NVE

EKSTERN RAPPORT NR. 3 / 2025

Trusselbildet for kraftforsyningen

SKREVET AV Thema Consulting Group

NVE Ekstern rapport nr. 3/2025
Trusselbildet i kraftforsyningen

Utgitt av:	Norges vassdrags-og energidirektorat
Redaktør:	Morten Groven
Forfatter:	Thema Consulting Group
Omslagsbilde:	NVE

ISBN:	978-82-410-2453-5
ISSN:	2535-8235
Saksnummer:	G25-01917

Sammendrag: Rapporten gir en overordnet beskrivelse av trusselbildet mot norsk kraftforsyning på kort og lang sikt. Kraftforsyning må forvente å bli utsatt for etterretning, forsøk på økonomisk posisjonering, påvirkningsoperasjoner og muligens sabotasje, både i form av dataangrep og angrep på fysisk infrastruktur. I en krig vil kraftforsyningen være et prioritert mål. Russland har utviklet en omfattende samling av metoder og virkemidler under nivået for direkte militær maktbruk, inkludert bruk av aktører som hackergrupper og kriminelle, samtidig som de fortsetter å videreutvikle evnen til militære angrep. Kinas søker kontroll over forsyningskjeder, rekrutterer norske borgere for å få tilgang til sensitiv og gradert informasjon, og bruker aktører uten offisiell tilknytning til landet som virkemidler for etterretning og dataangrep

Emneord: Trusselbilde, trusselaktører, kraftforsyning, Russland, Kina, maktposisjonering, påvirkning, tvang, sabotasje, militære angrep, etterretning, sikkerhet

Norges vassdrags- og energidirektorat
Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo

Telefon: 22 95 95 95
E-post: nve@nve.no
Internett: www.nve.no

Februar 2025

Forord

Tilgang til elektrisk kraft er en forutsetning for befolkningens trygghet og samfunnets funksjonsdyktighet, uansett hvilken sikkerhetstruende situasjon eller krise som Norge måtte havne i. Kraftforsyningen vil, i tillegg til utviklingen på det militære området, møte utfordringer med teknologiavhengighet og handelshindringer.

Grunnlaget for forebyggende sikkerhetsarbeid og evne til effektiv krisehåndtering er riktig og relevant kunnskap og forståelse. Selv om vi snakker mye om økt motstandskraft i samfunnet generelt og kraftsektoren spesielt, så er informasjonsbehovet lett å overse. Mye nyttig informasjon er åpent tilgjengelig, men krevende å sette sammen og tilegne seg i en hektisk sikkerhetshverdag.

NVE har derfor bestilt en rapport som sammenfatter denne informasjonen. Rapporten vil inngå som en del av NVE's arbeid knyttet til sikkerhet og beredskap i kraftforsyningen i Norge.

Rapporten beskriver det overordnede trusselbildet for kraftforsyningen, basert på åpne kilder og tilpasset kraftforsyningens ledere og medarbeidere. Arbeidet er utført av Thema og FFI, på oppdrag fra NVE. Rammeverket er ment å dekke den fulle bredden av trusler, uavhengig av den aktuelle situasjonen. Henvisningene til faktiske hendelser bidrar forhåpentlig til å tydeliggjøre bildet.

Vi vil takke Thema og FFI for vel gjennomført oppdrag.

Oslo, februar 2025

Kristian Markegård
direktør
Tilsyns- og beredskapsavdelingen

Dokumentet sendes uten underskrift. Det er godkjent i henhold til interne rutiner.

Trusselbildet for kraftforsyningen

Offentlig utredning for NVE av THEMA og FFI

FFI Forsvarets forskningsinstitutt

THEMA CONSULTING GROUP

Naviger trygt gjennom energiomstillingen

Publiseringsdato
13.02.2025

Om prosjektet

Prosjektnummer: NVE-24-01
Prosjektnavn: Trusselbildet for kraftforsyningen
Oppdragsgiver: NVE

Om rapporten

Tittel: Trusselbildet for kraftforsyningen
Rapportnummer: 2025-02
ISBN-nummer: 978-82-8368-158-1

Prosjektbeskrivelse

En pålitelig kraftforsyning er avgjørende for samfunnssikkerheten og totalforsvaret. Selv om truslene mot norsk kraftforsyning blir stadig bedre dokumentert, varierer det hvor godt kjent de er blant ansatte i kraftforsyningen. NVE har derfor gitt THEMA og FFI i oppdrag å utarbeide en tilgjengelig og oppdatert beskrivelse av truslene mot norsk kraftforsyning. Rapporten skal gi relevante aktører i kraftsektoren en bedre forståelse av trusselbildet de står ovenfor. Rapporten bygger på offentlige og ugraderte kilder, samt innspill fra forskere ved FFI.

Målgruppen for rapporten er ledelse og ansatte i kraftforsyningen. Innholdet er tilpasset målgruppen ved å fokusere på trusler og eksempler med relevans for kraftforsyningen, og ved å presentere disse på en måte som tydelig og forståelig bidrar til å danne et bilde av trusselbildet den norske kraftforsyningen står overfor. Enkelte sikkerhetsfaglige konsepter som kunne vært relevante i en mer militærfaglig sammenheng, er enten forenklet eller utelatt.

Prosjektteam

Svend Boye, partner THEMA
Stig Rune Sellevåg, sjefsforsker FFI
Håkon Taule, partner THEMA
Tora Dahl, konsulent THEMA

Om THEMA

THEMA Consulting Group tilbyr rådgivning og analyser for kraftforsyningen og energisektoren.

Om FFI

Forsvarets forskningsinstitutt (FFI) er forsvarssektorens egen forskningsinstitusjon.

INNHOLD

Sammendrag

Trusselaktører

Rapporter fra etterretnings- og sikkerhetstjenestene i Norge peker på trusler i regi av Russland og Kina som de viktigste for kraftforsyningen, både på kort og lang sikt. Etterretningstjenesten og Politiets sikkerhetstjeneste viser blant annet til at:

- Russland har utviklet en omfattende samling av metoder og virkemidler under nivået for direkte militær maktbruk, inkludert bruk av aktører som hackergrupper og kriminelle, samtidig som de fortsetter å videreutvikle evnen til militære angrep.
- Kinas søker kontroll over forsyningskjeder, rekrutterer norske borgere for å få tilgang til sensitiv og gradert informasjon, og bruker aktører uten offisiell tilknytning til landet som virkemidler for etterretning og dataangrep.

Rammeverk for å forstå trusselbildet for norsk kraftforsyning

På grunnlag av blant annet FFIs artikler om handlinger som kan true norsk kraftforsyning (2023) og scenarioklasser for forsvarsplanlegging (2022) har vi definert fire hovedkategorier av trusler som norsk kraftforsyning bør være forberedt på:

- Maktposisjonering, påvirkning og tvang: *Fremmede stater kan bruke økonomiske og politiske virkemidler, som investeringer i kritisk infrastruktur, kontroll over verdikjeder og påvirkningskampanjer, for å få makt over norsk og europeisk energiforsyning.*
- Sabotasje: *Digital sabotasje gjennom dataangrep kan forstyrre kraftforsyningens IT- og kontrollsystemer. Fysisk sabotasje av kabler og annen infrastruktur synes å forekomme oftere og oftere i Europa.*
- Militære angrep: *Kraftforsyningen vil være et prioritert strategisk mål i en væpnet konflikt. Langtrekkende presisjonsvåpen, satellittangrep og elektromagnetiske pulsangrep kan svekke kraftforsyningen og redusere samfunnets motstandskraft.*
- Etterretning: *Fremmede stater gjør forberedelser for å kunne gjennomføre de overnevnte handlingene dersom de ser seg tjent med det på et senere tidspunkt. Dette gjør de blant annet gjennom digital og fysisk etterretning, samt rekruttering av innsidere.*

Truslene som beskrives – maktposisjonering, påvirkning og tvang, sabotasje, militære angrep og etterretning – er ikke gjensidig utelukkende og forekommer ikke nødvendigvis i isolasjon. Tvert imot kan de kombineres for å oppnå en større og mer målrettet effekt. *Sammensatte trusler* er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt. Begrepet *hybride trusler* inkluderer alle virkemidler som ligger i sammensatte trusler, samt regulære militære virkemidler. Vår vurdering at det er mer nyttig for ledelse og ansatte i kraftforsyningen å fokusere på de mer konkrete trusselkategoriene «maktposisjonering, påvirkning og tvang», «sabotasje», «militære angrep» og «etterretning» enn å fokusere på begreper som sammensatte og hybride trusler. Samtidig er det viktig at ledelse og ansatte i kraftsektoren er klar over at virkemidler som sabotasje kan ha mål utover det å skade eller forstyrre kraftforsyningen i seg selv. En fremmed stat bruke trusler mot kraftforsyningen i kombinasjon med andre virkemidler for å skape mistillit i befolkningen og/eller legge press på norske myndigheter.

Maktposisjonering, påvirkning og tvang

En fremmed stat kan få Norge til å handle i tråd med deres interesser ved å påvirke det offentlige ordskiftet, opinionen og beslutningstakere, eller ved å true med økonomiske sanksjoner. I kraftforsyningens tilfelle vil det ikke nødvendigvis kun være effektivt for en fremmed stat å ødelegge eksisterende anlegg gjennom sabotasje eller militære angrep; den kan også bruke påvirkning eller maktposisjonering til å hindre at nye anlegg bygges. Aktuelle eksempler på maktposisjonering er Russlands

tilrettelegging for europeisk avhengighet av russisk gassforsyning, og den påfølgende reduksjonen i gassleveranser for å svekke europeiske lands vilje til å forsvare Ukraina. Flere er bekymret for at Kina er i ferd med å etablere en lignende økonomisk maktposisjon som Russland har hatt i gassforsyningen innenfor verdikjedene for solkraft-, vindkraft- og batteriproduksjon.

Sabotasje

I de senere årene har det vært økt oppmerksomhet rundt sabotasje som et virkemiddel brukt av fremmedstatlige aktører, både som følge av økt sabotasjeaktivitet mot europeiske land, og som følge av økt forståelse av slike virkemidlers betydning. *Digital sabotasje* i form av dataangrep kan forstyrre kraftforsyningens IT- og kontrollsystemer, og kan gjennomføres både isolert og i kombinasjon med andre virkemidler. I denne sammenhengen er det lettere for fremmede stater å lykkes med tilgangsangrep, datatyveri og driftsforstyrrende angrep enn med dataangrep med ødeleggende effekt. *Fysisk sabotasje*, som å ødelegge kommunikasjonsledninger, gassrørledninger, strømledninger, kraftverk og annen infrastruktur, vil ofte ha en ødeleggende og langvarig effekt, og kan også være forholdsvis lite ressurskrevende å gjennomføre.

Militære angrep

I et væpnet angrep mot Norge og NATO forventes ødeleggelse av kritisk sivil infrastruktur, inkludert kraftforsyning, å få prioritet tidlig, med svært kort varslingstid. Erfaringene fra Ukraina tilsier at norsk kraftforsyning vil være et hovedmål i en eventuell krig. Rapporten peker på at militære angrep mot Norge kan inkludere angrep på rominfrastruktur, spesielt GPS-systemer som kraftforsyningen er avhengig av, samt elektromagnetisk puls-angrep som kan slå ut strøm, kommunikasjon og datasystemer.

