forenende faktor (PST, 2023, s. 36). PST (2023) vurderer at fremmedstatlige aktører vil forsøke å påvirke antistatlige grupperinger gjennom spredning av desinformasjon. PST (2023) vurderer at det er lite sannsynlig at antistatlige ekstremister vil begå terrorhandlinger i Norge. De mest aktuelle målene for et eventuelt terrorangrep fra antistatlige ekstremister vil være mål som er knyttet til antistatlige kjernesaker og som er sentrale i dagsaktuelle konspirasjonsteorier. Kritisk infrastruktur og myndighetspersoner er eksempler på dette (PST, 2023, s. 36-37).

I nasjonal trusselvurdering for 2023 advarer PST om at klima-, miljø- og naturvernsaker har et potensial til å radikalisere. Dette er særlig knyttet til klimaendringer som kan oppfattes som en eksistensiell trussel, samt enkeltsaker knyttet til miljø- og naturvernsaker som kan skape et stort engasjement (PST, 2023, s. 39). PST (2023) vurderer det som svært lite sannsynlig at personer knyttet til klima -, miljø - og naturvern vil forøke og gjennomføre terrorhandlinger i Norge i 2023, men PST forventer økt aktivitet med bruk av ulovlige virkemidler som skadeverk og ordensforstyrrelser. PST advarer om at dette på sikt kan bidra til å radikalisere enkeltpersoner. Hvordan myndighetene velger å møte klimaaktivister som begår sivil ulydighet, vil også være en faktor som spiller inn. For harde mottiltak kan føre til radikalisering (Gayle *et al.*, 2023; Parker, 2014).

2.5 Trusler fra fremmedstatlige aktører

2.5.1 Stormaktsrivalisering og staters bruk av sammensatte trusler

Boks 2.3 – Sammensatte trusler

Norske myndigheter karakteriserer sammensatte trusler som (Meld. St. 9 (2022-2023), s. 9; Meld. St. 10 (2021-2022), s. 15):

«Sammensatte trusler er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt, som kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske, finansielle, etterretningsmessige og juridiske virkemidler for å nå strategiske målsettinger. Sammensatte trusler kan forekomme i sikkerhetspolitiske gråsoner, der formålet er å skape splid og destabilisering. Virkemiddelbruken kan være bredt distribuert og kombinere åpne, fordekte og skjulte metoder. Virkemiddelbruken kan være rettet mot konkrete aktiviteter eller situasjoner, eller være innrettet mer langsiktig for å skape tvil, undergrave tillit og ved dette svekke våre demokratiske verdier.»

Den sikkerhetspolitiske utviklingen har i lang tid vært preget av stormaktsrivalisering og bruk av sammensatte trusler (boks 2.3) for å utøve påvirkning og press. Bruken av sammensatte trusler kan sees på som et resultat av strategisk mulighet og av strategisk nødvendighet. Den strategiske muligheten oppstår som følge av økte gjensidige avhengigheter mellom ulike samfunnssektorer, hvor sårbarheter i avhengighetene kan utnyttes og manipuleres, mens den strategiske nødvendigheten følger av en innstramming av statlig handlefrihet og en vegring mot å ta høy økonomisk, militær eller diplomatisk risiko (Palmer, 2015, s. 2).

Russlands annektering av Krim i 2014 og invasjonen av Ukraina i 2022 har medført varige endringer i sikkerhetssituasjonen for Europa. Krigen i Ukraina har medført enorme menneskelige

lidelser og er den største bakkekrigen i Europa siden andre verdenskrig. Så langt har den vestlige responsen medført et styrket, men sårbart, vestlig sikkerhetsfellesskap og økte bevilgninger til forsvar (Skjelland *et al.*, 2023, s. 15-16). I tillegg ble Finland tatt opp som NATO-medlem 4. april 2023. Sverige ser i 2023 ut til å få sin NATO-søknad godkjent.

2.5.2 Et svekket og mer uforutsigbart Russland

Russland har de senere årene beveget seg i en autoritær retning, hvor Putin viser stor vilje til å ta politisk og militær risiko. Særlig har bruk av militærmakt blitt et viktigere virkemiddel i russisk utenrikspolitikk (Skjelland *et al.*, 2023, s. 17-18). Samtidig har Russlands krigføring i Ukraina avdekket store svakheter i Russlands militære evne uten at dette enn så lenge har ført til at Russland har endret sine overordnede strategiske målsettinger for krigen i Ukraina (Etterretningstjenesten, 2023).

Russlands stående militære landmakt har blitt vesentlig svekket som følge av krigen i Ukraina og forbruket av missiler har vært stort. Imidlertid er Russlands kjernefysiske kapasiteter de samme som før krigen, og luft- og sjøstyrkene er i hovedsak intakte (Etterretningstjenesten, 2023). Svekket konvensjonell militær evne medfører at kjernevåpen øker sin relative betydning. Kolahalvøya og Nordflåten får derfor en mer sentral plass i russisk sikkerhetspolitikk og forsvarsplanlegging (Etterretningstjenesten, 2023; Skjelland *et al.*, 2023, s. 19; Åtland, 2023).

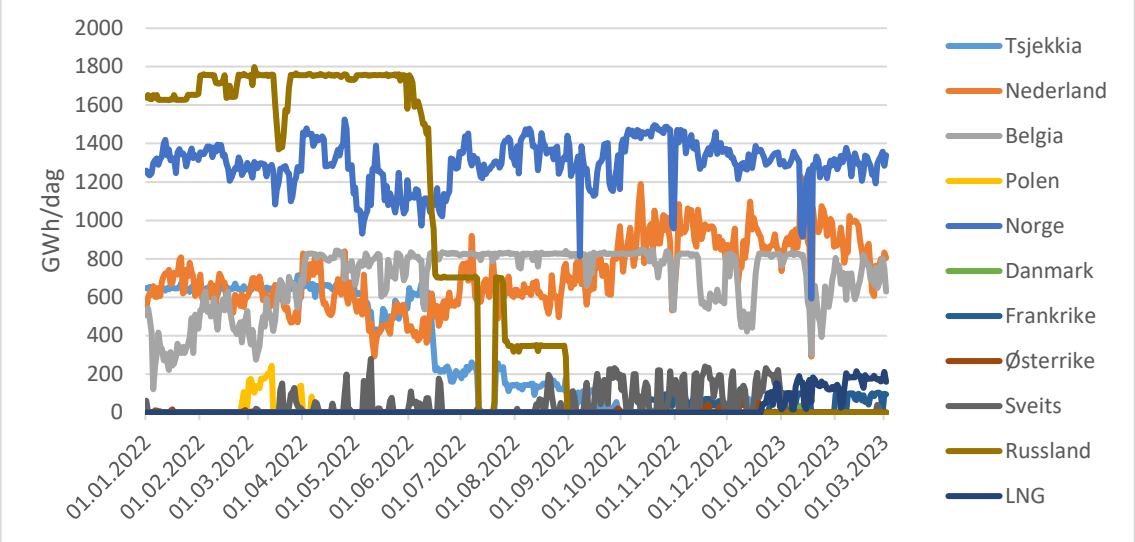
Etterretningstjenesten (2023) vurderer at det er fortsatt et russisk mål å svekke Vestens vilje til å støtte Ukraina, og presset mot Europas energiforsyning vil videreføres. Rask utfasing av russiske gassforsyninger har gjort Norge til Europas viktigste energileverandør (Figur 2.9). Dette sammen med nærheten til Kolahalvøya, har gjort at Norges geopolitiske rolle har økt. Selv om Norges rolle som energileverandør først og fremst er knyttet til gassleveranser, vil norsk evne til å levere gass være avhengig av pålitelig kraftforsyning. Denne avhengigheten vil øke med økt elektrifisering av petroleumssektoren.[2]

Økonomiske nedgangstider, demografisk utvikling og mangel på tilgang til vestlig teknologi vil gjøre det vanskelig for Russland å gjenoppbygge militærmakten selv om viljen er høy. Etterretningstjenesten (2023) vurderer at dette vil ta fem til ti år og at Russland i mellomtiden blir en mindre moderne, men fremdeles slagkraftig konvensjonell militærmakt. Etterretningstjenesten (2023) vurderer også at Russland vil forsøke å videreutvikle strategien om strategisk overfall. I et væpnet angrep mot Norge og NATO vil ødeleggelse av kritisk sivil infrastruktur få prioritet tidlig og varslingstiden vil være svært kort. Vi må også regne med at Russland vil fortsette å utvikle og benytte sammensatte trusler for å oppnå sine målsettinger under terskelen for væpnet konflikt (Skjelland *et al.*, 2023, s. 19).

På lengre sikt er den videre utviklingen i Russland mer usikker. Russland står overfor et uunngåelig makt- og generasjonsskifte det neste tiåret. Forskning viser at sammenbrudd av autoritære

[2] Elektrifisering av petroleumssektoren forventes å gi en økt kraftbruk på 6–10 TWh i et 2030-perspektiv (NOU 2023: 3, s. 77).

regimer er sjeldne hendelser (Wiig & Knutsen, 2022). Et autoritært regime erstattes derfor vanligvis med et nytt autoritært regime. Putins regime er et såkalt personalistisk regime (Wallander, 2021). Slike regimer overlever sjelden hvis øverste leder faller (Wiig & Knutsen, 2022). En mislykket maktoverføring kan føre til at Russland går i oppløsning. Etterretningstjenesten (2023) vurderer at Russland blir mer urolig og ustabilt fremover, og dermed en mer uforutsigbar nabo for Norge. Etterretningstjenesten vurderer også at det er svært lite som tyder på at Russland vil bevege seg i en mer demokratisk retning eller at Russlands interesser blir mer forenelige med Vestens i tiden frem mot 2030.



Figur 2.10 Tysk import av naturgass. Kilde: Bundesnetzagentur (2023)

2.5.3 Et fortsatt offensivt Kina

Kina har under Xi Jinpings ledelse beveget seg i en stadig mer autoritær retning. Nasjonal sikkerhet står sentralt i Kinas strategi, hvor hovedmålet er intern stabilitet og regimesikkerhet. I tillegg prioriteres nasjonal teknologiutvikling, selvforsyning og kulturell sikkerhet (Etterretningstjenesten, 2023).

Kina viderefører en offensiv utenrikspolitikk hvor målet om en regional og global lederposisjon og et mer Kina-orientert internasjonalt system består (Etterretningstjenesten, 2023). Etterretningstjenesten (2023) forventer også at spenningen rundt Taiwan vil tiltak.

Økonomisk styrke forblir Kinas viktigste maktmiddel. Etterretningstjenesten (2023) vurderer at silkeveistrategien forblir et viktig virkemiddel for å søke global innflytelse, og at strategien vil dreies ytterligere mot investeringer i digital infrastruktur og fornybar energi. Oppstartsbedrifter

og høyteknologibedrifter innen fornybar energi, maritim industri, elektriske kjøretøy, IKT, bioteknologi, kunstig intelligens og mikroelektronikk vil være av interesse for kinesiske investeringer. Samtidig styrker Kina sin militære evne i et hurtig tempo, hvor «informasjonsdominans» og «intelligent forsvar» vektlegges.

2.6 Usikkerhet i forventet fremtidig utvikling

Forventet fremtidig utvikling er nødvendigvis forbundet med usikkerhet. Det må derfor tas høyde for at trendbrudd og overraskelser kan skje. For å få en bedre forståelse av denne usikkerheten, er det tatt utgangspunkt i metoden «kreative kombinasjoner» (NATO, 2017, s. 53-55). Usikkerhet i dimensjonen «Fremtidig utvikling» beskrives gjennom verdiene «Dagens trend videreføres», «Dagens trend forsterkes», «Dagens trend svekkes» og «Joker».

2.6.1 Usikkerhet knyttet til mulige trusselaktører

En åpenbar kilde til usikkerhet er utviklingen knyttet til mulige trusselaktører. Med utgangspunkt i verdiene til dimensjonen «Fremtidig utvikling», er det fremsatt hypoteser om utviklingen innen dimensjonene «Russland», «Kina», «Terroraktører i Vest-Europa» og «Kriminelle aktører».

Hypoteser om fremtidig utvikling knyttet til mulige trusselaktører er gitt i Tabell 2.2. Hypotesene har tatt utgangspunkt i utviklingstrekkene som beskrives i det foregående. Hypotesene vurderes som relevante for scenarioer som kan true norsk kraftforsyning, men er ikke uttømmende for det fremtidige utfallsrommet. Hypotesene kan benyttes som et utgangspunkt for å beskrive mulige scenarioer som kan utspille seg.

2.6.2 Usikkerhet knyttet til andre samfunnsendringer

Usikkerhet i andre samfunnsendringer som ikke er direkte knyttet til mulige trusselaktører, vil også være av betydning. En åpenbar kilde til usikkerhet som vil ha betydning for norsk kraftforsyning, er hvor raskt energiomstillingen som følge av det grønne skiftet vil skje. En rask energiomstilling vil ha andre konsekvenser for kraftforsyningen sammenlignet med en situasjon hvor energiomstillingen tar lang tid eller bremser opp.

En annen faktor som er viktig for samfunnsutviklingen og norske myndigheters evne til å utvikle og gjennomføre politikk, er hvorvidt tillit i samfunnet opprettholdes på et høyt nivå. Høy tillit i samfunnet er ingen selvfølge og kan påvirkes av mange faktorer, så som ytringsfrihet, avstand mellom politikere og befolkningen, digitale rettigheter og økonomiske forskjeller (Kommunal- og moderniseringsdepartementet, 2019). Tilliten i samfunnet kan også undergraves av fremmedstatlige aktører (jf. boks 2.3). Faktorer som økonomisk og demografisk utvikling vil også være av betydning, men som en førsteordens tilnærming kan det antas at slike faktorer vil påvirke hvordan tilliten i samfunnet og energiomstillingen utvikler seg. Hypoteser om fremtidig utvikling knyttet til energiomstillingen og tillit i samfunnet er gitt i Tabell 2.3 og belyses nærmere i kapittel 5.

Tabell 2.2 Usikkerhet i forventet fremtidig utvikling knyttet til mulige trusselaktører i tiden frem mot 2030

Fremtidig utvikling	Russland	Kina	Terroraktører i Vest-Europa	Kriminelle aktører
Dagens trend videreføres	Regional stormakt med globale ambisjoner, men militært svekket på kort sikt som følge av Ukraina-krigen	Et offensivt Kina med globale interesser og økonomisk styrke som viktigste maktmiddel	Terrorangrep med enkle midler og som involverer få aktører	Stor bevegelses- og handlefrihet for kriminelle i det digitale rom
Dagens trend forsterkes	Styrket konvensjonell militærmakt og økte globale ambisjoner	Et mer Kina-orientert internasjonalt system	Terroraktører får styrket evne til å benytte teknologi. Jihadisme på fremmarsj som følge av krigen mellom Israel og Hamas på Gazastripen	«Crime-as-a-service» forsterkes
Dagens trend svekkes	Redusert konvensjonell militærmakt, men globale ambisjoner opprettholdes. Kjernevåpen og asymmetriske kapasiteter prioriteres	Økonomisk nedgangstid fører til tilbaketrekning og isolasjon	Høyreekstremisme på tilbakegang	Kriminalitet i det digitale rom reduseres
«Jokere»	Putin-regimet kollapser	Militær konfrontasjon med USA om Taiwan	Voldelige klima- og miljøaktivister	Nye kriminelle aktører etter Ukraina-krigen

Tabell 2.3 Usikkerhet i forventet fremtidig utvikling knyttet til energiomstilling og tillit i samfunnet i tiden frem mot 2030

Fremtidig utvikling	Energiomstilling	Tillit i samfunnet
Dagens trend videreføres	Elektrifisering av samfunnet pågår, men klimamålene for 2030 nås ikke	Høy tillit i samfunnet
Dagens trend forsterkes	Energiomstilling forsterkes for å nå klimamålene, etablering av ny industri og datasentre	Tillit i samfunnet styrkes som følge av trygg håndtering av persondata og ansvarlig bruk av kunstig intelligens
Dagens trend svekkes	Energiomstilling bremser opp pga. forsvars- og sikkerhetspolitikk og behov for å prioritere helse- og omsorgspolitikk	Tillit i samfunnet svekkes pga. økt politisk polarisering
«Jokere»	Rask utfasing av norsk olje- og gassindustri. Etablering av kjernekraft i Norge	Elitemotstand og økt avstand til politikere

3 Morfologisk analyse

Mulighetsrommet for scenarioer som kan true norsk kraftforsyning er stort og forbundet med betydelig grad av usikkerhet. Morfologisk analyse er en egnet metode å beskrive og strukturere dette mulighetsrommet, og for å håndtere usikkerheten på en sporbar og etterprøvbar måte (Ritchey, 2013a, 2013b; Zwicky, 1969). Metoden er derfor benyttet innen en rekke problemstillinger ved FFI (Bergaust & Sellevåg, 2023; Bjørgul *et al.*, 2022; Johansen, 2018; Johansen, 2022; Sellevåg, 2021; Waage *et al.*, 2021).

Morfologisk analyse er beskrevet i detalj i litteraturen (Ritchey, 2013a, 2013b; Zwicky, 1969). Kun en kort beskrivelse gis derfor her. Morfologisk analyse består av fem steg, hvor de tre første stegene utgjør analysefasen og de to siste stegene utgjør syntesefasen:

1. Problemet som skal løses må formuleres så presist som mulig.

2. Alle parametere som er av betydning for analyseproblemet må identifiseres og analyseres. Parameterne bør i størst mulig grad være uavhengige.

3. Konstruksjon av det *morfologiske rom* hvor hver parameter beskrives av et sett parameterverdier. Generelt bør verdiene være uttømmende for hvilken tilstand hver parameter kan ha.

4. Intern konsistensanalyse hvor logiske eller empirisk inkonsistente kombinasjoner av parameterverdier forkastes. Resultatet utgjør *løsningsrommet*.

5. Evaluering av foregående trinn (1–4) og kategorisering av løsninger.

Formulering av analyseproblemet og valg av parametere og parameterverdier er avgjørende for utfallet av analysen. Det er derfor viktig å forsøke å unngå tidlig kognitiv lukking i analysen (Beadle, 2016, s. 56-61).

3.1 Analysefase

Analyseproblemet for sikkerhetsutfordringer mot norsk kraftforsyning kan formuleres på følgende måte:

> *På hvilken måte kan utenlandske og/eller norske aktører oppnå sine målsetninger gjennom tilsiktede handlinger rettet mot norsk kraftforsyning i tiden frem mot 2030?*

Det forutsettes at Norge fortsetter å være medlem av NATO, EØS og Schengensamarbeidet, men ikke av EU i perioden frem mot 2030.

Valg av parametere er sentralt for beskrivelsen av mulighetsrommet for sikkerhetsutfordringer mot norsk kraftforsyning. Med utgangspunkt i Johansen (2022) og Bergaust og Sellevåg (2023), kan relevante parametere for mulighetsrommet identifiseres ut fra følgende spørsmål:

- Hvilke typer aktører kan utgjøre en sikkerhetsutfordring for Norges samfunnssikkerhet og nasjonale sikkerhetsinteresser?
- Hvilke overordnede målsettinger kan disse aktørene tenkes å handle ut fra?
- Hvilke verdier relatert til norsk kraftforsyning kan angripes for å oppnå disse målsettingene?
- Hvilke metoder kan trusselaktører benytte for å deres målsetninger?
- Hvilke virkemidler er nødvendige for å kunne benytte en gitt metode?
- Vil trusselaktøren forsøke å skjule sin identitet og/eller handlinger?

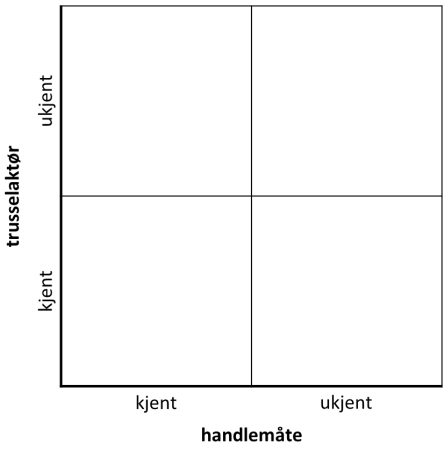
Dette gir følgende parametere:

- Trusselaktør
- Målsetting
- Angrepsmål
- Metode
- Virkemiddel
- Fordekthet

Når det gjelder valg av verdier for de ulike parameterne, er det viktig at parameterverdiene ikke er spesifikke for konkrete hendelser fordi dette kan medføre blindsoner i mulighetsrommet. Ved å gjøre parameterverdiene generiske, kan den «ukjente-ukjente» delen av mulighetsrommet utforskes (Figur 3.1). I det følgende diskuteres valg av parameterverdier.

3.1.1 Trusselaktør

Med *trusselaktør* menes både eksterne og interne aktører som kan tenkes å angripe verdier relatert til norsk kraftforsyning for å oppnå sine målsetninger. Valg av verdier for trusselaktør i dette arbeidet følger argumentasjonen til Bjørgul *et al.* (2022, s. 14-15). Vi vurderer det som usannsynlig at en koalisjon av fremmede stater vil ha en intensjon om å ramme norsk kraftforsyning på måter som kan true samfunnssikkerheten eller nasjonale sikkerhetsinteresser. Øverste parameterverdi er derfor *fremmedstatlig* trusselaktør, altså en trusselaktør som representerer eller er knyttet til en fremmed stat.



Figur 3.1 Mulighetsrommet for tilsiktede handlinger beskrevet som trusselaktør versus handlemåte

Også ikke-statlige trusselaktører kan tenkes å angripe verdier relatert til norsk kraftforsyning. Ikke-statlige trusselaktører er trusselaktører som ikke er

knyttet til en stat. Dersom en ikke-statlig aktør opererer på vegne av en statlig aktør, anses aktøren som statlig i dette arbeidet. Ikke-statlige aktører kan være alt fra en organisasjon/nettverk til enkeltindivider. Det er valgt å ikke spesifisere dette nærmere. Det er også valgt å ikke skille mellom norske og utenlandske ikke-statlige trusselaktører. I parameterverdien «ikke-statlige aktører» inngår både *politisk* motiverte ikke-statlige aktører og *kriminelle* ikke-statlige aktører. I dette arbeidet forstås politisk motiverte ikke-statlige trusselaktører som trusselaktører som begår politisk motivert vold eller straffbare handlinger med terrorhensikt. Videre forstås kriminelle ikke-statlige aktører som aktører som begår alvorlige kriminelle handlinger.

Parameteren «trusselaktør» er gitt følgende verdier:

- Fremmedstatlig
- Ikke-statlig

3.1.2 Målsetting

Det forutsettes at trusselaktører har et mål og en hensikt med sine tilsiktede handlinger mot norsk kraftforsyning.[3] Det kan være vanskelig å vite hvilke intensjoner trusselaktører har. Parameteren «målsetting» beskriver derfor hvilke overordnede målsettinger trusselaktørene kan tenkes å handle ut fra.

Øverste verdi for målsetting vil være *regimeendring* (Johansen, 2022, s. 27). Det er usannsynlig at opphevelse av norsk suverenitet kan skje utelukkende gjennom angrep mot kraftforsyningen. Vi forkaster derfor denne parameterverdien. Den neste parameterverdien som vurderes er *politisk omveltning* (Bjørgul *et al.*, 2022, s. 16); her forstått som politiske endringer som kan få store og langsiktige konsekvenser for Norge (eksempelvis at Norge melder seg ut av NATO). Det vurderes som usannsynlig at en trusselaktør vil lykkes med å oppnå politisk omveltning utelukkende gjennom angrep mot kraftforsyningen. Denne parameterverdien forkastes derfor også.

En mer begrenset målsetting er *endring av politikk*. Dette kan være endringer i enkeltsaker, endringer i en etablert politisk praksis eller krav om at politiske beslutninger ikke iverksettes. Slike saker kan eksempelvis være knyttet til nasjonale sikkerhetsinteresser og som berører det norske kraftsystemet, eller det kan være knyttet til norsk kraftutbygging. Denne parameterverdien er relevant for dette arbeidet og beholdes.

En annen målsetting kan være å oppnå *svekket norsk handlefrihet* (Bergaust & Sellevåg, 2023). Dette kan være relatert til tilgang på teknologi eller ressurser/innsatsfaktorer, oppnå en bedre forhandlingsposisjon eller legge grunnlaget for mer alvorlige handlinger.

En tredje målsetting kan være å *svekke tillit i samfunnet*, noe som ofte er et karakteristisk trekk ved fremmede staters bruk av sammensatte trusler (Bergaust & Sellevåg, 2023; Bjørgul *et al.*, 2022; Giannopoulos *et al.*, 2021). Undergraving av befolkningens tillit til myndigheter, gjøre

[3] Umotivert hærverk er utelatt fra scenariogrunnlaget.

befolkningen mer sårbar overfor konspirasjonsteorier eller forsterke polarisering i samfunnet er eksempler på handlinger som kan medføre svekket tillit i samfunnet.

Den siste målsettingen som inkluderes er *økonomisk vinning*. Dette er en målsetting som er karakteristisk for mange kriminelle aktører; særlig organiserte kriminelle nettverk. Legitime økonomiske interesser knyttet til næringsutvikling er utenfor tolkningen av parameterverdien.

Andre målsettinger som kan tenkes er *forsvare eget sosiale styresett*, *hevn* og *personlig tilfredsstillelse*. Det er imidlertid vanskelig å se for seg at det finnes trusselaktører med slike målsettinger og med tilstrekkelig kapasitet til at de kan gjennomføre handlinger mot norsk kraftforsyning som får konsekvenser for samfunnssikkerheten eller nasjonale sikkerhetsinteresser. Disse målsettingene forkastes derfor. Hærverk og vandalisme mot norsk kraftforsyning inngår derfor ikke i scenariogrunnlaget i denne rapporten.

Oppsummert er parameteren «målsetting» gitt følgende verdier:

- Endring av politikk
- Svekket handlefrihet
- Svekket tillit i samfunnet
- Økonomisk vinning

3.1.3 Angrepsmål

Parameteren «angrepsmål» beskriver hvilke verdier relatert til norsk kraftforsyning som kan angripes for å oppnå trusselaktørens målsettinger. Et åpenbart angrepsmål for dette arbeidet er *kraftsystemet*. Statnett (2018) beskriver kraftsystemet som «en samlebetegnelse for alle de komponentene som til sammen sørger for at kraft produseres og overføres fra for eksempel vannmagasinene, til de ulike kraftstasjonene og mellomlandsforbindelser og frem til deg». I dette arbeidet forstås derfor kraftsystemet som den cyber-fysiske infrastrukturen som sørger for kraftforsyning.

Et annet åpenbart angrepsmål er *virksomheter* som bidrar til produksjon, overføring, omsetning og fordeling av kraft, samt deres leverandører og underleverandører. Virksomheter som Statnett, Statkraft og Nord Pool inngår i denne parameterverdien, hvor Statnett har systemansvaret for kraftsystemet. Kraftkrevende industri er utelatt fra parameterverdien.

Et tredje angrepsmål er *myndigheter* med ansvar for norsk kraftforsyning. Dette gjelder Olje- og energidepartementet (OED) som har det overordnede ansvaret for norsk kraftforsyning, Norges vassdrags- og energiverk (NVE) som har det operative ansvaret for kraftforsyningsberedskapen, og Reguleringsmyndigheten for energi (RME) som regulerer nettselskapene og de fysiske kraftmarkedene. Andre myndigheter er utelatt fra parameterverdien.

Den siste parameterverdien som inkluderes er *befolkningen*. Vi inkluderer denne parameterverdien fordi befolkningens holdninger og adferd knyttet til kraftforsyning kan påvirkes av trusselaktører.