Etterretning

Politiets sikkerhetstjeneste vurderer at Russland allerede har kartlagt store deler av den kritiske infrastrukturen i Norge (2024), og at arbeidet med å kartlegge og identifisere sårbarheter i norsk kritisk infrastruktur vil fortsette (2025). Samtidig er Norge et etterretningsmål for Kina, og PST forventer at etterretningstrusselen fra Kina vil øke på sikt. Økonomisk posisjonering, gjennom oppkjøp og salg av varer og tjenester, kan også muliggjøre etterretning. Informasjon skaffet gjennom etterretning kan senere brukes av fremmede stater for etterretnings-, påvirknings- og sabotasjeaktivitet, eller i ytterste konsekvens i en eventuell fremtidig væpnet konflikt. Vi må forvente at trusselaktører vil fortsette å kartlegge norsk infrastruktur og leverandørkjedene til kraftforsyningen.

Bruk av rapporten

Den strategiske interessen og eksempler på virkemiddelbruk fra fremmede stater tyder på at norsk kraftforsyning må forvente å bli utsatt for etterretning, forsøk på økonomisk posisjonering, påvirkningsoperasjoner og muligens sabotasje, både i form av dataangrep og angrep på fysisk infrastruktur. I en krig forventer FFI og Etterretningstjenesten at kraftforsyningen vil være et prioritert mål. Det er derfor viktig for samfunnet at kraftforsyningen er rustet til å håndtere slike trusler. Vi håper rapporten vil bidra til å gjøre ledelse og ansatte i kraftforsyningen mentalt forberedt på bruk av virkemidler som maktposisjonering og -påvirkning, sabotasje og militære angrep, slik at flest mulig situasjoner kan håndteres med fatning der de oppstår.

Videre håper vi at rapporten kan brukes som et kunnskapsgrunnlag i vurderingen av mulige videre tiltak for å gjøre systemet mest mulig robust. Kraftforsyningen kan bidra til samfunnssikkerheten og totalforsvaret ved *effektivt* å gjøre det mest mulig ressurskrevende for fremmede stater å samle etterretningsinformasjon, etablere maktposisjoner og gjennomføre sabotasje.

1 Introduksjon

1.1 Kraftforsyningens betydning for norsk og europeisk sikkerhet

Pålitelig kraftforsyning er avgjørende for samfunnet. Av en samlet energibruk i Norge på 316 terrawattimer (TWh) i 2023, stod elektrisk kraft for 136 TWh, eller 43 prosent av samlet energibruk (NVE, 2024). Den reelle betydningen av kraftforsyningen er større enn det andelen på 43 prosent tilsier, ettersom forsyningen av fjernvarme, drivstoff og andre energibærere delvis er avhengig av elektrisk kraft.

Kraftforsyningens betydning øker med elektrifiseringen av transportsektoren og olje- og gassproduksjonen på sokkelen. Sistnevnte bidrar til at kraftforsyningen får en stadig større betydning for forsyningen av olje og gass til Europa, som var på rundt 2 300 TWh i 2021 (Sokkeldirektoratet, 2022). Etter bortfallet av russisk gass i 2022 er Norge blitt Europas største gassleverandør (Sokkeldirektoratet, 2023).

Russlands invasjon av Ukraina påvirket energiforsynings-sikkerheten i Europa, og resulterte i en betydelig økning i energiprisene og en påfølgende energikrise (SINTEF, 2024). Krigen og krisen har tydeliggjort vår avhengighet av et kraftsystem som kan levere stabilt og med økonomisk bærekraftige strømpriser, selv under store omveltninger. Samtidig er det av betydning for Norge å ha et kraftsystem som i størst mulig grad ivaretar miljø- og klimahensyn. Endringene kraftforsyningen står overfor karakteriseres av en stor utfordring: Å balansere hensyn til klima og miljø, økonomi og forsyningssikkerhet – et såkalt energitrilemma – som alle har innvirkning på nasjonale sikkerhetsinteresser (NSM, 2023).

1.2 Mandat og målgruppe

Selv om aktuelle trusler mot norsk kraftforsyning begynner å bli godt dokumentert, er det fortsatt varierende i hvilken grad sentrale aktører og personer i kraftforsyningen er bevisste på hvilke virkemidler de er eller kan bli utsatt for.

NVE har gjennom dette oppdraget fått bistand fra THEMA og FFI til å utarbeide en tilgjengelig og oppdatert beskrivelse av truslene mot norsk kraftforsyning. Målet kan være å sikre at flest mulig relevante personer, både hos bedrifter og myndigheter, får en riktig og oppdatert forståelse av de truslene kraftforsyningen står ovenfor. Vi har derfor lagt vekt på å bruke et mest mulig vanlig og tilgjengelig språk i rapporten, samt å vise til konkrete eksempler. Arbeidet er gjennomført mellom november 2024 og februar 2025.

Målgruppen for rapporten er ledelse og ansatte i kraftforsyningen. Innholdet er tilpasset målgruppen ved å fokusere på konsepter og eksempler med relevans for kraftforsyningen, og ved å presentere disse på en måte som tydelig og forståelig bidrar til å danne et bilde av trusselsituasjonen. Enkelte sikkerhetsfaglige konsepter som kunne vært relevante i en mer militærfaglig sammenheng, er enten forenklet eller utelatt.

1.3 Informasjonskilder

Det foregår et kontinuerlig arbeid med å oppdatere trusselvurderinger og iverksette nødvendige tiltak for å sikre kraftforsyningen. Av spesiell relevans kan vi nevne FFIs studie (2023) som analyserte tilsiktede handlinger mot norsk kraftforsyning. I tillegg til denne studien har FFI gjennomført en analyse av teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser (2023), en rapport om innsiderisiko (2023), samt analyser av sammensatte trusler (2023), og cyberoperasjoner (2023).

Videre har FFI publisert en analyse av Russlands cyberkrigføring (2022), sammenstilt erfaringer fra krigen i Ukraina (2024), og publisert en serie artikler om økonomisk statshåndverk (2024), (2022) og (2022).

Det finnes også flere andre nasjonale kilder som belyser trusler mot norsk kraftforsyning. Blant disse er Totalberedskaps-kommisjonen (2023), NSM sin risikovurdering «Risiko 2024:

Nasjonal sikkerhet» (2024), PST sine «Nasjonal Trusselvurdering 2024» (2024) og «Nasjonal Trusselvurdering 2025» (2025), Etterretningstjenestens trusselvurdering «Fokus 24» (2024), KraftCERT sine trusselvurderinger (2024) (2023), samt FFIs rapport «Scenarioklasser for forsvarsplanlegging» (2022).

I tillegg finnes det flere relevante internasjonale artikler, som blant annet NATO-rapporten "Energy Security in the Era of Hybrid Warfare" (2021), ENISAs "Threat Landscape 2024" (2024), samt en rekke rapporter fra Totalförsvarets forskningsinstitut i Sverige.

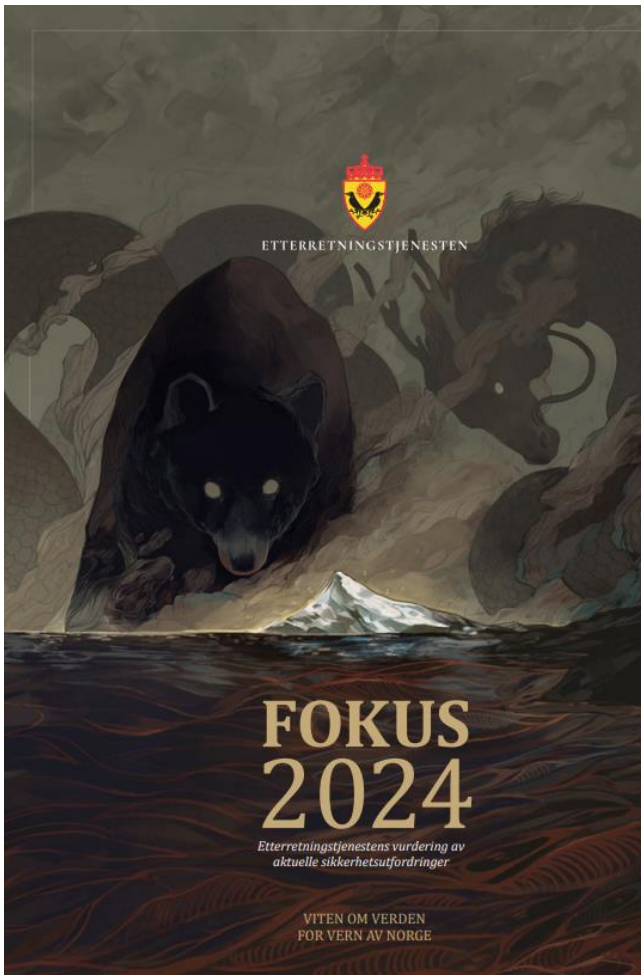
Flere av kildene omhandler såkalt «hybrid virkemiddelbruk», et tema som behandles nærmere i rapporten. Disse kildene inkluderer blant annet «Hybrid threats: A Comprehensive Resilience Ecosystem» (EU & Hybrid CoE, 2023), «MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare» (MCDC, 2017), samt "Russia's hybdrid threat tactics against the Baltic Sea Region: from disinformation to sabotage" (Hybrid CoE, 2024).

Som en del av arbeidet har vi gjennomført en workshop med forskere hos FFI og hatt flere statusmøter og utvekslinger med representanter fra NVEs tilsyns- og beredskapsavdeling og KraftCERT. For en fullstendig liste over kilder viser vi til referanselisten i rapporten.

1.4 Rapportstruktur

Rapporten er strukturert som følger: I kapittel 2 beskriver vi trusselaktørene for norsk kraftforsyning, og avgrenser den videre analysen til aktører som kan true selve kraftforsyningen i Norge. I kapittel 3 gir vi en introduksjon til rammeverket vi bruker for å beskrive trusselbildet for kraftforsyningen. I kapittel 4 beskriver vi hvordan maktposisjonering, påvirkning og tvang kan utgjøre en trussel. I kapittel 5 beskriver vi hvordan digital og fysisk sabotasje kan rettes mot kraftforsyningen. I kapittel 6 omtaler vi trusselen fra militære angrep rettet mot fysisk infrastruktur og rominfrastruktur, samt trusselen fra elektromagnetiske pulsangrep. I kapittel 7 omtaler vi etterretning mot kraftforsyningen, herunder etterretning i det fysiske rom, etterretning i det digitale rom og gjennom personell/innsidere. I etterordet (kapittel 8) deler vi kilder som virksomheter i kraftforsyningen kan ta utgangspunkt i for å holde seg oppdatert på trusselbildet og få informasjon om hvordan de kan bidra til å styrke forsyningssikkerheten.

E-tjenestens rapport: Fokus 2024



2 Trusselaktører

En trusselaktør er i denne sammenhengen en organisasjon, en gruppe eller enkeltaktør som har gjennomført eller kan tenkes å gjennomføre et angrep eller en tilsiktet handling mot kraftforsyningen i Norge. I dette kapitlet beskriver vi trusselaktørene som de norske etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-tjenestene), samt Politiet, vurderer som de mest relevante for norsk kraftforsyning.