Oppsummert er parameteren «angrepsmål» gitt følgende verdier:

- Kraftsystemet
- Virksomheter
- Myndigheter
- Befolkningen

3.1.4 Metode

Med parameteren «metode» menes plan for handling som trusselaktøren benytter for å nå sine målsettinger, for eksempel gjennom å utnytte sårbarheter til ulike angrepsmål. Valg av metoder tar utgangspunkt i arbeidet til Bergaust og Sellevåg (2023). Her benyttes metodene *påvirke*, *presse* og *skade* for å indikere en eskalering i metodebruk. «Påvirke» beskriver metoder som forsøker å endre motstanderens holdninger og adferd, «presse» er metoder som forsøker å destabilisere en motstander eller tvinge motstanderen til å gjøre noe den ellers ikke ville ha gjort, mens «skade» beskriver metoder som forårsaker fysiske skader og ødeleggelser (Bergaust & Sellevåg, 2023). I tillegg inkluderes også metoden «stjele» for å beskrive tilsiktede handlinger som har som målsetting å frarøve motstanderen verdier.

En metode som er vurdert, men forkastet, er *krigføring*; her forstått som krigføring med regulære militære styrker. Parameterverdien er forkastet fordi den vil ikke tilføre noe ekstra til mulighetsrommet enn hva «skade» vil gjøre (militær krigføring mot kraftforsyningen vil også forårsake fysiske skader og ødeleggelser).

Oppsummert er parameteren «metode» gitt følgende verdier:

- Skade
- Presse
- Påvirke
- Stjele

3.1.5 Virkemiddel

For å kunne gjennomføre en metode for å nå et mål, må aktøren benytte et *virkemiddel*. Valg av parameterverdier har tatt utgangspunkt i forståelse av virkemidler som kan benyttes i forbindelse med sammensatte trusler (Bergaust & Sellevåg, 2023; Cullen & Reichborn-Kjennerud, 2017; Giannopoulos *et al.*, 2021). Dette gir følgende parameterverdier for «virkemiddel»:

- Militære
- Fysiske
- Politiske
- Økonomiske
- Juridiske
- Informasjon
- Cyber

Beskrivelsen av virkemidlene er basert på Bergaust og Sellevåg (2023). Kun noen få detaljer gis derfor her. *Militære* virkemidler beskriver kapabiliteter som militære styrker besitter.[4] *Fysiske* virkemidler er våpentyper og andre fysiske virkemidler som er tilgjengelige for ikke-statlige trusselaktører eller stedfortredere for fremmedstatlige trusselaktører. *Politiske* virkemidler er knyttet til offentlig beslutningsvirksomhet og kan være diplomati, forhandlinger eller uttrykke støtte til ytterliggående grupperinger eller protestbevegelser. *Økonomiske* virkemidler kan være virkemidler som benyttes i forbindelse med økonomisk statshåndverk (Lindgren *et al.*, 2022; Waage *et al.*, 2021; Waage *et al.*, 2022) eller det kan være knyttet til ikke-statlige aktørers bruk av korrupsjon eller andre former for økonomisk kriminalitet. *Juridiske* virkemidler kan være utnyttelse av juridiske smutthull eller overbelaste myndigheter/rettsapparatet med juridiske krav. *Informasjon* beskriver bruk av informasjon[5] som virkemiddel for å utnytte eller manipulere informasjonsmiljøet,[6] mens *cyber* beskriver dataangrep og offensive cyberoperasjoner mot informasjons- og kommunikasjonsnettverk, samt industrielle kontrollsystemer.[7]

3.1.6 Fordekthet

Parameteren «fordekthet» beskriver om trusselaktøren vil forsøke å skjule sin identitet og/eller handlinger. Parameteren er gitt følgende verdier:

- Åpent
- Fordekt

Parameterverdien «fordekt» beskriver både handlinger hvor trusselaktøren skjuler sin identitet og hvor effekten av handlingen er skjult («hemmelige operasjoner»), og handlinger hvor effekten av handlingen er synlig, men hvor trusselaktøren sin identitet er skjult eller hvor trusselaktøren kan påberope seg plausibel fornektbarhet (se Bergaust og Sellevåg (2023) for en nærmere diskusjon rundt «fordekthet»).

Samlet gir dette det morfologiske rommet som er gitt i Tabell 3.1. Til sammen inneholder det morfologiske rommet 1 792 mulige løsninger.

[4] Militære virkemidler beskriver militære kapabiliteter i land-, sjø-, luft- og romdomenet. Militære kapabiliteter i cyberdomenet er inkludert i parameterverdien «cyber».
[5] Informasjonen kan være falsk eller skadelig (Wardle & Derakhshan, 2017, s. 6).
[6] Informasjonsmiljøet omfatter totaliteten av enkeltpersoner, organisasjoner og systemer som samler inn, behandler, sprer eller handler etter informasjon (National Institute of Standards and Technology, 2022).
[7] Inkluderer også offensive cyberoperasjoner utført av fremmedstatlige etterretnings- og sikkerhetstjenester.

Tabell 3.1 Morfologisk rom for tilsiktede handlinger mot norsk kraftforsyning i tiden frem mot 2030

Trusselaktør	Målsetning	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmedstatlig	Endring av politikk	Kraftsystemet	Skade	Militære	Åpent
Ikke-statlig	Svekke handlefrihet	Virksomheter	Presse	Fysiske	Fordekt
	Svekke tillit i samfunnet	Myndigheter	Påvirke	Politiske	
	Økonomisk vinning	Befolkningen	Stjele	Økonomiske	
				Juridiske	
				Informasjon	
				Cyber	

3.2 Syntesefase

I syntesefasen av den morfologiske analysen fjernes inkonsistente kombinasjoner av parameterverdier. Dette gjøres ved å stille spørsmålet: «Kan verdi *X* og verdi *Y* opptre samtidig?» Svaret på spørsmålet kan finnes ut fra logiske og empiriske vurderinger (Ritchey, 2013a). Logiske inkonsistenser oppstår når parkombinasjonen er selvmotsigende, mens empirisk inkonsistens oppstår når parkombinasjonen ikke er relevant for analyseproblemet eller at parkombinasjonen er svært lite sannsynlig. Imidlertid er det verdt å merke seg at det gjøres ingen vurderinger av *hvor* sannsynlig det er at *X* og *Y* opptrer samtidig, hvis *X* og *Y* er vurdert som en konsistent kombinasjon. Gjennom dette forsøker vi å unngå å sammenblande det ukjente med det usannsynlige, som er en vanlig kognitiv feilslutning (Beadle, 2016).

Konsistensanalysen er oppsummert i Tabell 3.2. Diskusjonen av parkombinasjoner er avgrenset til diskusjon av parkombinasjoner som er mest betydningsfulle eller hvor konsistensanalysen ikke er åpenbar.

3.2.1 Logisk inkonsistente parkombinasjoner

I dette arbeidet er metoden «skade» forbundet med tilsiktede handlinger som har til potensial å forårsake direkte fysisk skade eller ødeleggelser. Dette gjør at det er bare virkemidlene «militære», «fysiske» og «cyber» som er parvis konsistente med «skade». Videre er dette arbeidet avgrenset til fysisk skade eller ødeleggelser på kraftsystemet. Tilsiktede handlinger som forvolder direkte fysisk skade på myndigheter, virksomheter eller befolkningen er utelatt fordi det antas at dette ikke vil få konsekvenser for forsyningssikkerheten av kraft.

Videre legger vi til grunn at politikk er knyttet til offentlig beslutningsvirksomhet (Thorsen, 2023). Politikk er derfor noe som skjer åpent og det er et virkemiddel som bare er konsistent med fremmedstatlige aktører (i dette arbeidet).

3.2.2 Fremmedstatlige aktørers målsettinger og virkemidler

Vi legger til grunn at fremmedstatlige aktører kan benytte alle statens virkemidler for å ramme norsk kraftforsyning, også militære virkemidler, hvis de har intensjon om dette. Vi legger også til grunn at fremmedstatlige aktører kan ha som målsetting å endre norsk politikk, svekke norsk handlefrihet og/eller svekke tillit i samfunnet; de to sistnevnte er gjerne knyttet til fremmede staters bruk av sammensatte trusler (Bergaust & Sellevåg, 2023; Bjørgul *et al.*, 2022; Johansen, 2022).

En mindre åpenbar vurdering er hvorvidt fremmedstatlige aktører har *økonomisk vinning* som målsetting. Et kjent eksempel på fremmedstatlige aktører som har økonomisk vinning som målsetting, er nordkoreanske cyberkriminelle grupper. Amerikanske myndigheter har attribuert gruppene «Lazarus Group», «Bluenoroff» og «Andariel» til å være underlagt eller kontrollert av nordkoreanske myndigheter. Deler av aktiviteten til disse gruppene har vært tyverier for å skaffe finansiering til blant annet det nordkoreanske kjernevåpenprogrammet (U.S. Department of the

Treasury, 2019). Kripos (2023) og PST (2023) vurderer også at fremmede etterretningstjenesters egne digitale trusselaktører har vinningskriminalitet som mål. Parkombinasjonen *fremmedstatlig–økonomisk vinning* vurderes derfor som empirisk konsistent.

Tabell 3.2 Konsistensmatrise hvor inkonsistente parkombinasjoner er markert med «X»

	Fremmedstatlig	Ikke-statlig	Endring av politikk	Svekke handlefrihet	Svekke tillit i samfunnet	Økonomisk vinning	Kraftsystemet	Virksomheter	Myndigheter	Befolkningen	Skade	Presse	Påvirke	Stjele	Militære	Fysiske	Politiske	Økonomiske	Juridiske	Informasjon	Cyber	Åpent	Fordekt
Fremmedstatlig																							
Ikke-statlig																							
Endring av politikk																							
Svekke handlefrihet		x																					
Svekke tillit i samfunnet																							
Økonomisk vinning																							
Kraftsystemet			x			x																	
Virksomheter			x																				
Myndigheter																							
Befolkningen				x		x																	
Skade						x		x	x	x													
Presse							x			x													
Påvirke						x	x																
Stjele			x	x	x		x			x													
Militære		x			x	x		x	x	x				x									
Fysiske						x		x	x	x				x									
Politiske		x			x	x	x			x	x			x									
Økonomiske					x	x	x			x	x												
Juridiske		x				x	x			x	x			x									
Informasjon						x	x				x			x									
Cyber										x													
Åpent					x	x								x		x							
Fordekt																	x						

3.2.3 Ikke-statlige aktørers målsettinger og virkemidler

Ikke-statlige *kriminelle* aktørers handlinger er i dette arbeidet avgrenset til kriminalitet mot datasystemer og digital infrastruktur. Selv om også kraftbransjen kan bli gjenstand for økonomisk kriminalitet (Energi Norge, 2017), vurderes det som svært lite sannsynlig at dette kan føre til svekket forsyningssikkerhet i tiden frem mot 2030.

Når det gjelder ikke-statlige *politiske* aktører, vil målsettingen til slike aktører være endring av politikk. Det kan også tenkes at slike trusselaktører kan ha «svekket tillit i samfunnet» som målsetting. Vi kan imidlertid ikke identifisere noen ikke-statlige politiske aktører som kan ha intensjoner om eller kapasitet til å svekke norske myndigheters handlefrihet gjennom virkemiddelbruk som hovedsakelig er rettet mot norsk kraftforsyning i tiden frem mot 2030. Denne parkombinasjonen forkastes derfor. Ikke-statlige aktørers bruk av juridiske virkemidler mot virksomheter eller myndigheter knyttet til kraftforsyningen, vurderes å være innenfor demokratiets spilleregler. Parkombinasjonen *ikke-statlig–juridiske* forkastes også.

3.2.4 Angrepsmål for å svekke handlefrihet

Det vurderes som mulig at tilsiktede handlinger rettet mot myndigheter, kraftsystemet og virksomheter tilknyttet norsk kraftforsyning kan svekke norsk handlefrihet. En noe mindre åpenbar vurdering er hvorvidt norsk handlefrihet kan svekkes av tilsiktede handlinger rettet mot befolkningen. All den tid befolkningen ikke kan påvirke offentlig beslutningsvirksomhet direkte, vurderes parkombinasjonen *svekket handlefrihet–befolkningen* som empirisk inkonsistent.

3.2.5 Virkemidler for å svekke tillit i samfunnet

Bergaust og Sellevåg (2023) argumenterer for at det mangler empiri på at det er en direkte årsakssammenheng mellom fremmedstatlige aktørers bruk av militære, økonomiske eller politiske virkemidler, og svekket tillit i samfunnet i en annen stat. Disse parkombinasjonene vurderes derfor som empirisk inkonsistente.

3.2.6 Bruk av cyber: Kun fordekt eller også åpent?

Et spørsmål knyttet til dataangrep og offensive cyberoperasjoner er hvorvidt slike handlinger kan skje åpent eller om de utelukkende skjer fordekt. Offensive cyberoperasjoner deles gjerne inn i cyberoperasjoner med etterretningsformål og cyberoperasjoner med effektformål (Klepper *et al.*, 2022, s. 48). Offensive cyberoperasjoner med etterretningsformål vil utelukkende skje fordekt (PST, 2023). Når det gjelder avanserte offensive cyberoperasjoner med effektformål, krever slike operasjoner mye ressurser, kompetanse, etterretningsstøtte og forberedelsestid. Følgelig vil slike operasjoner også skje fordekt for at de skal lykkes. Alvorlig datakriminalitet vil også skje fordekt og det forventes at profesjonelle kriminelle vil fortsette å utnytte konfidensialitets- og anonymitetsløsninger (Sellevåg *et al.*, 2021, s. 86). Det digitale rom er derfor et område hvor avanserte trusselaktører kan operere med stor bevegelses- og handlefrihet.

Når det gjelder lite sofistikerte dataangrep som tjenestenektangrep mot nettsider og nettside-vandalisme, kan slike dataangrep i prinsippet skje åpent. Formålet med slike dataangrep kan være å få økt oppmerksomhet rundt trusselaktørens sak (NSM, 2022, s. 16). Begge parkombinasjoner beholdes derfor.

4 Kategorier av tilsiktede handlinger

Konsistensanalysen reduserer det teoretiske mulighetsrommet til 109 konsistente løsninger. Disse er gitt i vedlegg A og utgjør det som omtales som *løsningsrommet*. Det er innenfor dette løsningsrommet at mulige scenarioer for tilsiktede handlinger mot kraftforsyningen kan utspille seg slik problemet er beskrevet i denne rapporten.

Fellestrekk mellom konfigurasjonene gjør at de kan deles inn i meningsfulle kategorier som er en uttømmende og ikke-overlappende typologisk inndeling av løsningsrommet (Johansen, 2018; Johansen, 2022). Følgende kriterier legges til grunn for den typologiske inndelingen av løsningsrommet (Amer *et al.*, 2013):

- *Plausibilitet:* Det må være mulig eller plausibelt at løsningene innenfor kategoriene kan inntreffe
- *Konsistens:* Løsningene må være konsistente
- *Relevans:* Kategoriene må gi konkret innsikt om fremtiden som kan bidra til bedre beslutninger innenfor det aktuelle saksfeltet
- *Utfordring:* Kategoriene bør utfordre oppdragsgivers tankegang om fremtidige utfordringer
- *Differensiering:* Kategoriene bør representere kvalitativt ulike utfordringer

Kravene om plausibilitet, konsistens og relevans ivaretas gjennom formuleringen av analyseproblemet og den påfølgende morfologiske analysen. Fokus i det følgende er kriteriet om *differensiering*. Kriteriet om *utfordring* vil ivaretas i de konkrete scenarioene som utvikles på bakgrunn av kategoriene.

Følgende differensiering er benyttet:

- Trusler fra kriminelle aktører
- Trusler fra politisk motiverte ikke-statlige aktører
- Trusler fra fremmedstatlige aktører

I det følgende beskrives kategoriene som følger fra denne differensieringen.

4.1 Trusler fra kriminelle aktører

Trusler fra kriminelle aktører identifiseres ved å trekke ut konfigurasjoner med «økonomisk vinning» som målsetning fra løsningsrommet (Tabell- A.1). Disse konfigurasjonene utgjør kategorien som vi vil omtale som *datakriminalitet*, altså kriminalitet mot datasystemer (Tabell 4.1).

Scenarioer innenfor denne kategorien kan for eksempel inkludere datatyveri av kraftsensitiv informasjon, bruk av løsepengevirus, tjenestenektangrep eller ulike former for skadevare. Politiet (2023) vurderer løsepengevirus rettet mot virksomheter som den største kriminalitetstrusselen mot IKT-sikkerhet og digital infrastruktur. Politiet vurderer det som sannsynlig at virksomheter med samfunnskritiske funksjoner vil rammes av løsepengevirus, og at datakriminalitet motivert av Russlands krig i Ukraina vil fortsette. Politiet vurderer det også som sannsynlig at virksomheter med roller i kritiske samfunnsfunksjoner kan bli utsatt for datatyveri (Politiet, 2023, s. 9). Datakriminalitet er derfor en scenarioklasse som myndigheter og kraftbransjen må være forberedt på å håndtere.

Tabell 4.1 Forutsetninger for kategorien «Datakriminalitet» (markert med blått)

Trusselaktør	Målsetning	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmed-statlig	Endring av politikk	Kraftsystemet	Skade	Militære	Åpent
Ikke-statlig	Svekke handlefrihet	Virksomheter	Presse	Fysiske	Fordekt
	Svekke tillit i samfunnet	Myndigheter	Påvirke	Politiske	
	Økonomisk vinning	Befolkningen	Stjele	Økonomiske	
				Juridiske	
				Informasjon	
				Cyber	

4.2 Trusler fra politisk motiverte ikke-statlige aktører

Ulike former for aktivisme, fra demonstrasjoner til sivil ulydighet, fra ikke-statlige aktører som ikke opptrer fordekt og som skjer innenfor demokratiets spilleregler, er ikke en del av scenariogrunnlaget. Fokuset her er på ikke-statlige aktører som er villige til å bruke ekstreme handlinger for å nå sine politiske målsettinger. Trusler fra slike aktører identifiseres ved å trekke ut konfigurasjoner med «ikke-statlig» som parameterverdi for trusselaktør fra løsningsrommet (Tabell-A.1).

Spørsmålet som diskuteres her er hvorvidt utfordringen slike aktører representerer kan beskrives i én kategori eller om det er behov for å differensiere utfordringen i flere kategorier. Som utgangspunkt kan det trekkes et skille mellom voldelige og ikke-voldelige ekstremister. I denne

rapporten beskrives ikke-voldelige ekstremister som ikke-statlige aktører som er villige til å benytte fordekte og illegitime metoder utenfor demokratiets spilleregler, men som ikke tyr til voldshandlinger selv. Samtidig må man ta i betraktning at slike aktører kan akseptere bruk av vold selv om de ikke utfører voldshandlinger selv. Overgangen mellom voldelige og ikke-voldelige ekstremister er derfor glidende. I tillegg er det ikke slik at voldelige ekstremister kun bruker vold som virkemiddel; bruk av propaganda for å fremme sin sak kan være vel så viktig. Voldelige ekstremister kan også være avhengige av økonomiske virkemidler for å finansiere sine aktiviteter.

Det vurderes derfor at utfordringen som politisk motiverte ikke-statlige trusselaktører representerer, best beskrives som ulike scenarioer innenfor én kategori. Denne kategorien omtales som *ekstremisme* (Tabell 4.2). Eksempler på scenarioer som kan falle innunder denne kategorien og som kan være relevante for norsk kraftforsyning, er klimaaktivister eller klimamotstandere som bruker antidemokratiske virkemidler, økofascisme (Campion, 2022) eller ekstreme miljøvernere som ønsker å fjerne industrisamfunnet (LeVasseur, 2017).

Tabell 4.2 Forutsetninger for kategorien «Ekstremisme» (markert med blått)

Trusselaktør	Målsetning	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmed-statlig	Endring av politikk	Kraftsystemet	Skade	Militære	Åpent
Ikke-statlig	Svekke handlefrihet	Virksomheter	Presse	Fysiske	Fordekt
	Svekke tillit i samfunnet	Myndigheter	Påvirke	Politiske	
	Økonomisk vinning	Befolkningen	Stjele	Økonomiske	
				Juridiske	
				Informasjon	
				Cyber	

4.3 Trusler fra fremmedstatlige aktører

4.3.1 Tilsiktede handlinger under terskelen for direkte væpnet konflikt

Et fremtredende trekk ved trusler fra fremmedstatlige aktører under terskelen for direkte væpnet konflikt, er bruken av sammensatte trusler (jf. boks 2.3). I en rapport til Forsvarskommisjonen av 2021 som omhandler hva Norge kan lære av andre lands tilnærminger til sammensatte trusler, argumenterer Bergaust *et al.* (2022) for at det kan være utfordrende å utvikle politikk for å avskrekke, avdekke og håndtere sammensatte trusler når bruken av begrepet «ikke skiller mellom forskjellige typer aktiviteter, intensitetsnivå på innblandingen og alvorlighetsgrad» (s. 49). Bergaust *et al.* (2022) foreslår derfor å tydeliggjøre innholdet til begrepet «sammensatte trusler» gjennom å betrakte hva slags type aktiviteter det er som kan inngå.

En slik kategorisering av type aktiviteter som kan inngå i sammensatte trusler er foreslått av Bergaust og Sellevåg (2023). I dette arbeidet foreslås det at begrepet «sammensatte trusler» kan konseptualiseres i følgende kategorier:

- Tvangsdiplomati
- Maktposisjonering
- Fordekt tvang
- Sabotasje og likvidasjoner

Denne forståelsen benyttes også i dette arbeidet, men med to modifikasjoner. Den første modifikasjonen er at bruk av militære virkemidler ikke inngår i beskrivelsen av tvangsdiplomati i dette arbeidet. Dette skyldes at det er vanskelig å se for seg at det norske kraftsystemet og/eller kraftselskaper vil være det primære angrepsmålet for et tvangsdiplomati hvor militære virkemidler benyttes. Dog skal det sies at Norge som nasjon kan bli utsatt for tvangsdiplomati hvor militær styrkedemonstrasjon inngår (Johansen, 2022, s. 47). Slike situasjoner er det først og fremst regjeringen og Forsvaret som må håndtere, men kraftsektoren må være forberedt på forhøyet beredskap for å forhindre og håndtere scenarioer som involverer eksempelvis offensive cyberoperasjoner og/eller fysiske sabotasjehandlinger, som kan skje i en slik spent sikkerhetspolitisk situasjon. Den andre modifikasjonen fra kategoriseringen til Bergaust og Sellevåg (2023) er at likvidasjoner er utelatt. Dette skyldes at det er vanskelig å se for seg at fremmedstatlige aktører vil begå målrettede likvidasjoner av nøkkelpersoner i kraftsektoren under terskelen for direkte væpnet konflikt i tiden frem mot 2030 for å oppnå sine målsettinger. Kategorien «sabotasje og likvidasjoner» er derfor avgrenset til «sabotasje».

Samlet gir dette følgende kategorier for fremmedstatlige aktørers tilsiktede handlinger under terskelen for direkte væpnet konflikt:

- Tvangsdiplomati (Tabell 4.3)
- Maktposisjonering (Tabell 4.4)
- Fordekt tvang (Tabell 4.5)
- Sabotasje (Tabell 4.6)

Det henvises til Bergaust og Sellevåg (2023) for en mer inngående diskusjon av kategoriene. I denne rapport avgrenses diskusjonen til å beskrive kategoriene ved hjelp av eksempler. Tvangsdiplomati er en form for tvang som forsøker å få motstanderen til å endre politikk innenfor et saksfelt gjennom trusler om bruk av makt. Eksempler på tvangsdiplomati som er relevant i konteksten av dette arbeidet, er Kinas bruk av økonomisk makt og/eller diplomatiske sanksjoner (Forsby & Sverdrup-Thygeson, 2022).

Maktposisjonering tilsvarer på mange måter utøvelse av internasjonal politikk. Hovedforskjellen er at virkemiddelbruken gjøres fordekt (Bergaust & Sellevåg, 2023). Relevante eksempler for dette arbeidet kan være å skape splid i samfunnet gjennom bruk av påvirkningsoperasjoner for å øke politisk polarisering knyttet til kraftutbygging, eller bruk av utenlandske direkteinvesteringer i norske kraftselskaper.

Fordekt tvang representerer fordekte handlinger med forsterket grad av innblanding og alvorlighet sammenlignet med maktposisjonering. Fordekt tvang kan derfor, noe enkelt, sees på som en fordekt form for tvangsdiplomati. Relevante eksempler kan være manipulering av tilgang til teknologi eller innsatsfaktorer som sjeldne jordmetaller (Waage *et al.*, 2022, s. 52-54), eller bruk av offensive cyberoperasjoner.

Sabotasje representerer tilsiktede handlinger som kan forårsake fysisk skade og ødeleggelser (Bergaust & Sellevåg, 2023). Relevante eksempler her er fysisk sabotasje av komponenter i kraftsystemet eller bruk av offensive cyberoperasjoner med effektformål mot kraftsystemet. Under terskelen for direkte væpnet konflikt, vil slike scenarioer trolig skje som enkelthendelser. Hvis omfanget av sabotasjehandlinger mot kritisk infrastruktur blir stort, kan risikoen for eskalering til direkte væpnet konflikt øke.

Et spørsmål som kan reise seg er hva som skiller offensive cyberoperasjoner i kategorien «fordekt tvang» fra cyberoperasjoner i kategorien «sabotasje». Det er ikke noen enkle svar på dette, men et skille kan være omfanget og intensiteten til cyberoperasjonene som utføres. Et annet skille kan være cyberoperasjoner som forårsaker at digitale verdier i IT-systemer blir utilgjengeliggjort, forringet eller gjort verdiløse ved ødeleggelse, versus cyberoperasjoner som forårsaker skadeverk i industrielle kontrollsystemer/operasjonell teknologi (OT). Kjente eksempler på det siste er *Stuxnet* (Langner, 2013) og angrepene mot kraftforsyningen i Ukraina i 2015 og 2016 (Cherepanov & Lipovsky, 2016; Lipovsky *et al.*, 2017).

Tabell 4.3 Forutsetninger for kategorien «Tvangsdiplomati» (markert med blått)

Trusselaktør	Målsetning	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmedstatlig	Endring av politikk	Kraftsystemet	Skade	Militære	Åpent
Ikke-statlig	Svekke handlefrihet	Virksomheter	Presse	Fysiske	Fordekt
	Svekke tillit i samfunnet	Myndigheter	Påvirke	Politiske	
	Økonomisk vinning	Befolkningen	Stjele	Økonomiske	
				Juridiske	
				Informasjon	
				Cyber	

Tabell 4.4 Forutsetninger for kategorien «Maktposisjonering» (markert med blått)

Trusselaktør	Målsetning	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmedstatlig	Endring av politikk	Kraftsystemet	Skade	Militære	Åpent
Ikke-statlig	Svekke handlefrihet	Virksomheter	Presse	Fysiske	Fordekt
	Svekke tillit i samfunnet	Myndigheter	Påvirke	Politiske	
	Økonomisk vinning	Befolkningen	Stjele	Økonomiske	
				Juridiske	
				Informasjon	
				Cyber	

Tabell 4.5 Forutsetninger for kategorien «Fordekt tvang» (markert med blått)

Trusselaktør	Målsetning	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmedstatlig	Endring av politikk	Kraftsystemet	Skade	Militære	Åpent
Ikke-statlig	Svekke handlefrihet	Virksomheter	Presse	Fysiske	Fordekt
	Svekke tillit i samfunnet	Myndigheter	Påvirke	Politiske	
	Økonomisk vinning	Befolkningen	Stjele	Økonomiske	
				Juridiske	
				Informasjon	
				Cyber	

Tabell 4.6 Forutsetninger for kategorien «Sabotasje» (markert med blått)

Trusselaktør	Målsetning	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmedstatlig	Endring av politikk	Kraftsystemet	Skade	Militære	Åpent
Ikke-statlig	Svekke handlefrihet	Virksomheter	Presse	Fysiske	Fordekt
	Svekke tillit i samfunnet	Myndigheter	Påvirke	Politiske	
	Økonomisk vinning	Befolkningen	Stjele	Økonomiske	
				Juridiske	
				Informasjon	
				Cyber	

4.3.2 Væpnet angrep

Løsningsrommet (Tabell A.1) inneholder også åpen og fordekt bruk av militære virkemidler. I denne rapporten vil vi omtale slike tilsiktede handlinger som *væpnet angrep* (Tabell 4.7). Denne kategorien representerer de mest alvorlige tilsiktede handlingene mot Norge.