2.1 Nye sikkerhetspolitiske rammebetingelser

Ifølge Etterretningstjenesten (2024) er forholdet mellom Russland og Vesten på et lavmål, og russisk politikk overfor Vesten og Norge forventes å bli mer uforutsigbar i årene som kommer. Utviklingen kan føre til økt risiko for misforståelser, ulykker og eskalering. Både Russland og Kina har en målrettet agenda om å endre verdensordenen slik at den i større grad ivaretar deres interesser. Nasjonal sikkerhetsmyndighet (NSM) vurderer at det er fare for at fremmede staters, herunder Russland og Kinas, bruk av teknologi kan utvikle seg raskere enn åpne demokratiers evne til å beskytte seg (NSM, 2024). Samtidig som Russland og Kina utgjør hovedtruslene, forventer PST også aktivitet fra Iran og Nord-Korea mot norske mål (2025).

2.2 Russland og russiskstøttede aktører

Et hovedmål for Russland er å svekke Vestens vilje til å støtte Ukraina, og presset mot Europas energiforsyning vil derfor fortsette. Rask utfasing av russiske gassforsyninger har gjort Norge til Europas viktigste energileverandør. Dette har styrket Norges geopolitiske betydning (Etterretningstjenesten, 2023). 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.

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. Samtidig har Russlands krigføring i Ukraina avdekket svakheter i Russlands militære evne (Etterretningstjenesten, 2023). Til gjengjeld har Russland utviklet en omfattende samling av metoder og virkemidler under nivået for direkte militær maktbruk, som er tilpasset landets strategiske stilling i forhold til NATO (FFI, 2022).

Etterretningstjenesten (2023) vurderer at Russland vil forsøke å videreutvikle strategien om strategisk overfall[1]. FFI (2022) anser at Russland i uoverskuelig fremtid er den eneste staten med kapasitet og motiv til å gjennomføre et konvensjonelt militært angrep mot Norge. I et væpnet angrep mot Norge og NATO vil ødeleggelse av kritisk sivil infrastruktur, herunder kraftforsyning, få prioritet tidlig, og varslingstiden vil være svært kort (Etterretningstjenesten, 2023).

2.3 Kina og kinesiskstøttede aktører

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 teknologi-utvikling, selvforsyning og kulturell sikkerhet. Kina viderefører

[1] Strategisk overfall er en situasjon hvor en stat setter inn store militære styrker for å etablere militær kontroll over deler av en annen nasjons territorium, typisk en landsdel (FFI, 2022).

en offensiv utenrikspolitikk med mål om en regional og global lederposisjon og et mer Kina-orientert internasjonalt system.

Et eksempel på Kinas forsøk på økt global kontroll er situasjonen i Sør-Kinahavet, der Kina kombinerer virkemidler som økonomi, informasjon, diplomati, jus og bygging av infrastruktur og kunstige øyer for å gjøre krav på havområder. Samtidig ruster Kina opp for å avskrekke Kinas naboer fra å foreta seg noe (NUPI, 2016).

Økonomisk styrke forblir Kinas viktigste maktmiddel. Etterretningstjenesten (2023) vurderer at *silkeveistrategien*, som har gitt Kina økonomisk makt gjennom omfattende infrastrukturprosjekter og investeringer i andre land, forblir et viktig virkemiddel for å søke global innflytelse, og vil dreies ytterligere mot investeringer i digital infrastruktur og fornybar energi.

Politiets sikkerhetstjeneste (2025) forventer at trusselen fra Kina vil øke de nærmeste årene, som følge av det forverrede forholdet mellom Kina og Vesten, samt Kinas ønske om økt kontroll over forsyningskjeder og posisjonering i Arktis. Kinesisk etterretning vil fortsette innsatsen for å innhente informasjon om Norge, blant annet gjennom å rekruttere norske borgere for å få tilgang til sensitiv og gradert informasjon. Ofte er dette personer som har tilknytning til Kina i form av studier, arbeid, venner eller familie. I tillegg vil Kina fortsette å bruke ulike virkemidler for å forsøke å stilne kritiske stemmer og påvirke grupper og enkeltpersoner i Norge.

Kina bruker i flere sammenhenger aktører uten offisiell tilknytning til Kina for å nå sine mål, for eksempel hackergruppene som stod bak datainnbruddene hos Stortinget og statsforvalterembetet (se kapittel 7.2). Kinas etterretnings-tjenester benytter i stor grad sivile personer med tilgang til informasjon. Disse bruker sin posisjon frivillig eller under press. Enhver kinesisk borger eller virksomhet kan ifølge kinesisk lovverk pålegges å samarbeide med landets etterretnings-apparat. Resultatet er at det er svært utfordrende/ umulig å skille mellom rent kommersielle kinesiske aktører og aktører som utnyttes til etterretningsformål (PST, 2022).

Kinas dominans i forsyningskjeden for kritiske mineraler

Sjeldne jordarter lastes for eksport ved havnen i Lianyungang i Øst-Kina (Foto: Imaginechina Limited / Alamy)

Kina dominerer og kontrollerer i stor grad verdikjedene for kritiske mineraler. Landet står for omtrent 70 prosent av verdens utvinning av sjeldne jordarter, og kontrollerer 85–100 prosent når prosesseringen av disse inkluderes (Finansavisen, 2024).

Bekymringen øker for at Vestens avhengighet av import av kritiske mineraler fra Kina, som er essensielle for produksjonen av blant annet fornybar energiteknologi, kan gi Kina økt makt og en strategisk fordel over Vesten. Dette har blant annet ført til at EU har satt et eksplisitt mål om å "redusere risiko fra Kina" (*derisking*) for å adressere EUs økonomiske og teknologiske avhengighet (EU, 2024).

Et eksempel på at Kina utnytter sin dominans i verdikjeden for å utøve makt, er hendelsen i 2010 da Kina, etter en territorial konflikt, innførte et to måneder langt eksport-forbud for sjeldne jordarter, spesielt rettet mot Japan (Rusi, 2024). Dette førte til at Japan endret sin tilnærming til mineralavhengige industrier og forsyningskjeder.

2.4 Ikke-statlige aktører

Terrorister

PST (2025) vurderer det som mulig at ekstreme islamister og/eller høyreekstreme vil forsøke å gjennomføre terrorhandlinger i Norge i 2025. PST vurderer det som lite sannsynlig med terrorangrep fra anti-statlige aktører og svært lite sannsynlig med angrep fra venstreradikale og miljøaktivister (2024).

Kriminelle og samarbeid mellom kriminelle og fremmedstater

Politiets vurdering er at trusselen fra organiserte kriminelle nettverk er betydelig og økende, blant annet på grunn av økt profesjonalisering, grensekryssende samarbeid og stadig mer komplekse forretningsmodeller (Politiet, 2024).

Digitaliseringen av samfunnet og integreringen av økonomier og arbeidsmarkeder øker mulighetene for grensekryssende økonomisk kriminalitet. Politiet ser at kriminelle organiserte nettverk har direkte eller indirekte kontroll over foretak, og det benyttes profesjonelle aktører og stråpersoner for å skjule kriminelle handlinger og eierskap. Samtidig trues deler av velferdsstatens finansieringsgrunnlag gjennom arbeidslivs-kriminalitet (Politiet, 2024).

Politiet relaterer endringer på cyber-kriminalitetsfeltet til den geopolitiske utviklingen og nye teknologiske muligheter. De cyberkriminelle fortsetter å utvikle og tilpasse teknikker, metoder, verktøy og strategier, blant annet for å omgå mottiltak fra offentlige og private virksomheter. Flertallet av de cyberrettede kriminelle lovbruddene i 2023 var både opportunistiske og profittmotiverte (Politiet, 2024). Ett datainnbrudd kan gi angriperne flere verdier, for eksempel både profitt for organisasjonen som utfører den, og etterretningsverdi for statene som støtter organisasjonene. Det er verdt å merke seg at kriminelle dataangrep kan gi uforutsette og større skadevirkninger enn det angriperen har hatt som hensikt.

2.5 Analysen avgrenses til trusler fra stater og statsstøttede aktører

Det finnes eksempler på at kriminelle utfører fysiske tyverier fra kraftanlegg, samt datainnbrudd som tilsiktet eller utilsiktet forstyrrer energiforsyningen. Det finnes også eksempler på fysiske sabotasjeangrep på kraftforsyningen fra ikke-statlige grupper, som høyreekstreme i USA. Vår vurdering er imidlertid at kriminelle grupper og ikke-statlige aktører per i dag ikke har kapasitet til å true kraftforsyningen i Norge på samme måte som stater som Russland og Kina, eller russisk- og kinesiskstøttede aktører.

Den videre analysen av trusselbildet for kraftforsyningen er derfor basert på en analyse av trusler fra fremmede stater og statsstøttede aktører.

3 Rammeverk for å forstå trusselbildet for norsk kraftforsyning

Tradisjonelt er fred, krise og krig betraktet som steg på en alvorlighetslinje. Slike sekvensielle steg er stadig oftere upresise størrelser for å forstå den nye sikkerhetssituasjonen. Norsk sikkerhet blir direkte og indirekte utfordret av flere aktører, på flere arenaer, hjemme og ute, hver dag (Totalberedskapskommusjonen, 2023). På grunnlag av blant annet FFIs artikler om handlinger som kan true norsk kraft-forsyning (2023) og scenarioklasser for forsvarsplanlegging (2022) har vi definert tre hovedkategorier av trusler[2] som norsk kraftforsyning bør være forberedt på:

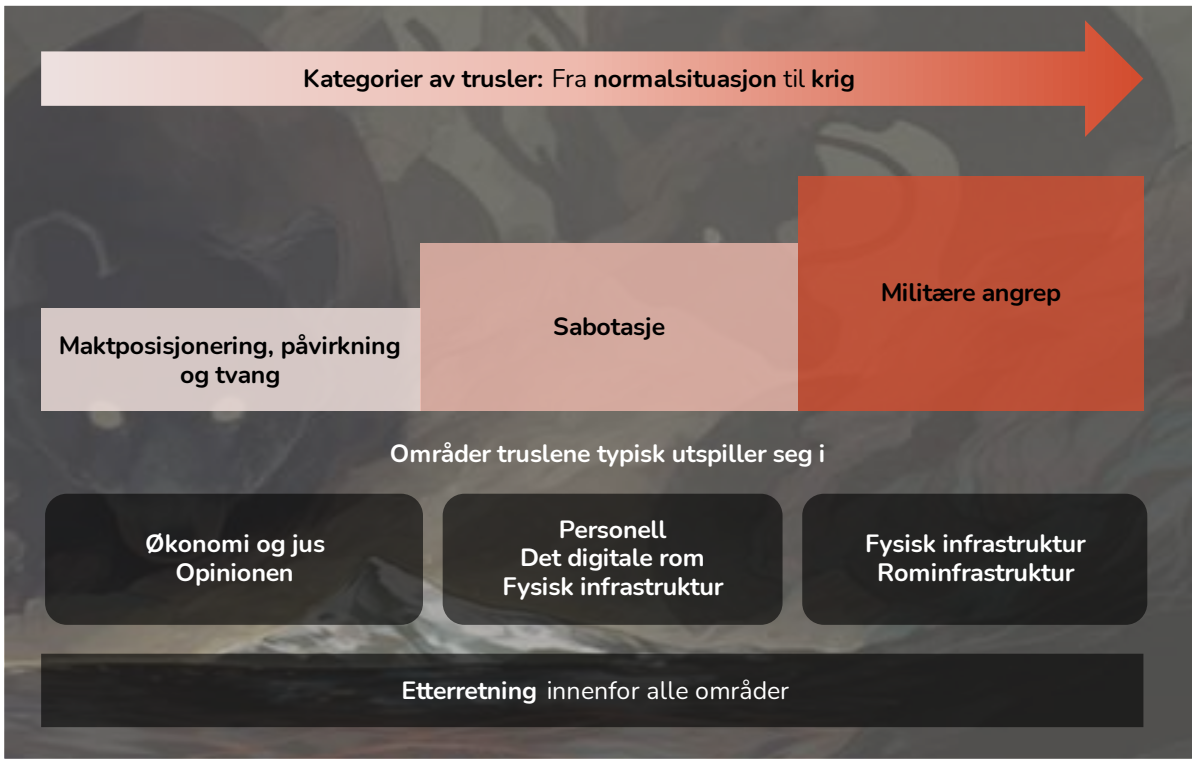
- Maktposisjonering, påvirkning og tvang
- Sabotasje (både i det digitale og fysiske rom)
- Militære angrep

I tillegg omtales etterretning, som stater bruker for å vurdere slike trusler og identifisere relevante virkemidler.