Det har ikke vært denne rapportens intensjon å beskrive scenarioer for væpnede angrep mot Norge. Kategorien «væpnet angrep» sier derfor ikke noe om hvor stort det væpnede angrepet på Norge er eller noe om dets karakter; kun at norsk kraftforsyning kan rammes i slike scenarioer. For å få mer innsikt i hvordan et væpnet angrep på Norge kan utspille seg, støtter vi oss på FFIs scenariogrunnlag som benyttes til støtte for forsvarsplanlegging. I dette scenariogrunnlaget beskrives tre scenarioklasser for væpnet angrep mot Norge (Johansen, 2022):

- Strategisk overfall
- Begrenset angrep
- Ukonvensjonell krigføring

Tabell 4.7 Forutsetninger for kategorien «Væpnet angrep» (markert med blått)

Trusselaktør	Målsetning	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmed-statlig	Endring av politikk	Kraftsystemet	Skade	Militære	Åpent
Ikke-statlig	Svekke handlefrihet	Virksomheter	Presse	Fysiske	Fordekt
	Svekke tillit i samfunnet	Myndigheter	Påvirke	Politiske	
	Økonomisk vinning	Befolkningen	Stjele	Økonomiske	
				Juridiske	
				Informasjon	
				Cyber	

Strategisk overfall

Ifølge Johansen (2022, s. 41), representerer strategisk overfall en situasjon hvor:

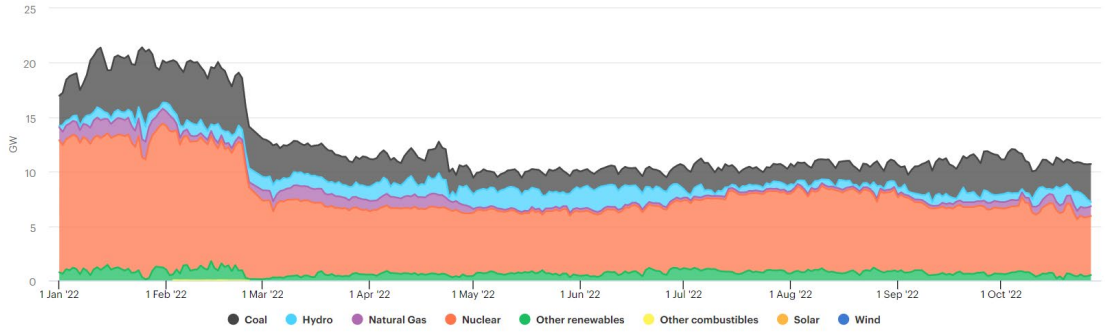
> *[…] en stat setter inn store militære styrker med sikte på å etablere militær kontroll over en del av norsk territorium, typisk en landsdel. Formålet med angrepet kan være å tvinge frem en bestemt løsning i et konkret politisk stridsspørsmål, eller det kan mer generelt ta sikte på å styrke angriperens strategiske stilling i en konflikt med andre aktører.*

I overskuelig fremtid vurderes Russland som den eneste staten som både har intensjon og kapasitet til å gjennomføre et konvensjonelt væpnet angrep mot Norge (Johansen, 2022, s. 41). Samtidig er den konvensjonelle militærmakten til Russland underlegen NATOs. En omfattende styrkeoppbygging på russisk side mot Norge vil derfor oppdages og kunne utløse overføring av allierte forsterkningsstyrker til Norge. Dette kan avskrekke russisk aggresjon.

Ifølge Etterretningstjenesten (2023), er hurtige forkjøpsangrep med mål om å slå ut kritiske mål langt inne på fiendens territorium et sentralt aspekt i russisk militærdoktrine. Russlands mest realistiske handlemåte i et strategisk overfall er derfor å gjennomføre et overraskende angrep med minimale synlige angrepsforberedelser hvor hovedsakelig regionalt tilgjengelige styrker med korte oppsettingstider benyttes (Johansen, 2022, s. 42). Etterretningstjenesten (2023) vurderer også at angrep mot kritisk sivil infrastruktur vil få prioritet tidlig i et væpnet angrep på Norge og varslingstiden vil være kort. Erfaringer fra Ukraina viser at Russland angriper kraftforsyningen på en målrettet og metodisk måte med langtrekkende presisjonsstyrte missiler (Brunbaum *et al.*, 2022; Lister *et al.*, 2022; Santora *et al.*, 2022; UNDP, 2023). Britisk etterretning vurderer at dette gjøres som en del av Russlands såkalte SODCIT-strategi[8] (Santora *et al.*, 2022; UK Ministry of Defence [@DefenceHQ], 2022). Formålet med SODCIT er å gjennomføre strategiske operasjoner mot kritisk sivil infrastruktur for å oppnå materiell skade og påvirke forsvarsviljen i befolkningen og blant den politiske ledelsen (Kofman *et al.*, 2021, s. 69; McDermott & Bukkvoll, 2018, s. 203). Samtidig vurderer Politiets sikkerhetstjeneste at Russland allerede har kartlagt veldig mye av den kritiske infrastrukturen i Norge (Foss & Olsen, 2022). Det må derfor tas høyde for at Russland kan forsøke å slå ut norsk kraftforsyning i en tidlig fase av et strategisk overfall ved hjelp av målrettede angrep med langtrekkende presisjonsstyrte missiler. Slike missilangrep kan få store og langvarige konsekvenser for kraftforsyningen slik man har sett i Ukraina (Figur 4.1 og Figur 4.2).

Figur 4.1 Reduksjon i elektrisitetsforbruk (GW) i Ukraina siden Russlands invasjon 24. februar 2022. Kilde: Reprodusert fra IEA (2022a) under CC BY 4.0-lisens

[8] SODCIT: «Strategic Operation for the Destruction of Critically Important Targets» (se Kofman *et al.*, 2021, med tilhørende referanser).



Figur 4.2 Reduksjon i kraftproduksjon (GW) i Ukraina siden Russlands invasjon 24. februar 2022. Kilde: Reprodusert fra IEA (2022a) under CC BY 4.0-lisens

Begrenset angrep

Johansen (2022, s. 44-45) beskriver også en klasse av scenarioer som omfatter militære angrep mot Norge, men som krever mindre militær innsats enn et strategisk overfall. Dette er omtalt som *begrenset angrep*. I denne scenarioklassen vil de militære angrepene ha en klarere avgrensning i både rom og tid sammenlignet med strategisk overfall. Et begrenset militært angrep mot norsk energiforsyning til Europa som et resultat av en regional konflikt mellom NATO og Russland, kan inngå i denne scenarioklassen.

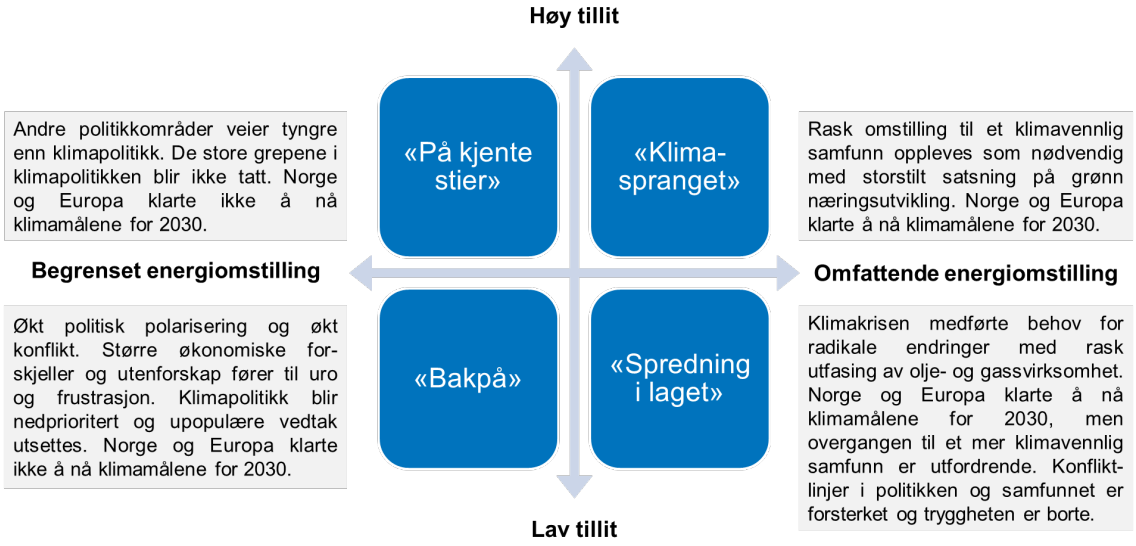
Ukonvensjonell krigføring

Ukonvensjonell krigføring beskrives av Johansen (2022, s. 46) som en type maktbruk hvor en stat benytter irregulære styrker, agenter («proxy»), spesialstyrker eller organiserte sivile (f.eks. privat-militære selskaper) for å gjennomføre militære eller hybride[9] operasjoner på en fordekt eller ikke-attribuerbar måte. Mindre angrep mot sivile mål som fysiske objekter eller infrastruktur kan inngå i denne scenarioklassen.

[9] Hybride operasjoner i konteksten av ukonvensjonell krigføring er operasjoner hvor militære virkemidler benyttes i kombinasjon med ikke-militære midler og metoder (Johansen, 2022, s. 46).

5 Fremtidsbilder

Hvilke konkrete scenarioer som utspiller seg vil avhenge av hvordan samfunnet utvikler seg fremover. For å få en bedre forståelse av hvilke «fremtidsbilder»[10] som kan oppstå som følge av samfunnsendringer, er 2 × 2 scenariomatriseteknikken (Government Office for Science, 2017) benyttet. Usikkerhetsaksene som er valgt, er «tillit i samfunnet» og «energiomstilling» som ble diskutert i kapittel 2.6.2. Vurderingene av de alternative fremtidene har tatt utgangspunkt i «Scenarioer for offentlig sektor i 2040» (Kommunal- og moderniseringsdepartementet, 2019).



Figur 4.1 Alternative fremtider som kan oppstå som følge av usikkerhet knyttet til tillit i samfunnet og energiomstilling

Dette gir følgende alternative fremtider (Figur 4.3):

- **«På kjente stier»:** I dette fremtidsbildet er det fortsatt høy tillit i samfunnet og demokratiet står sterkt i Norge. Olje- og gassvirksomhet er fremdeles en motor i norsk økonomi, men Norge innstiller seg på at aktiviteten skal avta. De økonomiske forskjellene i samfunnet har økt, men er fremdeles små. Andre politikkområder ble prioritert foran klimapolitikk. De store grepene i klimapolitikken blir ikke tatt. Norge og Europa klarte ikke å nå klimamålene for 2030, men opprettholder klimaambisjonene for 2050.

[10] Det er valgt å bruke begrepet «fremtidsbilder» fremfor «scenarioer» for å tydeliggjøre at det er knyttet til samfunnsendringer og ikke trusselaktørers tilsiktede handlinger.

- **«Bakpå»:** I dette fremtidsbildet er tillit i samfunnet svekket som følge av økt politisk polarisering og økt konflikt. Redusert økonomisk vekst har ført til større forskjeller og utenforskap som igjen førte til uro og frustrasjon. Klimapolitikk har blitt nedprioritert og upopulære vedtak utsettes. Norge og Europa klarte ikke å nå klimamålene for 2030 og har ingen gjennomførbare planer for å nå klimamålene for 2050. Konsekvenser av klimaendringer fungerer som trusselmultiplikator.

- **«Klimaspranget»:** I dette fremtidsbildet er det høy tillit i samfunnet som følge av at store samfunnsutfordringer tas tak i. Rask omstilling til et klimavennlig samfunn oppleves som nødvendig, med storstilt satsning på grønn næringsutvikling. Eksperimentering og bruk av ny teknologi skjer offensivt. Norge og Europa klarte å nå klimamålene for 2030 og har gjennomførbare planer for å nå klimamålene for 2050.

- **«Spredning i laget»:** I dette fremtidsbildet har tilliten i samfunnet blitt svekket. Klimakrisen medførte behov for radiale endringer med rask utfasing av norsk olje- og gassvirksomhet. Norge og Europa klarte å nå klimamålene for 2030, men overgangen til et mer klimavennlig samfunn er utfordrende og grønn næringsutvikling går sakte. Konfliktlinjer i politikken og samfunnet forsterkes som følge av at noen løp foran og tok seg til rette, mens andre aldri kom etter. Økt arbeidsløshet som følge av omstilling i private og offentlige virksomheter førte til at flere opplevde at tryggheten ble borte. Dette forsterket konfliktlinjer i politikk og samfunn med demonstrasjoner og mistro som resultat.

Det er liten tvil om at overgangen til et klimavennlig samfunn er nødvendig og Norge har et lovfestet mål om å bli et lavutslippssamfunn i 2050 (jf. klimaloven). Klimautvalget 2050 har utredet hvilke veivalg Norge står overfor for å oppnå dette målet på en mest mulig kostnadseffektiv måte med effektiv ressursbruk og et konkurransedyktig næringsliv.