Truslene kan berøre flere områder [3], inkludert økonomi og jus, i opinionen, hos personell i kraftforsyningen, i det digitale rom, i det fysiske rom og i verdensrommet.

Som vi vil redegjøre nærmere for i de neste kapitlene, er Norge og Norges allierte allerede i dag utsatt for kategoriene etterretning, maktposisjonering, påvirkning og forsøk på tvang, samt sabotasjeangrep (digitale og fysiske angrep). Norge og NATOs kraftforsyning er ikke utsatt for militære angrep i dag, men sektorens betydning og erfaringene fra Ukraina tilsier at norsk kraftforsyning vil være et hovedmål i en eventuell krig.

Figur 1: Utvalgte trusler mot kraftforsyningen på en skala fra normalsituasjon til krig



[2] En trussel er en risikokilde som vanligvis er knyttet til ønskede eller planlagte handlinger (SNL, 2023).

[3] Områdene tilsvarer sikkerhetsdomenene som er definert av NSM (2023).

Virkemidler som sabotasje kan ha mål utover det å skade eller forstyrre kraftforsyningen i seg selv. Slike virkemidler kan være en del av en fremmed stats større plan for å skape mistillit i befolkningen og/eller legge press på norske myndigheter til å fatte eller avstå fra visse politiske vedtak.

Truslene som beskrives – maktposisjonering, påvirkning og tvang, sabotasje, militære angrep og etterretning – er ikke gjensidig utelukkende og forekommer heller ikke i isolasjon. Tvert imot kan de kombineres for å oppnå en større og mer målrettet effekt. *Sammensatte trusler* er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt (FFI, 2023a). Sammensatte trusler omtales noen ganger som «gråsoneaktiviteter» eller «gråsonekonflikter». Begrepet *hybride trusler* inkluderer alle virkemidler som ligger i sammensatte trusler, men inkluderer også regulære militære virkemidler.[4]

Som FFI har påpekt kan begrepene sammensatte trusler og hybride trusler være uklare og forvirre mer enn de oppklarer. Overordnet handler begrepene om at aktører, som for eksempel stater, tar i bruk hele verktøykassen av tilgjengelige virkemidler for å nå sine mål. Dette gjøres imidlertid gjerne i det skjulte for å unngå direkte konflikt, og innebærer ofte at aktørene gjennomfører skjulte handlinger som forsøker å manipulere andre staters interesser, som ved å så tvil i befolkningen, svekke demokratiske institusjoner, eller påvirke statens handlefrihet på andre måter. Eksempler på slike virkemidler er oppkjøp av eiendom, påvirkningsoperasjoner mot befolkningen og sabotasje (FFI, 2023a).

Vår vurdering at det er mer nyttig for ledelse og ansatte i kraftforsyningen å fokusere på trusselkategoriene «maktposisjonering, påvirkning og tvang», «sabotasje», «militære angrep» og «etterretning» enn å fokusere på begreper som sammensatte trusler, hybride trusler og gråsonekonflikter. Vi fokuserer derfor på de nevnte kategoriene i det videre, samtidig som vi omtaler hvordan disse kan inngå i et større bilde og som deler av en mer omfattende virkemiddelbruk.

Energisektoren er et mål for sammensatte trusler

Flere har pekt på hvordan energisektoren i økende grad er blitt et mål for sammensatte/ hybride trusler, spesielt fra Russland (NATO, 2021). Eksempelvis har Russland gjennomført påvirkningskampanjer for å undergrave forslag om å gjøre Bulgaria og Romania mindre avhengige av russisk gass og gjennomført dataangrep mot energiforsyningen i Polen, Tyrkia, Storbritannia og USA (NATO, 2024). Russlands aktiviteter mot de baltiske landene inkluderer virkemidler som påvirkningskampanjer (desinformasjon), dataangrep, politisk press, migrasjon og sabotasje (Hybrid CoE, 2024). I den senere tid er flere handelsfartøy med tilknytning til Russland og Kina blitt mistenkt for å skade undersjøisk infrastruktur i Østersjøen.

[4] Sammensatte eller hybride trusler kan defineres som «synkronisert bruk av ulike virkemidler, rettet mot sårbarheter i samfunnet som helhet, med mål om å oppnå synergiskadevirkninger» (MCDC, 2017). Dette innebærer at flere typer virkemidler kan kombineres for å oppnå en samlet effekt som er større enn summen av de enkelte virkemidlene. Slike virkemidler kan rettes mot sårbarheter innen politikk, samfunn, infrastruktur, informasjon, økonomi og militærvesen.

For vestlig sikkerhetspolitikk utgjør hybrid krigføring en betydelig utfordring. Dette skyldes blant annet at hybrid krigføring er utydelig og vanskelig å identifisere, noe som gjør det utfordrende å etablere en samordnet respons innad i for eksempel NATO og EU (NUPI, 2016). Slik kan hybride taktikker skape handlingslammelse og undergrave styringsevnen og den politiske beslutningstakingen i statene som rammes. En annen utfordring for Norge og NATO er at autoritære stater, som for eksempel Russland, kan bruke skjulte og kontroversielle virkemidler som demokratiske og ikke-autoritære land ikke kan ta i bruk like lett.

4 Maktposisjonering, påvirkning og tvang

Tradisjonelt har stater benyttet militære maktmidler for å forsvare sin suverenitet, territorium og befolkning, og for å dominere andre stater. Det er nå økt fokus på hvordan andre virkemidler kan benyttes for å oppnå strategiske mål (Waage, et al., 2021). Det kan være mer effektivt for en fremmedstat å få Norge til å gjøre som de vil gjennom påvirkning av ordskiftet, opinionen og beslutningstakere, og/eller gjennom åpne eller skjulte trusler om økonomiske sanksjoner, enn gjennom direkte militære angrep. I kraftforsyningens tilfelle vil det ikke nødvendigvis kun være effektivt for en fremmed stat å ødelegge eksisterende anlegg gjennom sabotasje eller militære angrep; de kan også tenkes å bruke påvirkning eller maktposisjonering til å hindre at nye anlegg bygges. I dette kapitlet vil vi omtale hvordan maktposisjonering, påvirkning og tvang rettet mot energisektoren kan utspille seg i økonomien og opinionen.

4.1 Økonomisk posisjonering og makt

Hva er økonomisk makt?

Begrepet makt er sentralt for å forstå hvordan økonomiske virkemidler kan brukes av stater for å oppnå sine mål. Tradisjonelt lyder maktdefinisjonen som legges til grunn i studier av internasjonal politikk som følger: "A har makt over B i den grad A kan få B til å gjøre noe B ikke ellers ville gjort" (Dahl 1957, sitert av Waage, et al (2021)). En stat med økonomisk makt, for eksempel over leverandørkjeden til norsk kraftproduksjon eller eierskap til kraftproduksjon- eller distribusjon direkte, kan bruke denne til å tvinge eller motivere norske politikere eller andre sentrale aktører til å endre oppførsel og/eller beslutninger, for eksempel gjennom trusler om forstyrrelser i leveransene.

Økonomisk posisjonering betegner en bevisst strategi for å etablere et maktforhold med sikte på å utnytte avhengighetene som er etablert i en fremtidig konkurranse- eller konfliktsituasjon. Avhengighetsforhold kan være teknologiske, for eksempel knyttet til drift og vedlikehold av kritisk infrastruktur. Etablering av monopol eller kontroll over deler av en verdikjede kan også skape avhengighetsforhold (FFI, 2022). Globaliseringen øker mulighetene til å bruke økonomisk virksomhet som metode for å skape avhengigheter og sårbarheter som tidligere ikke eksisterte (FFI, 2022). Som svar på dette har flere land innført screeningsmekanismer for utenlandsinvesteringer de senere årene. I Norge trådte en ny lov for nasjonal sikkerhet i kraft i 2019 (Waage, et al., 2021). I 2022 nedsatte regjeringen Eierskapskontrollutvalget, et offentlig utvalg som skal utrede behovet for screening av økonomisk aktivitet mot virksomheter som ikke er omfattet av sikkerhetsloven (NSM, 2023).

Virkemidler for økonomisk maktposisjonering

Virkemidler for å oppnå økonomisk makt omfatter blant annet investeringer, handel, lån og forskningssamarbeid, alt på tilsynelatende fordelaktige vilkår. Når den posisjonen først er blitt oppnådd kan den gi bedre grunnlag for etterretning, bruk av juridiske virkemidler, påvirkning og sabotasje (NSM, 2023). PST forventer at både Russland og Kina vil forsøke å sikre nasjonale sikkerhetsinteresser gjennom innvesteringer i og oppkjøp av selskaper og eiendom i Norge. Dette kan blant annet innebære strategiske oppkjøp av eiendom i nærheten av kritisk infrastruktur for å muliggjøre etterretning (PST, 2025).

I 2021 ble det kjent at Bergen Engines, en produsent av dieselmotorer for skip ved Hordvikneset i Bergen, hadde inngått en avtale om å bli kjøpt opp av det russiske selskapet Transmashholding (E24, 2021). Blant Bergen Engines' største kunder var det norske Sjøforsvaret, og oppkjøpet ville medført at spionskipet Marjata, ett av Norges mest sensitive fartøy, ville blitt vedlikeholdt av russisk personell (TU, 2021). Det kom også frem at United Shipbuilding Corporation, Russlands største produsent av marinefartøy og krigsskip, underlagt amerikanske sanksjoner, planla et samarbeid med Transmashholding for teknisk utvikling av skipsmotorer (TU, 2021).

Nord Stream 2

Illustrasjon: Samuel Bailey (CC BY 3.0)

"Som jeg har sagt ved gjentatte anledninger er dette et rent kommersielt prosjekt, uten politiske baktanker"

President Vladimir Putin, 15. februar 2022

Norske myndigheter besluttet til slutt å stanse oppkjøpet av sikkerhetshensyn. Bekymringen var at Russland på en fordekt måte kunne få tilgang til kunnskap og teknologi av stor strategisk militær betydning for Russland.

Et annet eksempel på økonomisk maktposisjonering er gassrørledningen Nord Stream 2 mellom Russland og Tyskland. Kritikere hevdet at gassledningen ikke var et rent økonomisk prosjekt, slik både den russiske og tyske regjeringen lenge påstod, men snarere et eksempel på økonomisk posisjonering for å muliggjøre senere maktbruk.

Kritikerne, blant annet USA, pekte på at rørledningen kunne gjøre det mulig for Russland å øke EUs avhengighet av russisk gass, samtidig som den ville gjøre russisk gasseksport mindre avhengig av transitt gjennom Ukraina. Sistnevnte forhold kunne igjen gjøre det lettere for Russland å bruke gassforsyningen til å presse gjennom politiske målsetninger i Ukraina (Mills, 2022), (Politico, 2021).

Flere er bekymret for at Kina er i ferd med å etablere en lignende økonomisk maktposisjon innenfor verdikjedene for blant annet solkraft, vindkraft og batterier, som det Russland har hatt og fortsatt har innenfor verdikjedene for olje og gass.

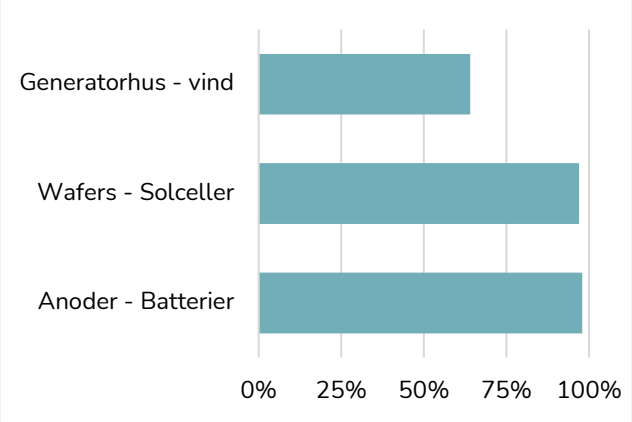
Amerikanske myndigheter tok i 2020 beslag i en kinesisk transformator som skulle installeres i Colorado, som de fryktet kunne bli brukt til å skade strømnettet i USA. Kort tid etter vedtok amerikanske myndigheter at «Foreign adversaries», som Kina, ikke får levere kritisk utstyr til strømnettet (NATO, 2021).

Litauen vedtok mot slutten av 2024 en lovendring for å hindre kinesiske selskaper i å få fjernadgang til kontrollsystemene for sol- og vindparker og større batterier i nettet, på grunn av bekymringer om at kinesisk-produserte og fjernstyrte kontrollsystemer i kraftforsyningen kunne utgjøre en trussel (LRT, 2024).

Det internasjonale energibyrået (IEA) har definert seks nøkkelteknologier for utslippsfri kraftproduksjon: Solceller, vindmøller, elektriske biler, batterier, elektrolysører og varmepumper. Kina står for rundt 70 prosent av verdensproduksjonen for flere av disse teknologiene i dag, og har økt sin markedsandel siden 2021 (IEA, 2024).

Den siste norske solcelleprodusenten, Norsun i Årdal, gikk konkurs i desember 2024. I pressemeldingen i forbindelse med konkursen pekte Norsun på at det europeiske solenergimarkedet har vært under betydelig press fra overkapasitet i Kina og Sørøst-Asia med påfølgende salgspriser i Europa under produksjonskost (NorSun, 2024).

Kinas andel av verdensproduksjonen i et utvalg av fornybarteknologier



"Kinas største solcelleproduksjonsanlegg kan lage nok moduler til å dekke all EU-etterspørsel i dag" IEA (2024).

I tillegg til å etablere seg som en hovedleverandør av produksjonsteknologier, gjennomfører Kina oppkjøp i selve kraftproduksjonen og nettvirksomheten i Europa. Kina har over en lang periode har drevet strategiske oppkjøp i energisektoren i Europa. Enkelte nettselskap i Portugal, Hellas og Italia har i dag kinesiske selskaper i sin eierstruktur (GEG, 2021).

Sanksjoner: Bruk av økonomisk makt

Sanksjoner er tiltak – politiske, diplomatiske, økonomiske eller lignende – som kan iverksettes for å legge press på norske og andre lands myndigheter gjennom å true med eller påføre kostnader. Sanksjoner kan være formelle, eller uformelle/ fordekte, hvor intensjon og metode ikke kommuniseres åpent.

Et eksempel på bruk av økonomisk makt er Russlands begrensninger på gasstilførselen til Europa i forkant av og etter fullskalainvasjonen av Ukraina 24. februar 2022. Et annet eksempel er de uformelle politiske og økonomiske sanksjonene Kina iverksatte mot Norge etter tildelingen av Nobels fredspris til Liu Xiaobo i 2010.

En utfordring med å beskrive kinesisk økonomisk maktbruk er at Kina sjelden, om noensinne, eksplisitt innrømmer å ha benyttet det. Ofte forklares handlinger som kan fremstå som straff eller press mot mottakerlandet, for eksempel importforbud eller stans i turisme, med andre hensyn enn utenrikspolitiske og strategiske interesser. I mange tilfeller oppgis bekymringer rundt matkvalitet eller sikkerheten til kinesiske borgere på ferie i utlandet som begrunnelser. Selv sanksjonene mot norsk laks etter utdelingen av Nobels fredspris til Liu Xiaobo i 2010, var i stor grad fordekte. For eksempel var det helseinspeksjoner som stanset norske SalMar fra å eksportere laks til Kina i perioden (FFI, 2022).

Mulig scenario: Bruk av juridiske virkemidler

Økonomisk makt kan gi både rettslig interesse gjennom investeringer og handel, og midler til å finansiere juridiske konflikter på en fordekt måte, gjennom organisasjoner uten åpenbar tilknytning til fremmedstaten. En mulig sårbarhet for norsk og europeisk kraftforsyning er at aktører støttet av fremmedstater kan utnytte rettsvesenet til å forsinke prosesser som skal styrke kraftproduksjonen og kraftnettet. Dette kan på sikt gjøre kraftforsyningen mer sårbar.

4.2 Påvirkning av opinionen og beslutningstakere

Opinionen, politikk og kognitiv påvirkning

Politikk er all aktivitet som bidrar til felles handling og fordeling av verdier i grupper, internt i land og mellom land. Politikken påvirkes av agendaen, som settes av aktørenes og menneskenes erfaringer, observasjoner og meninger (Harris, 2006). Kommunikasjons- og informasjonsteknologi – spesielt sosiale medier – har radikalt endret fremmedstaters muligheter for å påvirke individers tanker og meninger for blant annet sikkerhetspolitiske formål (se Bergh 2020). «Kognitiv påvirkning» kan i denne sammenhengen defineres som tiltak for å manipulere prosessene som bearbeider data til informasjon og kunnskap hos et individ eller en gruppe (FFI, 2022). Det er mye rimeligere og mindre risikofylt for en stat å påvirke befolkningen i et annet land til å gjøre som de vil enn å forsøke å oppnå det samme gjennom tradisjonell militærmakt.

Påvirkningsoperasjoner

En påvirkningsoperasjon innebærer at en fremmed makt forsøker å påvirke folkemeningen eller vedtak som skal fattes av styrende organer (NAOB, 2024). Påvirkningsoperasjoner kan gjøres gjennom sosiale medier, tradisjonelle medier, agitering og/eller påvirkning av ledende enkeltpersoner.

Kinesisk interesse for norske beslutningsprosesser

Etterretningstjenestens (2022) vurdering er at Kina viser økende interesse for innsyn i norske beslutningsprosesser. Som et eksempel kan vi nevne de to dataangrepene mot Stortinget i 2021. I den første ble epostene til Stortingets fremste Kina-kritiker, Michael Tetzschner, hentet ut. I den andre operasjonen, som er blitt knyttet til Kina, fikk angriperne tilgang til Stortingets epostserver.

Russiske påvirkningsoperasjoner mot opinionen

Det pågår en omfattende russisk påvirkningsoperasjon støttet av kunstig intelligens og rettet spesielt mot meningsdannelsen i Vesten, både generelt og med hensyn til krigen i Ukraina (FFI, 2024). Frankrike sier at Russland stod bak graffitien på 250 Davidsstjerner i Paris i november 2024, i et forsøk på å gi næring til antisemittisme som allerede finnes (Economist, 2024).

V4-landene varsler om russiske påvirkningsoperasjoner for å svekke energidiversifisering i Europa

Witold Waszczykowski, tidligere utenriksminister i Polen (Foto: Public, Wikimedia)

Russisk desinformasjon har hatt en betydelig innvirkning på energisektoren i V4-landene Polen, Tsjekkia, Slovakia og Ungarn (Warzaw Institute, 2024). Etter Russlands invasjon av Ukraina i 2022 økte disse landene innsatsen for å diversifisere energikildene sine, noe Russland har motarbeidet gjennom blant annet desinformasjon og cyberangrep mot kritisk energiinfrastruktur.

Desinformasjonskampanjene har hatt som mål å påvirke opinionen rundt vestlig-orienterte energidiversifiserings-prosjekter og er ofte utformet for å skape tvil om deres effektivitet ved å gi falsk informasjon om ineffektiviteter eller feil ved prosjektene.

I 2022 advarte Polens tidligere utenriksminister, Witold Waszczykowski, om russisk lobbyaktivitet som arbeidet for å øke Vestens avhengighet av russisk energiforsyning, blant annet gjennom påvirkning av opinionen mot utviklingen av atomkraft (EU, 2022).

Et annet eksempel er russiske påvirkningsoperasjoner mot det amerikanske presidentvalget i 2016, som spilte på eksisterende motsetninger mellom folkegrupper og religiøse grupper i USA (Aftenposten, 2016). NSA, CIA og FBI vurderte i ettertid at Putin hadde beordret en påvirkningskampanje med mål om å blant annet undergrave offentlig tro på den amerikanske demokratiske prosessen (NSA, CIA og FBI, 2017).

På samme måte som russiske påvirkningsoperasjoner har rettet seg mot allerede eksisterende etniske motsetninger i Frankrike og USA, kan en se for kan en se for seg at fremtidige påvirkningsoperasjoner mot norsk offentlighet i fremtiden vil spille på allerede etablerte og splittende temaer knyttet til utviklingen av norsk kraftforsyning.

For å svare på trusselen har Norge nylig revidert straffeloven for å kunne straffe «den som på vegne av eller etter avtale med en fremmed etterretningsaktør bidrar i virksomhet som har til formål å påvirke beslutninger eller den allmenne meningsdannelsen» (Justis- og beredskapsdepartementet, 2023-2024).

5 Sabotasje

Sabotasje innebærer å skade, hindre eller forstyrre eiendom, produksjonsmidler eller tekniske systemer med hensikt. Det er blitt økt oppmerksomhet knyttet til sabotasje som et virkemiddel for fremmedstatlige aktører i de senere år, både som følge av økt sabotasjeaktivitet mot europeiske land, og som følge av økt forståelse av slike virkemidlers betydning. I dette kapitlet vil vi omtale sabotasje i det digitale rom og sabotasje mot fysiske anlegg.

5.1 Sabotasje i det digitale rom

Det digitale rom og nye sårbarheter

Digitalisering, altså tilrettelegging for og bruk av ny informasjons- og kommunikasjonsteknologi, har muliggjort sabotasje i form av dataangrep.