Klimautvalget peker på et «stort misforhold mellom de uttalte ambisjonene i klimapolitikken og vedtatte tiltak og virkemidler» (NOU 2023: 25, s. 11). Klimautvalget vurderte blant annet at klimapolitikken må favne bredere, den må understøttes av et beslutningssystem som er bedre tilpasset målet om en helhetlig omstilling av samfunnet og at det er behov for politisk lederskap for å avveie kryssende hensyn og interesser. Blant annet foreslår utvalget at det utarbeides en strategi for sluttfasen av norsk petroleumsvirksomhet og at denne legges frem så raskt som mulig (NOU 2023: 25, s. 11-12). Klimautvalget konkluderer med at samfunnet står overfor flere komplekse og sektorovergripende problemstillinger som ikke bare gjelder klimapolitikken, men også «temaer som forsvar, sikkerhet, digitalisering, og helse og omsorg», og at omstillingen til et lavutslippssamfunn skjer under usikkerhet (NOU 2023: 25, s. 262, 263). Klimautvalget peker også på at «alle viktige ressurser for overgangen til et lavutslippssamfunn er knappe», det være seg «kraft, biomasse, kapital, arealer, mineraler, metaller, andre naturressurser og kompetanse» (NOU 2023: 25, s. 268). Gitt Kinas dominans når det gjelder produksjon av sjeldne jordarter og andre kritiske råmaterialer (jf. Tabell 2.1), er det også et spørsmål om en rask og omfattende energiomstilling til et lavutslippssamfunn vil være mulig uten at man blir svært avhengig av tilgang til kinesiske råmaterialer. Dette gjelder særlig hvis man går i retning av et lavutslippssamfunn med høyt forbruk av kraft, mineraler og metaller og hvor man ikke har fått til en omstilling

til en mer sirkulær økonomi. Alternativt vil økt utvinning av mineraler og metaller være nødvendig, men dette kan føre til tap av natur og biologisk mangfold.

Store samfunnsendringer vil altså være nødvendige for at Norge skal bli et lavutslippssamfunn. Hvorvidt en omfattende energiomstilling vil føre til at samfunnet går i retning av «Klimaspranget» eller «Spredning i laget», vil blant annet være avhengig av i hvilken grad Norge lykkes med slike omfattende samfunnsendringer på måter som gjør at tilliten i samfunnet opprettholdes.

Norges beliggenhet mot Arktis, nærhet til Nord-Atlanteren og nærhet til det russiske basekomplekset på Kolahalvøya har stor geopolitisk betydning. Med økt aktivitet i Arktis og økt utnyttelse av romdomenet, kan Norges strategiske beliggenhet gjøre Norge mer sårbart overfor press og aggresjon (NOU 2023: 14, s. 155-156; Pedersen, 2023). Fremtidsbildet «Bakpå» fremstår i så måte som den farligste utviklingsretningen hvor økt politisk polarisering og økt konflikt i samfunnet kan gjøre Norge mer sårbart overfor sammensatte trusler.

6 Konklusjoner

Norge vil være en viktig energinasjon for Europa i overskuelig fremtid, også innen fornybar energi slik det norsk-tyske samarbeidet viser (Regjeringen, 2023). Det norske kraftsystemet vil derfor spille en stadig viktigere rolle i tiden fremover. Dette skjer i en tid hvor Russland fører en brutal utmattelseskrig mot Ukraina og hvor forholdet mellom USA og Kina bestemmer graden av stormaktsrivalisering og konfrontasjon.

Pålitelig kraftforsyning er av vital betydning for verdiskaping og befolkningens velferd (NOU 2023: 3, s. 148), samt for evnen til å ivareta samfunnssikkerhet og nasjonale sikkerhetsinteresser (DSB, 2016; NATO, 2022b; NSM, 2021). Energisikkerhet har blitt storpolitikk og vår posisjon som energinasjon sammen med vår geografiske nærhet til Russland, gjør at Norge kan bli utsatt for press og angrep (NOU 2023: 14, s. 155-159). Forsvarskommisjonen av 2021 peker på at norske kraftinstallasjoner «strekker seg over store områder som er krevende å beskytte og overvåke» og at hele verdikjeden for kraftforsyning vil være utsatt (NOU 2023: 14, s. 159).

Formålet med dette arbeidet har vært å belyse tilsiktede handlinger som kan norsk kraftforsyning og som det er nødvendig å ha beredskap for å håndtere. Dette har blitt gjort gjennom en scenariobasert tilnærming som har tatt utgangspunkt i utviklingstrekk knyttet til klimaendringer, teknologisk utvikling, kriminalitetsutvikling i det digitale rom, terrorisme i Vest-Europa og trusler fra fremmedstatlige aktører. Basert på morfologisk analyse av utfordringsbildet og andre studier ved FFI (Bergaust & Sellevåg, 2023; Johansen, 2022), er følgende kategorier av tilsiktede handlinger identifisert som norsk kraftforsyningsberedskap bør ta høyde for:

- Trusler fra kriminelle aktører:
  - Datakriminalitet

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

- Trusler fra fremmedstatlige aktører:
  - Sammensatte trusler i form av maktposisjonering, fordekt tvang, sabotasje og/eller tvangsdiplomati
  - Væpnet angrep i form av ukonvensjonell krigføring, begrenset angrep eller strategisk overfall

Hvilke fremtidige tilsiktede handlinger som kan true norsk kraftforsyning er beheftet med stor usikkerhet og utfallsrommet er stort. Kategoriene ovenfor kan benyttes for å utvikle scenarioer for tilsiktede handlinger som norsk kraftforsyningsberedskap må ta høyde for. Eksempler på scenarioer som kan falle innenfor *datakriminalitet* kan være datatyveri av kraftsensitiv informasjon, bruk av løsepengevirus, tjenestenektangrep eller ulike former for skadevare. Eksempler på scenarioer som kan falle innenfor *ekstremisme* og som kan være relevante for norsk kraftforsyning, er klimaaktivister eller klimamotstandere som bruker antidemokratiske virkemidler, økofascisme (Campion, 2022) eller ekstreme miljøvernere som ønsker å fjerne industrisamfunnet

(LeVasseur, 2017). Eksempler på scenarioer for sammensatte trusler fra fremmedstatlige aktører kan være *maktposisjonering* i form av utenlandske direkteinvesteringer i norske kraftselskaper eller bruk av informasjonsmanipulasjon og innblanding for å oppnå økt politisk polarisering knyttet til kraftutbygging; bruk av *fordekt tvang* gjennom bruk av såkalte wiperangrep[11] mot norske kraft- og nettselskaper eller utøve press på forsyningskjeder for kritiske komponenter til kraftsystemet; *sabotasje* gjennom bruk av offensive cyberoperasjoner mot operasjonell teknologi eller fysisk ødeleggelse av komponenter i kraftsystemet; eller *tvangsdiplomati* i form av økonomisk maktbruk og diplomatisk press mot Norge som rammer kraftforsyningen. Eksempler på scenarioer for væpnede angrep fra fremmedstatlige aktører kan være missil- og droneangrep mot kraftsystemet som en del av et begrenset militært angrep eller et strategisk overfall på Norge. *Det fremheves at dette arbeidet ikke vurderer sannsynligheten for slike scenarioer. Denne studien viser kun at slike kategorier av tilsiktede handlinger kan være mulige.*

Det er også stor usikkerhet knyttet til samfunnsutviklingen mot lavutslippssamfunnet som er nødvendig for å nå Norges klimaforpliktelser. Dette gjelder både omfanget av og tempoet på energiomstillingen, og i hvilken grad tilliten i samfunnet opprettholdes. Dette arbeidet har beskrevet denne usikkerheten i form av fire fremtidsbilder: «På kjente stier», «Klimaspranget», «Spredning i laget» og «Bakpå» (jf. Figur 4.3). Hvorvidt en omfattende energiomstilling vil føre til at samfunnet går i retning av «Klimaspranget» eller «Spredning i laget», vil blant annet være avhengig av i hvilken grad Norge lykkes med slike omfattende samfunnsendringer på måter som gjør at tilliten i samfunnet opprettholdes. Norges strategiske beliggenhet med grense til Russland gjør at Norge kan bli utsatt for press og aggresjon (NOU 2023: 14, s. 155-156). Fremtidsbildet «Bakpå» fremstår i så måte som den farligste utviklingsretningen hvor økt politisk polarisering og økt konflikt i samfunnet kan gjøre Norge mer sårbart overfor sammensatte trusler. Hvilke konkrete scenarioer for tilsiktede handlinger som kan utspille seg, vil derfor også avhenge av hvordan samfunnet utvikler seg mot lavutslippssamfunnet. I en slik sammenheng må det tas med i betraktningen at konsekvenser av klimaendringer kan fungere som en trusselmultiplikator.

Videreutviklingen av norsk kraftforsyningsberedskap må ta hensyn til både usikkerheten og ustabiliteten i den sikkerhetspolitiske situasjonen, og energiomstillingen mot et lavutslippssamfunn. I situasjoner hvor det er et «informasjonsgap» mellom hva som er kjent og hva som må være kjent for å ta gode valg (Ben-Haim, 2019), bør robuste strategier som fungerer godt over et bredt spektrum av mulige utfall velges (Lempert *et al.*, 1996; Rosenhead *et al.*, 1972). I et slikt perspektiv bør norsk kraftforsyningsberedskap ta høyde for realistiske verstefallsscenarioer i hele konfliktspekteret, også krig.

[11] Datanettverksangrep som sletter data.

A Løsningsrom for tilsiktede handlinger mot norsk kraftforsyning

Tabell A.1 Løsningsrom for tilsiktede handlinger mot norsk kraftforsyning sortert etter trusselaktør

Trusselaktør	Målsetting	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Politiske	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Økonomiske	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Økonomiske	Fordekt
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Juridiske	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Juridiske	Fordekt
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Informasjon	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Informasjon	Fordekt
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Cyber	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Presse	Cyber	Fordekt
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Politiske	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Økonomiske	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Økonomiske	Fordekt
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Juridiske	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Juridiske	Fordekt
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Informasjon	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Informasjon	Fordekt
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Cyber	Åpent
Fremmedstatlig	Endring av politikk	Myndigheter	Påvirke	Cyber	Fordekt
Fremmedstatlig	Endring av politikk	Befolkningen	Påvirke	Informasjon	Åpent
Fremmedstatlig	Endring av politikk	Befolkningen	Påvirke	Informasjon	Fordekt
Fremmedstatlig	Svekke handlefrihet	Kraftsystemet	Skade	Militære	Åpent
Fremmedstatlig	Svekke handlefrihet	Kraftsystemet	Skade	Militære	Fordekt
Fremmedstatlig	Svekke handlefrihet	Kraftsystemet	Skade	Fysiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Kraftsystemet	Skade	Cyber	Åpent
Fremmedstatlig	Svekke handlefrihet	Kraftsystemet	Skade	Cyber	Fordekt
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Politiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Økonomiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Økonomiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Juridiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Juridiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Informasjon	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Informasjon	Fordekt
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Cyber	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Presse	Cyber	Fordekt
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Politiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Økonomiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Økonomiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Juridiske	Åpent

Tabell A.1 (forts.)

Trusselaktør	Målsetting	Angrepsmål	Metode	Virkemiddel	Fordekthet
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Juridiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Informasjon	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Informasjon	Fordekt
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Cyber	Åpent
Fremmedstatlig	Svekke handlefrihet	Virksomheter	Påvirke	Cyber	Fordekt
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Politiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Økonomiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Økonomiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Juridiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Juridiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Informasjon	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Informasjon	Fordekt
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Cyber	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Presse	Cyber	Fordekt
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Politiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Økonomiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Økonomiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Juridiske	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Juridiske	Fordekt
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Informasjon	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Informasjon	Fordekt
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Cyber	Åpent
Fremmedstatlig	Svekke handlefrihet	Myndigheter	Påvirke	Cyber	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Kraftsystemet	Skade	Fysiske	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Kraftsystemet	Skade	Cyber	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Virksomheter	Presse	Juridiske	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Virksomheter	Presse	Informasjon	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Virksomheter	Presse	Cyber	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Virksomheter	Påvirke	Juridiske	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Virksomheter	Påvirke	Informasjon	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Virksomheter	Påvirke	Cyber	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Myndigheter	Presse	Juridiske	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Myndigheter	Presse	Informasjon	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Myndigheter	Presse	Cyber	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Myndigheter	Påvirke	Juridiske	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Myndigheter	Påvirke	Informasjon	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Myndigheter	Påvirke	Cyber	Fordekt
Fremmedstatlig	Svekke tillit i samfunnet	Befolkningen	Påvirke	Informasjon	Fordekt
Fremmedstatlig	Økonomisk vinning	Virksomheter	Presse	Cyber	Fordekt
Fremmedstatlig	Økonomisk vinning	Virksomheter	Stjele	Cyber	Fordekt
Fremmedstatlig	Økonomisk vinning	Myndigheter	Presse	Cyber	Fordekt
Fremmedstatlig	Økonomisk vinning	Myndigheter	Stjele	Cyber	Fordekt

Tabell A.1 (forts.)

Trusselaktør	Målsetting	Angrepsmål	Metode	Virkemiddel	Fordekthet
Ikke-statlig	Endring av politikk	Myndigheter	Presse	Økonomiske	Åpent
Ikke-statlig	Endring av politikk	Myndigheter	Presse	Økonomiske	Fordekt
Ikke-statlig	Endring av politikk	Myndigheter	Presse	Informasjon	Åpent
Ikke-statlig	Endring av politikk	Myndigheter	Presse	Informasjon	Fordekt
Ikke-statlig	Endring av politikk	Myndigheter	Presse	Cyber	Åpent
Ikke-statlig	Endring av politikk	Myndigheter	Presse	Cyber	Fordekt
Ikke-statlig	Endring av politikk	Myndigheter	Påvirke	Økonomiske	Åpent
Ikke-statlig	Endring av politikk	Myndigheter	Påvirke	Økonomiske	Fordekt
Ikke-statlig	Endring av politikk	Myndigheter	Påvirke	Informasjon	Åpent
Ikke-statlig	Endring av politikk	Myndigheter	Påvirke	Informasjon	Fordekt
Ikke-statlig	Endring av politikk	Myndigheter	Påvirke	Cyber	Åpent
Ikke-statlig	Endring av politikk	Myndigheter	Påvirke	Cyber	Fordekt
Ikke-statlig	Endring av politikk	Befolkningen	Påvirke	Informasjon	Åpent
Ikke-statlig	Endring av politikk	Befolkningen	Påvirke	Informasjon	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Kraftsystemet	Skade	Fysiske	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Kraftsystemet	Skade	Cyber	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Virksomheter	Presse	Informasjon	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Virksomheter	Presse	Cyber	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Virksomheter	Påvirke	Informasjon	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Virksomheter	Påvirke	Cyber	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Myndigheter	Presse	Informasjon	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Myndigheter	Presse	Cyber	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Myndigheter	Påvirke	Informasjon	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Myndigheter	Påvirke	Cyber	Fordekt
Ikke-statlig	Svekke tillit i samfunnet	Befolkningen	Påvirke	Informasjon	Fordekt
Ikke-statlig	Økonomisk vinning	Virksomheter	Presse	Cyber	Fordekt
Ikke-statlig	Økonomisk vinning	Virksomheter	Stjele	Cyber	Fordekt
Ikke-statlig	Økonomisk vinning	Myndigheter	Presse	Cyber	Fordekt
Ikke-statlig	Økonomisk vinning	Myndigheter	Stjele	Cyber	Fordekt

Referanser

Amer, M., Daim, T. U. & Jetter, A. (2013). A review of scenario planning. *Futures*, *46*, 23-40. https://doi.org/https://doi.org/10.1016/j.futures.2012.10.003

Amini, S., Pasqualetti, F. & Mohsenian-Rad, H. (2018). Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Transactions on Smart Grid*, *9*(4), 2862-2872. https://doi.org/10.1109/TSG.2016.2622686

Andås, H. (2020). *Emerging technology trends for defence and security* (FFI-rapport 20/01050). Forsvarets forskningsinstitutt.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*, 5-26.

Beadle, A. W. (2016). *Å forske på Forsvaret i fremtiden – muligheter, begrensninger og kognitive fallgruver* (FFI-rapport 16/01810). Forsvarets forskningsinstitutt.

Beadle, A. W., Diesen, S., Nyhamar, T. & Bostad, E. K. (2019). *Globale trender mot 2040 – et oppdatert fremtidsbilde* (FFI-rapport 19/00045). Forsvarets forskningsinstitutt.

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.

Bergaust, J. C. & Sellevåg, S. R. (2023). Improved conceptualising of hybrid interference below the threshold of armed conflict. *European Security*, 1-27. https://doi.org/10.1080/09662839.2023.2267478

Bergaust, J. C., Skjei, F. & Sellevåg, S. R. (2022). *Hva kan Norge lære av andre lands tilnærming til sammensatte trusler? - rapport til Forsvarskommisjonen* (FFI-rapport 22/02310). Forsvarets forskningsinstitutt.

Bergenggruen, V. (2023, 9. januar). *'Is There Something More Sinister Going On?' Authorities Fear Extremists Are Targeting U.S. Power Grid*. TIME. Hentet 18. april 2023 fra https://time.com/6244977/us-power-grid-attacks-extremism/

Bjørgo, T. (2018). Introduksjon til rapporten. I T. Bjørgo (Red.), *Høyreekstremisme i Norge. Utviklingstrekk, konspirasjonsteorier og forebyggingsstrategier* (PHS Forskning 2018: 4). Politihøgskolen.

Bjørgul, L., Sivertsen, E. G. & Sellevåg, S. R. (2022). *Scenarioer for uønsket påvirkning i forbindelse med norske valg* (FFI-rapport 22/01424). Forsvarets forskningsinstitutt.

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/

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E. & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, *464*(7291), 1025-1028. https://doi.org/10.1038/nature08932

Bundesnetzagentur. (2023, 9. mars). *Gasimporte in GWh/Tag*. Hentet 9. mars 2023 fra https://www.bundesnetzagentur.de/DE/Gasversorgung/aktuelle_gasversorgung/_svg/Gasimporte/Gasimporte.html

Caldwell, M., Andrews, J. T. A., Tanay, T. & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*, 14. https://doi.org/10.1186/s40163-020-00123-8

Campion, K. (2022, 9. desember). *From Brownshirts to Greenshirts: Understanding Ecofascism in a Time of Climate Crisis*. C-REX - Center for Research on Extremism, University of Oslo. Hentet 29. mars 2023 fra https://www.sv.uio.no/c-rex/english/news-and-events/right-now/2022/from-brownshirts-to-greenshirts.html

Cardenas, A. (2021). *Cyber-Physical Systems Security Knowledge Area* (Version 1.0.1). T. N. C. S. C. CyBOK. https://www.cybok.org/media/downloads/Cyber_Physical_Systems-v1.0.1.pdf

Chen, J., Liang, G., Cai, Z., Hu, C., Xu, Y., Luo, F. & Zhao, J. (2016). Impact analysis of false data injection attacks on power system static security assessment. *Journal of Modern Power Systems and Clean Energy*, *4*(3), 496-505. https://doi.org/10.1007/s40565-016-0223-6

Cherepanov, A. & Lipovsky, R. (2016, 5-7 October). *Blackenergy - What we really know about the notorious cyber attacks*. Virus Bulletin Conference, Denver, U.S. https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf

Cullen, P. J. & Reichborn-Kjennerud, E. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. A Multinational Capability Development Campaign project*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

DSB. (2016). *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

DSB. (2019). *Analyser av krisescenarioer 2019*. https://www.dsb.no/rapporter-og-evalueringer/analyser-av-krisescenarioer-2019/

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

Energi Norge. (2017). *Økonomisk kriminalitet i energibransjen*. Hentet 28. mars 2023 fra https://www.digiblad.no/energinorge/veileder-okonomisk-kriminalitet/files/assets/common/downloads/publication.pdf

energiloven. *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (LOV-1990-06-29-50). Lovdata. https://lovdata.no/dokument/NL/lov/1990-06-29-50?q=energiloven

ENTSO-E. (2022). *TYNDP 2022 Scenario Report*. https://2022.entsos-tyndp-scenarios.eu/

Etterretningstjenesten. (2023). *Fokus 2023. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf/_/attachment/inline/c1a9a458-aa1d-4bf6-a558-9cec57acde8f:9b2050d897a2b2db1bddc8e505db7b666e608b98/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf

European Commission. (2020a). *Critical Raw Materials for Strategic Technologies and Sectors in the EU - A Foresight Study*. https://rmis.jrc.ec.europa.eu/uploads/CRMs_for_Strategic_Technologies_and_Sectors_in_the_EU_2020.pdf

European Commission. (2020b). *Critical Raw Materials Resilience: Charting a Path towards greater Security and Sustainability* (COM(2020) 474 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0474&from=EN

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

Europol. (2017). *European Union (EU) Serious and Organised Crime Threat Assessment 2017 (SOCTA 2017)*. https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf

Europol. (2020a). *European Union Terrorism Situation and Trend report 2020*. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020

Europol. (2020b). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. Hentet 8. april 2020 fra https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Europol. (2023). *ChatGPT - The impact of Large Language Models on Law Enforcement*. https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf

Farsund, B. H., Søndrol, T., Nystuen, K. O., Hornfelt, L., Sellevåg, S. R. & Pham, V. (2022). *Utviklingen av nye IoT-baserte infrastrukturer i samfunnet – utfordringer for nasjonal sikkerhet (revidert rapport)* (FFI-rapport 22/00631). Forsvarets forskningsinstitutt.

Forsby, A. B. & Sverdrup-Thygeson, B. (2022). *China's coercive diplomacy: Why it's on the rise and what it means for Scandinavia* (NUPI Policy Brief 6/2022). Norwegian Institute of International Affairs. https://www.nupi.no/en/publications/cristin-pub/chinas-coercive-diplomacy-why-it-s-on-the-rise-and-what-it-means-for-scandinavia

Foss, A. B. & Olsen, O. (2022, 29. oktober). *PST åpner opp om truslene: Slik skapes det frykt og usikkerhet i Norge*. Aftenposten. Hentet 8. mars 2023 fra https://www.aftenposten.no/norge/i/WR0lXQ/pst-aapner-opp-om-truslene-slik-skapes-det-frykt-og-usikkerhet-i-norge

Gayle, D., Taylor, M. & Niranjan, A. (2023, 12. oktober). *Human rights experts warn against European crackdown on climate protesters*. Guardian. Hentet 5. desember 2023 fra https://www.theguardian.com/environment/2023/oct/12/human-rights-experts-warn-against-european-crackdown-on-climate-protesters

Giannopoulos, G., Smith, H. & Theocharidou, M. (2021). *The Landscape of Hybrid Threats: A conceptual model* (EUR 30585 EN). Publications Office of the European Union.

Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N. & Wollman, D. A. (2021). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0* (NIST Special Publication 1108r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1108r4

Government Office for Science. (2017). *The Futures Toolkit: Tools for Futures Thinking and Foresight Across UK Government. Edition 1.0*. UK Government Office for Science. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf

Griffor, E. (2017). *Framework for Cyber-Physical Systems: Volume 1, Overview* (NIST Special Publication 1500-201). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

Huang, B., Cardenas, A. & Baldick, R. (2019). Not everything is dark and gloomy: Power grid protections against IoT demand attacks. Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA.

IEA. (2022a). *Ukraine Real-Time Electricity Data Explorer*. Hentet 9. mars 2023 fra https://www.iea.org/data-and-statistics/data-tools/ukraine-real-time-electricity-data-explorer

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

IPCC. (2021). *Climate Change 2021: The Physical Science Basis. Contribution of Working Group I to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change* (V. Masson-Delmotte, P. Zhai, A. Pirani, S. L. Connors, C. Péan, S. Berger, N. Caud, Y. Chen, L. Goldfarb, M. I. Gomis, M. Huang, K. Leitzell, E. Lonnoy, J. B. R. Matthews, T. K. Maycock, T. Waterfield, O. Yelekçi, R. Yu & B. Zhou, Red.). Cambridge University Press.

IPCC. (2022). Summary for Policymakers. I P. R. Shukla, J. Skea, A. Reisinger, R. Slade, R. Fradera, M. Pathak, A. Al Khourdajie, M. Belkacemi, R. van Diemen, A. Hasija, G. Lisboa, S. Luz, J. Malley, D. McCollum, S. Some & P. Vyas (Red.), *Climate Change 2022: Mitigation of Climate Change. Working Group III Contribution to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change*. Cambridge University Press.

Johansen, I. (2018). Scenario modelling with morphological analysis. *Technological Forecasting & Social Change*, *126*, 116-125.

Johansen, I. (2022). *Scenarioklasser for forsvarsplanlegging - revisjon av FFIs scenariogrunnlag* (FFI-rapport 21/01788). Forsvarets forskningsinstitutt.

Johansen, I. & Gråtrud, H. (2018). *Fra taktisk elite til strategisk tilrettelegger - hvordan Forsvarets spesialstyrker kan møte fremtidens utfordringer* (FFI-rapport 18/01435). Forsvarets forskningsinstitutt.

Kagge, G. (2023, 6. februar). *Nynazister skal ha planlagt å sprenge kraftnett*. Aftenposten. Hentet 18. april 2023 fra https://www.aftenposten.no/verden/i/8JE3jA/nynazister-skal-ha-planlagt-aa-sprenge-kraftnett

Kampevoll, F. & Lorch-Falch, S. (2022, 18. august). *Fortellingen om kraftkablene*. NRK. Hentet 1. april 2023 fra https://www.nrk.no/norge/xl/fortellingen-om-kraftkablene-1.16060842

Klepper, K. B., Windvik, R., Broen, T., Kveberg, T., Bentstuen, O. I., Sjøvik, Ø., Svenes, K., Waage, K., Lindgren, P. Y., Sivertsen, E. G. & Bergh, A. (2022). *Teknologiske og*

samfunnsmessige utviklingstrekk av særskilt betydning for nasjonale sikkerhetsinteresser (FFI-rapport under utgivelse). Forsvarets forskningsinstitutt.

Kofman, M., Fink, A., Gorenburg, D., Chesnut, M., Edmonds, J. & Waller, J. (2021). *Russian Military Strategy: Core Tenets and Operational Concepts*. Center for Naval Analyses. https://www.cna.org/archive/CNA_Files/pdf/russian-military-strategy-core-tenets-and-operational-concepts.pdf

Kommunal- og moderniseringsdepartementet. (2019). *Scenarioer for offentlig sektor i 2040. Utarbeidet i forbindelse med stortingsmelding om innovasjon i offentlig sektor*. https://www.regjeringen.no/no/dokumenter/scenarioer-for-offentlig-sektor-i-2040/id2654101/

Kripos. (2019). *Arbeid med drivkrefter*.

Kripos. (2023). *Cyberkriminalitet 2023. Politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer*. https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

Kaati, L., Cohen, K., Pelzer, B., Fernquist, J. & Sarnecki, H. P. (2020). *Ekofascism. En studie av propaganda i digitala miljöer* (FOI Memo 7441). FOI.

Langner, R. (2013). *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve*. The Lagner Group. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

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

LeVasseur, T. (2017). Decisive Ecological Warfare: Triggering Industrial Collapse via Deep Green Resistance. *Journal for the Study of Religion, Nature and Culture*, *11*(1), 109-130. https://doi.org/10.1558/jsrnc.29799

Lindgren, P. Y., Hemnes, P. F. & Waage, K. (2022). *Kinas potensial for økonomisk statshåndverk – kinesisk økonomi og interaksjon med omverden og Norge* (FFI-rapport 22/00421). Forsvarets forskningsinstitutt.