Kraftproduksjonen og distribusjonen i Norge er blitt stadig mer fjernstyrt over tid. For å muliggjøre økt elektrifisering og en økt andel uregulerbar og distribuert kraftproduksjon, planlegges det å ta i bruk teknologi som bidrar til økt utnyttelse av det eksisterende kraftnettet. Slike digitaliserte og integrerte kraftsystemer omtales gjerne som «smartgrids» er i såkalte cyber-fysiske systemer. En fjernstyrt og digitalisert kraft-forsyningen kan være sårbar for cyberangrep (FFI, 2023), (NSM, 2023).

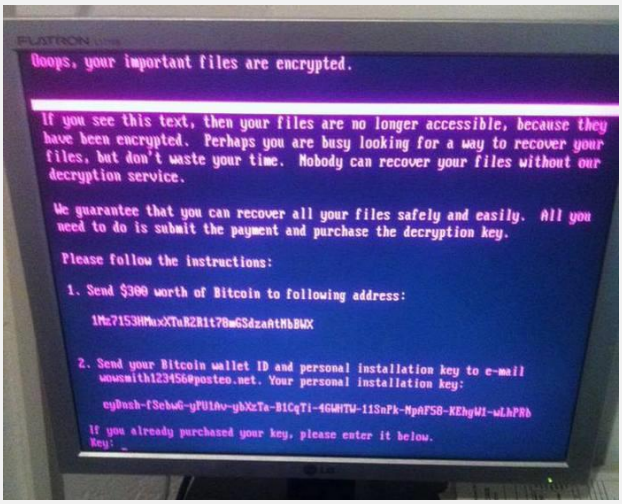
Statnett selv påpeker at de er stadig mer avhengige av IT-systemer for å styre operasjonell teknologi (OT). Koblingen mellom IT og OT innebærer at den digitale og fysiske verden kobles tettere sammen. Dette forsterkes ytterligere av automatisering av balansering med en 15-minutters tidsoppløsning. Når kapasitetsmarkedene for sekundær- og tertiærreserver ikke lenger kan styres manuelt (på grunn av tidsoppløsningen), øker dette avhengigheten av datakvalitet, nettverk og kommunikasjonsløsninger.

En felles nordisk balansemodell (NBM) og etter hvert europeisk kapasitetsmarked vil øke alle former for kompleksitet i kraftsystemet. Alle gevinster til tross, gjør dette kraftsystemet mer sårbart for at et dataangrep får fysiske konsekvenser i nettet og påvirker forsyningssikkerheten (Statnett, 2024).

Hva er dataangrep og hva kan de føre til?

Et dataangrep er et teknisk angrep mot en maskin eller tjeneste som truer deres konfidensialitet, integritet og/eller tilgjengelighet (Store norske leksikon, 2024). For kraft-forsyningen er vi særlig opptatt av dataangrep på kontrollsystemer.

Dataangrep har sjelden ødeleggende effekt



Petya angrep mot ukrainske departementer, banker, aviser og strømforsyning m.m. i 2017 (Foto: Jbuket, CC BY-SA 4.0)

Det er lettere å lykkes med tilgangsangrep, datatyveri og driftsforstyrrende angrep, enn å lykkes med ødeleggende angrep. Ukrainakrigen er et godt eksempel på dette. Krigen har vart i over ti år, og det er kun ett kjent angrep som faktisk har hatt ødeleggende effekt: Angrepet på Viasat/KA-SAT-modemene som satte dem varig ut av spill. De resterende har hatt forstyrrende effekter, inkludert angrepene i 2015 og 2016 som resulterte i strømutfall i store områder i Ukrainske byer (KraftCERT, 2024)

Slike angrep kan kategoriseres etter målsetningene og vanskelighetsgraden for angrepene (KraftCERT, 2024):

1. Tilgangsangrep - For å kunne gjennomføre videre angrep eller for å selge tilgangen til aktører som ønsker denne
2. Datatyveri - For å hente ut informasjon om nettverk og systemer, samt forberede senere angrep
3. Driftsforstyrrelse - Stoppe leveranser gjennom angrep på kontrollsystemet eller støttesystemer
4. Ødeleggelse - Angrep med mål om å ødelegge utstyr, forårsake ytre ødeleggelser og/eller ta liv
5. Kontroll - Ta kontroll over og styre prosesser i kontrollsystemet

Erfaringer fra russiske dataangrep mot Ukraina

De mange russiske dataangrepene på Ukraina i hele perioden etter annekteringen av Krim og intervensjonen i konflikten i Donbas i 2014 gir nyttige læringspunkter. Diesen m. fl. (2024) beskriver at ingen av cyberangrepene hadde en varighet som strakte seg utover noen dager. Det bekrefter hypotesen om at et cybervåpen som skal gi en umiddelbar effekt er en «one shot gun»; når det er brukt, er det også forbrukt. Ingeniørene og programteknikerne som drifter målsystemet for et cyberangrep vil normalt kunne finne skadevaren relativt raskt og gjenopprette systemets integritet, gitt at de har en stor og kompetent driftsorganisasjon.

Dataangrep kan brukes til å svekke befolkningens tillit

Selv om dataangrep per i dag vurderes å ha mindre skadepotensial enn militære angrep, kan de få virkninger i form av etterretning (se kapittel 7) og ved å gi en negativ effekt på befolkningens tillit til at myndighetene kan beskytte samfunnsviktig informasjonsinfrastruktur. Det er derfor all grunn til å opprettholde en høy bevissthet og beredskap rundt denne angrepsformen, også i fredstid (Israelsen & Broen, 2024, sitert av (FFI, 2024)).

Oppnåelse og opprettholdelse av tilganger er ressurskrevende for trusselaktører

Det er ifølge KraftCERT (2024) meget sannsynlig at nasjoner og oppdragsstyrte aktører kontinuerlig forsøker å utvikle evne til å gjennomføre ødeleggende dataangrep. Samtidig er det ikke gitt at det er en prioritet for fremmede stater å jobbe for å oppnå og vedlikeholde tilganger til kontrollsystemer til norsk kraftproduksjon i skrivende stund. Opprettholdelsen av eventuelle tilganger til godt beskyttede systemer vil normalt være ressurskrevende, og er derfor gjenstand for prioritering.

5.2 Fysisk sabotasje

Hva er fysisk sabotasje

Fysisk sabotasje, som å ødelegge kommunikasjonsledninger, gassrørledninger, strømledninger, kraftverk og annen infrastruktur vil ofte kunne ha en ødeleggende/ langvarig effekt, og kan også være forholdsvis lite ressurskrevende å gjennomføre.

Tegn på økning i sabotasjeaktivitet i Norge og Europa

Sjefen for Etterretningstjenesten i Norge, Nils Andreas Stensønes, sier de ser eksempler på sabotasjeaksjoner over hele Europa (Economist, 2024). Ifølge PST har sabotasjetrusselen fra Russland mot Norge økt, og de vurderer det som sannsynlig at russisk etterretning vil forsøke å utføre sabotasjeaksjoner eller forstyrrende aktiviteter mot mål i Norge i 2025 (2025). Opp mot 100 «mistenkelige hendelser», i form av angrep, etterretning og påvirknings-operasjoner i Europa i 2024 kan knyttes til Russland, hevdet den tsjekkiske utenriksministeren, Jan Lipavsky, under NATOs utenriksministermøte nylig. Historikeren Sergey Radchenko hevdet i Economist (2024) at slike spesialoperasjoner, som tidligere støttet russisk utenrikspolitikk, nå er blitt russisk utenrikspolitikk.

Ett av flere eksempler slike «mistenkelige hendelser» skjedde i 2021 og 2022, da en kabel ble fjernet og det oppstod kabelbrudd utenfor henholdsvis Vesterålen og Svalbard. Gjennom AIS-data avdekket NRK at de tre russiske fiskefartøyene «Yagry», «Vitus Bering» og «Sevryba» hadde oppholdt seg der kabelen ble fjernet utenfor Vesterålen i april 2021. De samme tre russiske fiskefartøyene var ifølge AIS-data til stede i området der kabelbruddet skjedde utenfor Svalbard i januar 2022 (NRK, 2022).

Den amerikanske kommisjonen for sikkerhet og samarbeid i Europa publiserte i desember 2024 en oversikt over det de kaller skyggekrigen, og Russlands angrep på NATO-land. Studien (CSCE, 2024) kartlegger det de har identifisert som 150 russiske hybridangrep på NATO siden starten av Russlands fullskala invasjon av Ukraina (2022), fordelt på kategoriene påvirkningsoperasjoner, migrasjon, vold og angrep på kritisk infrastruktur.

Brudd på gassrørledning mellom Finland og Estland i 2023 ble forårsaket av et kinesisk containerskip

Newnew Polar Bear i 2005. Skipet het da Baltic Fulmar (Foto av Alf van Beem, Public Domain)

I oktober 2023 dukket det kinesiske containerkipet «Newnew Polar Bear» opp i Østersjøen. Etter først å ha vært innom den russiske enklaven Kaliningrad gikk ferden nordover og inn i Finskebukten, hvor skipet senket ned det ene ankeret og rev med seg gassrørledningen mellom Finland og Estland. Estiske myndigheter hadde per januar 2024 ikke fått svar fra Kina da de ba om opplysninger i saken (NRK, 2024).

Mistenkte sabotasjeangrep inkluderer blant annet rekruttering av kriminelle til brannstiftinger og vandalisme, avsporinger på Ofotbanen, som brukes til transport av jernmalm mellom Kiruna og Narvik (NRK, 2024), droneflyving som har stoppet lufttrafikk og andre angrep på infrastruktur, samt kuttingen av en gassrørledning mellom Estland og Finland (se faktaboks).

Utviklingen går raskt og bare de siste månedene i 2024 er det oppstått mistanke om sabotasje knyttet til kuttingen av en stor kabel i forkant av en sikkerhetstest på Andøya (BT, 2024). Det kinesiske skipet, Yi Peng 3, mistenkes for å ha brutt to undersjøiske kommunikasjonskabler i Østersjøen i november 2024 (TV2, 2024).

Nato sender ti skip til Østersjøen som skal vokte kritisk infrastruktur under vann etter brudd på Estlink 2 og flere undersjøiske kommunikasjonskabler 1. juledag 2024 (EnergiWatch, 2024). Finske myndigheter mener bruddet skyldes sabotasje. Oljetankeren Eagle S, som kobles til den russiske skyggeflåten, mistenkes for å stå bak.

Det er viktig å være oppmerksom på at det kan være utfordrende å avdekke årsaken til kabelbrudd og skader på kabler. Selv om undersjøiske kabler kan være mål for sabotasjeangrep fra fremmede stater, viser erfaringer at de fleste hendelser som rammer undersjøiske kabler har vært tilfeldige og utilsiktede. Utilsiktede kabelskader oppstår ofte som følge av kommersielt fiske og skipsfart. I tillegg kan naturlige fenomen, som undersjøiske jordskjelv, forårsake kabelbrudd. Årlig oppstår det omtrent 150-200 tilfeldige, utilsiktede feil på undersjøiske kabler (Enisa, 2023) .