Lipovsky, R., Cherepanov, A., Lee, R. M., Miller, B. & Slowik, J. (2017, 26-27 July). *Industroyer/Crashoverride: Zero Things Cool About A Threat Group Targeting The Power Grid*. Black Hat USA, Las Vegas, NV. https://www.blackhat.com/docs/us-17/wednesday/us-17-Lee-Industroyer-Crashoverride-Zero-Things-Cool-About-A-Threat-Group-Targeting-The-Power-Grid.pdf

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

Liu, Y., Ning, P. & Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.*, *14*(1), Article 13. https://doi.org/10.1145/1952982.1952995

Maimon, D. & Louderback, E. R. (2019). Cyber-Dependent Crimes: An Interdisciplinary Review. *Annual Review of Criminology*, *2*, 191-216.

McDermott, R. N. & Bukkvoll, T. (2018). Tools of Future Wars — Russia is Entering the Precision-Strike Regime. *The Journal of Slavic Military Studies*, *31*(2), 191-213. https://doi.org/10.1080/13518046.2018.1451097

Meld. St. 9 (2022-2023). *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet - Så åpent som mulig, så sikkert som nødvendig*. Justis- og beredskapsdepartementet.

Meld. St. 10 (2021-2022). *Prioriterte endringer, status og tiltak i forsvarssektoren*. Forsvarsdepartementet.

Meld. St. 13 (2020-2021). *Klimaplan for 2021-2030*. Klima- og miljødepartementet.

National Institute of Standards and Technology. (2022, 20. september). *Glossary*. Hentet 27. mars 2023 fra https://csrc.nist.gov/glossary

NATO. (2017). *The NATO Alternative Analysis Handbook* (2. utg.). https://www.act.nato.int/images/stories/media/doclibrary/alta-handbook.pdf

NATO. (2022a). *Climate Change & Security Impact Assessment*. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/280622-climate-impact-assessment.pdf

NATO. (2022b, 20. september). *Resilience, civil preparedness and Article 3*. Hentet 5. oktober 2022 fra https://www.nato.int/cps/en/natohq/topics_132722.htm

NATO Science and Technology Organization. (2023). *Science & Technology Trends 2023-2043 Across the Physical, Biological, and Information Domains. Volume 1: Overview*. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf

Nesser, P. & Stenersen, A. (2014). The Modus Operandi of Jihadi Terrorists in Europe. *Perspectives on Terrorism*, *8*(6). http://www.terrorismanalysts.com/pt/index.php/pot/article/view/388

Nesser, P., Stenersen, A. & Oftedal, E. (2016). Jihadi Terrorism in Europe: The IS-Effect. *Perspectives on Terrorism*, *10*(6), 3-24.

NOU 2022: 6. *Nett i tide - om utvikling av strømnettet*. Olje- og energidepartementet.

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

NOU 2023: 14. *Forsvarskommisjonen av 2021 - Forsvar for fred og frihet*. Forsvarsdepartementet.

NOU 2023: 25. *Omstilling til lavutslipp - Veivalg for klimapolitikken mot 2050*. Klima- og miljødepartementet.

NSM. (2021, 15. oktober). *Oversikt over innmeldte grunnleggende nasjonale funksjoner*. Hentet 24. januar 2022 fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/grunnleggende-nasjonale-funksjoner/oversikt-over-innmeldte-grunnleggende-nasjonale-funksjoner/

NSM. (2022). *Nasjonalt digitalt risikobilde 2022*. https://nsm.no/getfile.php/1311995-1664550278/NSM/Filer/Dokumenter/Rapporter/NDIG%202022.pdf

NVE. (2021). *Langsiktig kraftmarkedsanalyse 2021-2040. Forsterket klimapolitikk påvirker kraftprisene* (NVE Rapport nr. 29/2021). https://publikasjoner.nve.no/rapport/2021/rapport2021_29.pdf

OECD. (2022). *OECD Environmental Performance Reviews: Norway 2022*. https://doi.org/doi:https://doi.org/10.1787/59e71c13-en

Palmer, D. A. R. (2015). *Back to the future? Russia's hybrid warfare, revolutions in military affairs, and Cold War comparisons* (Research Paper No. 120). Research Division – NATO Defense College. https://www.files.ethz.ch/isn/194718/rp_120.pdf

Parker, T. (2014). *Avoiding the Terrorist Trap. Why Respect for Human Rights is the Key to Defeating Terrorism* (Bd. Volume 12) [doi:10.1142/p995]. World Scientific. https://doi.org/doi:10.1142/p995

Pedersen, M. N. (2023). *Et varmere Arktis i en kald krig - klimaendringenes sikkerhetspolitiske konsekvenser i Arktis* (FFI-rapport 23/01594). F. forskningsinstitutt.

Politiet. (2023). *Politiets trusselvurdering 2023*. https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2023.pdf

PST. (2023). *Nasjonal trusselvurdering 2023*. https://pst.no/globalassets/ntv/2023/ntv_2023_nor_web.pdf

Regjeringen. (2023, 5. januar). *Tettere samarbeid mellom Norge og Tyskland for å utvikle grønn industri*. Hentet 30. november 2023 fra https://www.regjeringen.no/no/aktuelt/tettere-samarbeid-mellom-norge-og-tyskland-for-a-utvikle-gronn-industri/id2958102/

Ritchey, T. (2013a). *General Morphological Analysis. A General Method for Non-Quantified Modelling*. Swedish Morphological Society. Hentet 2. april 2021 fra https://www.swemorph.com/pdf/gma.pdf

Ritchey, T. (2013b). Wicked problems. Modelling social messes with morphological analysis. *Acta Morphologica Generalis*, *2*, 1-7.

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

Santora, M., Biggs, M. M. & Nechepurenko, I. (2022, 1. desember). *Brace for Bombs, Fix and Repeat: Ukraine's Grim Efforts to Restore Power*. The New York Times. Hentet 8. mars 2023 fra https://www.nytimes.com/2022/12/01/world/europe/russia-ukraine-war-infrastructure.html

Sellevåg, S. R. (2021). *Morfologisk analyse av trusler mot Norges sikkerhet – utfordringskategorier for politiet, PST og påtalemyndigheten* (FFI-rapport 20/03171; Unntatt offentlighet). Forsvarets forskningsinstitutt.

Sellevåg, S. R., Bergh, A., Bruvoll, J. A., Høibråten, S., Jacobsen, H. L., Strand, M. & Barland, B. (2021). *Samfunnsutvikling mot 2030 - utfordringer for politiet, PST og påtalemyndigheten* (FFI-rapport 21/01132). Forsvarets forskningsinstitutt.

Sellevåg, S. R., Brattekås, K., Bruvoll, J. A., Buvarp, P. M. H., Fardal, H., Farsund, B., Fykse, E. M., Gisnås, H., Hellesø-Knutsen, K., Kirkhorn, S., Nystuen, K. O., Olsen, R. & Seehuus, R. A. (2020). *Samfunnssikkerhet mot 2030 – utviklingstrekk* (FFI-rapport 20/00530). Forsvarets forskningsinstitutt.

Skjelland, E., Arnfinnsson, B., Birkemo, G. A., Bråthen, K., Glærum, S., Graarud, E., Hakvåg, U., Klepper, K. B., Kvalvik, S. N., Larsen, M. V., Mayer, M. J., Minos-Stensrud, M., Monsen, I. H. L., Mørkved, T., Nordvang, E. U., Presterud, A. O., Sellevåg, S. R., Sendstad, C., Sivathas, K., Strand, K. R., Thuv, A. & Voldhaug, J. E. (2023). *Forsvarsanalysen 2023* (FFI-rapport 23/00659). Forsvarets forskningsinstitutt.

Soltan, S., Mittal, P. & Poor, H. V. (2018). BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. Proceedings of the 27th USENIX Security Symposium, Baltimore, MD, USA.

Statnett. (2018, 19. oktober). *Slik fungerer kraftsystemet*. Hentet 26. mars 2023 fra https://www.statnett.no/om-statnett/bli-bedre-kjent-med-statnett/slik-fungerer-kraftsystemet/

Statnett. (2023, 11. september 2023). *Kortsiktig markedsanalyse 2023-2028*. Hentet 26. oktober 2023 fra https://www.statnett.no/globalassets/for-aktorer-i-kraftsystemet/planer-og-analyser/kma/kortsiktig-markedsanalyse-kma-2023-2028.pdf

Stenersen, A. (2017). Thirty years after its foundation - Where is al-Qaida going? *Perspectives on Terrorism*, *11*, 5-16.

Thorsen, D. E. (2023, 19. januar). *politikk i Store norske leksikon på snl.no*. Hentet 28. mars 2023 fra https://snl.no/politikk

Tønnessen, T. H. (2017). Islamic State and Technology – A Literature Review. *Perspectives on Terrorism*, *11*, 101-111.

U. S. Department of Energy. (u.å.). *Electric Disturbance Events (OE-417) Annual Summaries*. Hentet 18. april 2023 fra https://www.oe.netl.doe.gov/OE417_annual_summary.aspx

U.S. Department of the Treasury. (2019, 13. september). *Treasury sanctions North Korean state-sponsored malicious cyber groups*. Hentet 28. mars 2023 fra https://home.treasury.gov/news/press-releases/sm774

UK Ministry of Defence [@DefenceHQ]. (2022, 1. desember). *Latest Defence Intelligence update on the situation in Ukraine - 01 December 2022. Find out more about the UK government's response: http://ow.ly/8p2850LS1El #StandWithUkraine [tweet]*. Twitter. Hentet 8. mars 2023 fra https://twitter.com/DefenceHQ/status/1598206953087541248

UNDP. (2023). *Towards a green transition of the energy sector in Ukraine. Update on the Energy Damage Assessment*. United Nations Development Programme. https://www.undp.org/ukraine/publications/towards-green-transition-energy-sector-ukraine?gad_source=1&gclid=Cj0KCQiA35urBhDCARIsAOU7QwmUmyT08drab35gXSsI8JT5zr8gpDXdkA1xBZF_rJ-xJfuBRc3OykEaApSXEALw_wcB

Wallander, C. (2021). How the Putin Regime Really Works. *Journal of Democracy*, *32*, 178-183.

Wardle, C. & Derakhshan, H. (2017). *Information disorder: Towards an interdiciplinary framework or research and policy making* (DGI(2017)09). Council of Europe.

Wiig, T. & Knutsen, C. H. (2022, 22. mars). *Putin kan falle*. VG. Hentet 13. november 2022 fra https://www.vg.no/nyheter/meninger/i/bG2OdA/putin-kan-falle

Wråke, M., Karlsson, K., Kofoed-Wiuff, A., Bolkesjø, T. F., Lindroos, T. J., Hagberg, M., Simonsen, M. B., Unger, T., Tennbakk, B., Jåstad, E. O., Lehitlä, A., Putkonen, N. & Koljonen, T. (2021). *Nordic Clean Energy Scenarios. Solutions for Carbon Neutrality*. Nordic Energy Research. http://doi.org/10.6027/NER2021-01

Waage, K., Kvalvik, S. N. & Lindgren, P. Y. (2021). *Utenlandske investeringer og andre økonomiske virkemidler - når truer de nasjonal sikkerhet?* (FFI-rapport 20/03149). Forsvarets forskningsinstitutt.

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

Waage, K., Lindgren, P. Y., Boye, E. & Haug, I. D. (2022). *Kinesisk økonomisk statshåndverk og implikasjoner for norsk sikkerhet* (FFI-rapport 22/00422). Forsvarets forskningsinstitutt.

Zwicky, F. (1969). *Discovery, Invention, Research through the Morphological Approach*. The Macmillan Company.

Åtland, K. (2023, 25. mars). *Norges sikkerhetssituasjon etter Russlands invasjon av Ukraina*. Stratagem. Hentet 7. april 2023 fra https://www.stratagem.no/norges-sikkerhetssituasjon-etter-russlands-invasjon-av-ukraina/

Om FFI

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

FFIs formål

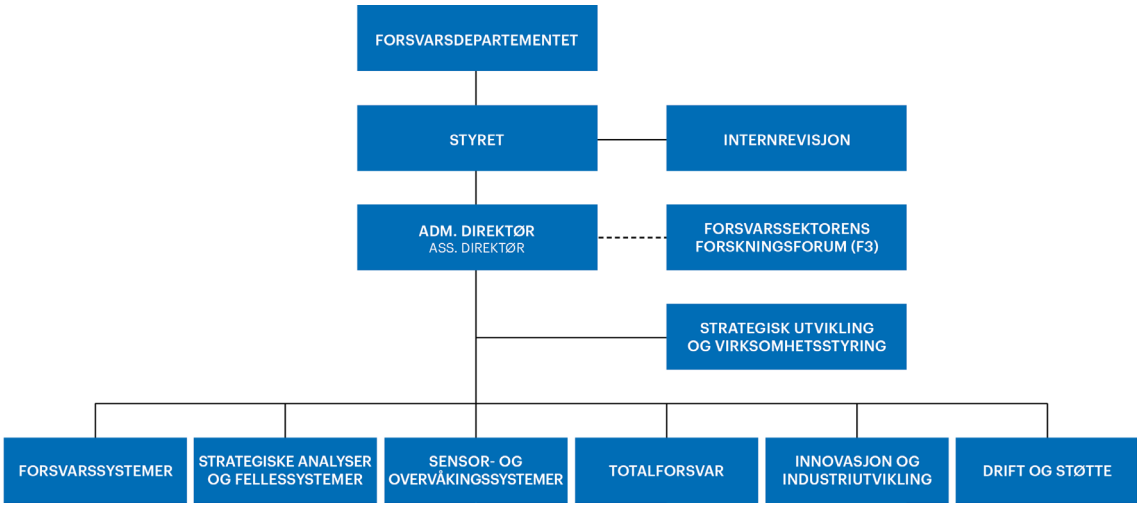
Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som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