Relevans for kraftforsyningen

Basert på kraftforsyningens betydning for Norge og NATO, samt hendelser i den senere tid, er det grunn til å frykte sabotasjeangrep mot norsk kraftforsyning. Slike angrep kan gjennomføres med mål om å svekke økonomien generelt, olje- og gassproduksjon, våpenproduksjon -og transport og/eller svekke befolkningens tillitt til myndighetene.

6 Militære angrep

Krig er en organisert bruk av våpenmakt mellom grupper av mennesker i den hensikt å tilintetgjøre motparten eller påtvinge ham den annen parts vilje. I dette kapitlet beskriver vi mulige scenarier for militære angrep mot Norge, som inkluderer angrep mot fysisk infrastruktur, rominfrastruktur og det elektromagnetiske spektrum, og hvordan disse kan true kraftforsyningen i Norge.

6.1 Militære angrep mot fysisk infrastruktur

Sivil kraftforsyning må forventes å bli et prioritert angrepsmål i krig

Ifølge Etterretningstjenesten (2023), er hurtige angrep, med mål om å slå ut kritiske mål langt inne på fiendens territorium, sentrale i russisk militærdoktrine. Etterretningstjenesten (2023) vurderer at angrep mot kritisk sivil infrastruktur vil få prioritet tidlig i et væpnet angrep på Norge, og at varslingstiden vil være kort. Erfaringer fra Ukraina viser at Russland angriper kraftforsyningen på en målrettet og metodisk måte med langtrekkende presisjonsstyrte missiler. Formålet med slike angrep er å oppnå materiell skade og påvirke forsvarsviljen i befolkningen og blant den politiske ledelsen (FFI, 2023).

Som vi vil omtale under kapitlet om etterretning (kapittel 7) vurderer Politiets sikkerhetstjeneste at Russland allerede har kartlagt mye av den kritiske infrastrukturen i Norge (PST, 2024). 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.

Erfaringer fra krigen i Ukraina

Diesen m.fl (2024) har beskrevet hvordan russisk bruk av langtrekkende våpen i Ukraina har gått over flere faser. I starten av krigen var missilsalvene rettet mot tradisjonelle militære mål. Etter hvert fokuserte russerne på ukrainsk forsvarsindustri, kommunikasjonsinfrastruktur og symbolske bygninger i viktige byer, for deretter å konsentrere seg om drivstofflagre, raffinerier og jernbaneinfrastruktur som primære mål for langdistanseangrep. Når heller ikke dette ga noen avgjørende effekt på krigens gang, har russerne angrepet sivile mål og sivil infrastruktur, herunder kraftforsyningen (FFI, 2024).

Illustrasjon av angrep mot kraftforsyningen i Ukraina mellom 22. mars og 11. april 2024

Illustrasjon: NV.ua, Ukrenergo (Geostrategy, 2024)

Luftangrepene mot Ukrainas kraftforsyning konsentrerte seg i perioden 22. mars til 11. april 2024 på transformator-stasjoner som forsynte forsvarsindustri og jernbane.

6.2 Angrep på rominfrastruktur

Sikker og nøyaktig tidsreferanse er viktig for overvåking og drift av ledninger og stasjoner. Den vanligste tidskilden i norske kraftforsyningsanlegg og driftskontrollsystemer er direkte synkronisering ved bruk av GPS-mottakere (Statnett, 2021). Rominfrastrukturen som GPS-systemet hviler på vil kunne angripes direkte i en krigssituasjon (RUSI, 2021). Dette kan være noe av bakgrunnen for Statnett og andre aktørers arbeid med å utvikle teknologi til en ny tidskilde. Den nye tidskilden vil bli et uavhengig tillegg til dagens tidskilde (Statnett, 2021).

6.3 Elektromagnetisk pulsangrep

Ved å detonere et atomvåpen i det ytre rom (høyere enn 30 kilometer over jordens overflate) kan en trusselaktør utløse en elektromagnetisk puls (EMP) som kan slå ut både kraftforsyning, kommunikasjon og datasystemer. Slike detonasjoner fremstilles i russisk militærdoktrine som en del av informasjonsdomenet, ettersom detonasjon av atomvåpen i ytre rom ikke gir nedfall eller eksplosjoner på bakken (EMP Task Force, 2021).

I henhold til kraftberedskapsforskriftens paragraf 7-13 skal relevante virksomheter vurdere driftskontrollsystemets sårbarhet for elektromagnetisk puls (EMP) eller elektromagnetisk interferens (EMI). Dersom sårbarheter avdekkes, skal det gjennomføres sikrings- eller beredskapstiltak etter driftskontrollsystemets betydning for sikker drift og gjenoppretting av funksjon i kraftforsyningen (Energidepartementet, 2013).

7 Etterretning

Etterretning er resultatet av statlig sanksjonert innhenting, analyse og vurdering av data og informasjon for å gi fortrinn i beslutningsprosesser. Det er glidende overganger mellom etterretning og bruk av virkemidler som økonomisk maktbruk, påvirkningsoperasjoner, sabotasje og militære angrep. I dette kapitlet vil vi beskrive hvordan statsstøttede trusselaktører kan få tilgang til informasjon om norsk kraftforsyning, som de kan bruke dersom de ser seg tjent med det på et senere tidspunkt.

7.1 Etterretning i det fysiske rom

Politiets sikkerhetstjeneste vurderer at Russland allerede har kartlagt store deler av den kritiske infrastrukturen i Norge (2024), og at arbeidet med å kartlegge og identifisere sårbarheter i norsk kritisk infrastruktur vil fortsette (2025). Samtidig er Norge et etterretningsmål for Kina, og PST forventer at etterretningstrusselen fra Kina vil øke på sikt. Vi må forvente at trusselaktører også i fremtiden vil fortsette å kartlegge norsk infrastruktur og leverandørkjedene til kraftforsyningen.

Dette kan være noe av bakgrunnen for at NVE fra 1. januar 2025 strammer inn reglene for kraftsensitiv informasjon (NVE, 2024). I sin interne trusselvurdering oppfordres ansatte i Statnett til å være oppmerksomme på kjøretøy som over tid observeres i nærheten av nettanlegg og arrangementer, folk som tar bilder, etterspør informasjon og/eller vise uvanlig interesse for virksomheten, også fra folk som ikke virker å ha tilknytning til andre land (Statnett, 2024).

7.2 Etterretning i det digitale rom

Det har i de siste årene vært flere dataangrep mot Norge, som er blitt attribuert til kinesiske og russisk etterretning.

Høsten 2020 ble Stortingets IT-systemer kompromittert i en global kampanje, som ble knyttet til Russland av norske myndigheter. I løpet av tre uker i februar–mars 2021 ble Stortinget igjen rammet av to nettverksoperasjoner, som omtalt i kapittel 4.2, som norske myndigheter knyttet offentlig til Kina (Etterretningstjenesten, 2022). Fra andre land finnes det eksempler på at angivelig kinesiskstøttede aktører infiltrert og gjennomført digital etterretning og forberedelse av dataangrep mot digital infrastruktur (se faktaboks).

Økonomisk posisjonering, gjennom oppkjøp og salg av varer og tjenester, som omtalt i kapittel 4, kan muliggjøre etterretning. Et eksempel er salg av moderne elbiler, som kan samle inn og overføre store mengder data. I Kina får ikke amerikanske Tesla-biler kjøre i nærheten av statlige kontorer (Aftenposten, 2024).

7.3 Etterretning gjennom personell

En innsider er en nåværende eller tidligere ansatt, konsulent eller kontraktør/leverandør/eier som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap (NSM, 2020).

Kinesisk etterretning mot infrastruktur i USA

FBIs leder Chris Wray (Foto: Public, Wikimedia)

I begynnelsen av 2024 gikk FBI ut og sa at amerikanske myndigheter hadde avdekket at kinesiske hackergrupper, blant annet Volt Typhoon, hadde infiltrert datasystemene til amerikansk infrastruktur gjennom en periode på fem år med formål om å posisjonere Kina til å kunne bryte leveransene i en krigssituasjon (Guardian, 2024).

For å beskytte seg mot etterretning og sabotasje mot innsidere skal virksomheter som er underlagt sikkerhetsloven i Norge utføre risikoreduserende tiltak, herunder vurdere landbakgrunnen til ansatte og leverandører.

Det er viktig å merke seg at også personer uten bakgrunn i fremmedstater kan bli brukt som innsidere. Dette kan skje gjennom påvirkning, for eksempel overfor misfornøyde ansatte eller gjennom utpressing av lojale ansatte. Trusselaktører bruker sosiale medier til å kartlegge og komme i kontakt med potensielle innsidere og til å finne sårbarheter (NSM, 2023).

8 Etterord

Arbeidet i denne rapporten har vært avgrenset til å beskrive trusselbildet for norsk kraftforsyning. Som et etterord til arbeidet vil vi kort omtale noen konklusjoner, anbefalinger til hvordan sektoren kan holde seg oppdatert på trusselbildet videre og utvikle en mest mulig robust kraftforsyning.

Rapporten viser at den strategiske interessen og eksempler på virkemiddelbruk fra fremmedstater tyder på at norsk kraftforsyning må forvente å bli utsatt for forsøk på økonomisk posisjonering, påvirkningsoperasjoner og muligens sabotasje, både i form av dataangrep og angrep på fysisk infrastruktur. I en krig forventer FFI og Etterretningstjenesten at kraftforsyningen vil være et prioritert mål. Det er derfor viktig for samfunnet at kraftforsyningen er rustet til å håndtere slike trusler. Vi håper rapporten vil bidra til å gjøre ledelse og ansatte i kraftforsyningen mentalt forberedt på bruk av virkemidler som maktposisjonering og -påvirkning, sabotasje og militære angrep, slik at flest mulig situasjoner kan håndteres med fatning der de oppstår.

Kraftforsyningen kan spille en viktig rolle for samfunnssikkerheten og totalforsvaret ved å gjøre det mest mulig ressurskrevende for fremmedstater å samle etterretningsinformasjon, etablere maktposisjoner og gjennomføre sabotasje. Økt bevissthet og en oppdatert forståelse av trusselbildet blant aktører i kraftbransjen kan bidra til at nødvendige tiltak for å styrke beredskapen blir iverksatt. Å utvikle et robust system, med redundans og evne til å gjenoppretning også i en krigssituasjon, kan bidra til totalforsvaret. Som Stig Fretheim, leder for selskapet REN, som blant annet jobber med beredskaps-ordninger for kraftsektoren, fastslår (Europower, 2024):

> *«Hvis en potensiell fiende vet at Norge generelt har god beredskap, er sannsynligheten for sabotasje mindre»*

Samtidig som et mest mulig robust system er et gode, er fullstendig sikring av sivil infrastruktur ikke gjennomførbart. Et mulig mål for norsk kraftforsyning kan være å oppnå robusthet på en mest mulig effektiv måte, og på den måten endre kost-nytte-vurderingene til trusselaktørene. En robust og redundant kraftforsyning med evne til rask gjenoppretting og reparasjon vil begrense de direkte konsekvensene av eventuelle anslag. Et mål bør være at kraftforsyningen ikke blir en svakhet som en fiendtlig stat effektivt kan bruke for å påvirke Norge.

Med denne rapporten har vi forsøkt å gjøre funn og vurderinger fra norske og allierte lands etterretnings-, overvåkings- og sikkerhetstjenester forståelige og aktuelle for personer og virksomheter som jobber i og for kraftforsyningen. For å holde seg oppdatert vil vi anbefale de som jobber i sektoren å holde seg orientert om relevante deler av følgende årlige rapporter:

- Nasjonal sikkerhetsmyndighets årlige rapport «Risiko»
- Etterretningstjenesten årlige trusselvurdering «Fokus»
- Politiets sikkerhetstjenestes nasjonale trusselvurdering
- KraftCERT sin årlige trusselvurdering

Det foregår et kontinuerlig arbeid med å oppdatere vurderingene av trusselbildet og iverksette nødvendige tiltak for å sikre kraftforsyningen. Flere relevante regelverk, inkludert lov om digital sikkerhet (NIS2) og kraftberedskapsforskriften, oppdateres for å møte nye trusler.

Faktaboksen under viser viktige eksempler på tiltak som allerede er iverksatt for å beskytte kraftforsyningen.

Eksempler på defensive eksisterende tiltak i kraft-forsyningen

Det er utenfor denne rapportens mandat å foreslå ytterligere tiltak eller justering av eksisterende tiltak for å beskytte kraftforsyningen mot trusler. Vi håper rapporten vil bidra til økt årvåkenhet og bedre trusselforståelse blant relevante personer og aktører i kraftsektoren, og dermed bedre grunnlag for stadig videreutvikling av tiltak som styrker beredskapen i norsk kraftforsyning.

Årvåkenhet fra aktørene i kraftforsyningen er viktig for PST, NSM, E-tjenesten, NVE og KraftCERT. Gi beskjed og tips til relevant organisasjon ved mistanke om konkrete trusler mot kraftforsyningen.

9 Referanser

Aftenposten. (2016). Hentet fra https://www.aftenposten.no/verden/i/v2jy4/fbi-og-cia-enige-russland-blandet-seg-inn-i-usa-valget-for-at-trump-skulle-vinne

Aftenposten. (2024). Hentet fra https://www.aftenposten.no/verden/i/GMo5Eq/kina-innfoerer-tesla-forbud-flere-steder-vesten-boer-laere

Antiy. (2026). *Comprehensive Analysis Report on Ukraine Power System Attacks*. Antiy.

Bakke, S. (2022, 04 02). *Hybride trusler og sammensatt virkemiddelbruk*. Hentet fra politiforum.no: https://www.politiforum.no/hybride-trusler-kronikk-sammensatte-trusler/hybride-trusler-og-sammensatt-virkemiddelbruk/224962

BMWK. (2023). *Risikovorsorgeplan*. Berlin: BMWK.

Booz Allen. (2019). *A comprehensive review of the 2015 attacks on Ukrainan critical infrastructure*. Booz Allen Hamilton.

BT. (2024). Hentet fra https://www.bt.no/innenriks/i/xmMGbV/ffi-mistenker-at-sikkerhetstest-er-blitt-sabotert

CSCE. (2024). *Spotlight on the Shadow War: Inside Russia's attacks on NATO Territory*. CSCE.

DNV. (2024). *Metode for måling av IKT-sikkerhetstilstanden i kraftforsyningen*. Oslo: NVE.

E24. (2021). *Historisk vedtak: Nå er Bergen Engines-salget offisielt stanset*. Hentet fra E24: https://e24.no/norsk-oekonomi/i/OQ73Qb/historisk-vedtak-naa-er-bergen-engines-salget-offisielt-stanset

Economist. (2024). Vladimir Putin's spies are plotting global chaos. *Economist*.

EMP Task Force. (2021). *The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack*. EMP Task Force on National and Homeland Security.

Energidepartementet. (2013). Hentet fra https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

EnergifaktaNorge. (2024, 4 15). Hentet fra www.energifaktanorge.no: https://energifaktanorge.no/norsk-energibruk/energibruken-i-ulike-sektorer/

EnergiWatch. (2024). *Nato sender skip til Østersjøen for å vokte undersjøiske kabler*. Hentet fra EnergiWatch: https://energiwatch.no/nyheter/offshore/article17790038.ece

EnergiWatch. (2025). *Washington Post: Kabelbrudd i Østersjøen skyldes kanskje ikke sabotasje*. Hentet fra https://energiwatch.no/nyheter/nett_teknologi/article17821792.ece?utm_campaign=EnergiWatch%20Morgen&utm_content=2025-01-20&utm_medium=email&utm_source=energiwatch_no

Enisa. (2023). *SUBSEA CABLES - .* Hentet fra https://www.enisa.europa.eu/sites/default/files/publications/Undersea%20cables%20-%20What%20is%20a%20stake%20report.pdf

Enisa. (2024). *Enisa threat landscape 2024*. Enisa.

Etteretningstjenesten. (2024). *Fokus 24: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*. Oslo: Etteretningstjenesten.

Etterretningstjenesten. (2022). *Fokus*. Oslo.

Etterretningstjenesten. (2023). *Fokus 2023*.

Etterretningstjenesten. (2024, 03 14). *Hva er etterretning*. Hentet fra etterretningstjenesten.no:

https://www.etterretningstjenesten.no/om-etterretning/hva-er-etterretning

EU & Hybrid CoE. (2021). *The Landscape of Hybrid Threats: A Conceptual Model*. Europakommisjonen & Hybrid CoE.

EU & Hybrid CoE. (2023). *Hybrid threats - A Comprehensive Resilience Ecosystem*. EU & Hybrid CoE.

EU. (2022). *The role of Russian-funded environmental organisations in shaping EU climate policy*. Hentet fra European Parliament: https://www.europarl.europa.eu/doceo/document/P-9-2022-001275_EN.html

EU. (2024). *EU-China relations: De-risking or de-coupling – the future of the EU strategy towards China*. Hentet fra European Parliament: https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2024)754446

Euronews. (2025, 1 14). Hentet fra https://www.youtube.com/watch?v=cRHKAh8oflQ

Europower. (2023, 7 17). Hentet fra https://www.europower.no/nett/nytt-prosjekt-kan-endre-beredskapsarbeidet-i-bransjen-vil-lare-av-ukraina/2-1-1485403

Europower. (2023). *Nytt prosjekt kan endre beredskapsarbeidet i bransjen – vil lære av Ukraina*. Hentet fra Europower : https://www.europower.no/nett/nytt-prosjekt-kan-endre-beredskapsarbeidet-i-bransjen-vil-lare-av-ukraina/2-1-1485403

Europower. (2024). *I dag kommer beredskapsmeldingen – er det nok av disse delene hvis det oppstår konflikt?* Hentet fra Europower: https://www.europower.no/nett/i-dag-kommer-beredskapsmeldingen-er-det-nok-av-disse-delene-hvis-det-oppstar-konflikt-/2-1-1762351?mc_cid=4ac50ff8ac&mc_eid=f0ad99d74d&utm_campaign=2025-01-10&utm_content=daily&utm_medium=email&utm_source=email_campaign&utm_t

EUvsDisinfo. (2024). Hentet fra https://euvsdisinfo.eu/

FFI. (2016). *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart*. Kjeller: FFI.

FFI. (2018). *Lavintensivt hybridangrep på Norge i en fremtidig konflikt*. Kjeller: FFI.

FFI. (2022). *Hva kan Norge lære av andre lands tilnærming til sammensatte trusler?* . Kjeller: FFI.

FFI. (2022). *Kinesisk økonomisk statshåndverk og implikasjoner for norsk sikkerhet*. Kjeller: FFI.

FFI. (2022). *Russisk økonomisk statshåndverk – implikasjoner for norsk sikkerhet*. Kjeller: FFI.

FFI. (2022, 03 22). *Russland i cyberkrig: Hvor gode er de og hvordan går de fram?* Hentet fra FFI: https://www.ffi.no/aktuelt/nyheter/russland-i-cyberkrig-hvor-gode-er-de-og-hvordan-gar-de-frem

FFI. (2022). *Scenarioklasser for forsvarsplanlegging – revisjon av FFIs scenariogrunnlag*. Kjeller: FFI.

FFI. (2022a, 6 15). *www.ffi.no*. Hentet fra https://www.ffi.no/aktuelt/podkaster/kan-mennesker-hackes#:~:text=Det%20kognitive%20domenet,-I%20milit%C3%A6r%20doktrine&text=%E2%80%93%20Dette%20domenet%20best%C3%A5r%20av%20menneskers,gruppes%20oppfatninger%2C%20holdninger%20og%20handlinger.

FFI. (2023). *Cyberoperasjoner i et statsperspektiv – utfordringer og analytiske verktøy for militær kontekst*. Kjeller: FFI.

FFI. (2023). *Hva vet vi om innsiderisiko?* Kjeller: FFI.

FFI. (2023). *Improved conceptualising of hybrid interference below the threshold of armed conflict*. Kjeller: FFI.

FFI. (2023). *Teknologiske og samfunnsmessige utviklingstrekk av betydning for nasjonale sikkerhetsinteresser i et 2030-perspektiv*. Kjeller: FFI.

FFI. (2023). *Tilsiktede handlinger som kan true norsk kraftforsyning*. Kjeller: FFI.

FFI. (2023a). Hentet fra https://www.ffi.no/aktuelt/nyheter/sammensatte-trusler--hva-kan-vi-laere-av-andre-land

FFI. (2023a). Hentet fra https://www.ffi.no/aktuelt/podkaster/kort-forklart-hva-er-sammensatte-trusler

FFI. (2024). *Effekter av økonomisk statshåndverk – internasjonal faglitteratur og implikasjoner for norsk sikkerhet*. Kjeller: FFI.

FFI. (2024). *Erfaringer fra krigen i Ukraina*. Kjeller: FFI.

Finansavisen. (2024). *Grønn omstilling gir geopolitisk hodepine*. Hentet fra Finansavisen: https://www.finansavisen.no/esg/2024/09/06/8158790/kina-har-stalkontroll-over-kritiske-mineraler-og-jordarter

FOI. (2020). *Beyond Bursting Bubbles – Understanding the Full Spectrum of the Russian A2/AD Threat and Identifying Strategies for Counteraction* . Totalförsvarets forskningsinstitut.

GEG. (2021). *China at the gates of the European power grid*. Hentet fra https://geopolitique.eu/: https://geopolitique.eu/wp-content/uploads/2021/07/EN_Policy_paper_electricity.pdf

Geostrategy. (2024). *Russian tactics targeting Ukrainian critical energy infrastructure*. Geostrategy.

Guardian. (2024). Hentet fra https://www.theguardian.com/technology/2024/feb/08/chinese-hack-us-transportation-infrastructure

Harris, C. (2006). *Electricity Markets*. Bath.

Hybrid CoE. (2024). *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*. Hybrid Coe.

IEA. (2024). *Energy Technology Perspectives*. Paris: IEA.

Justis- og beredskapsdepartementet. (2023-2024). *Prop. 42 L. Endringer i straffeloven mv. (påvirkning fra fremmed etterretning)*. Oslo: Regjeringen.

KraftCERT. (2023). *Trusselvurdering 2023*. Oslo: KraftCERT.

KraftCERT. (2024). *Trusselvurdering 2024*. Oslo: KraftCERT.

LRT. (2024). *Lithuania passes law to block Chinese access to solar and wind farm systems*. Hentet fra www.lrt.lt: https://www.lrt.lt/en/news-in-english/19/2411602/lithuania-passes-law-to-block-chinese-access-to-solar-and-wind-farm-systems

m.fl., D. (2024). *Why renewables should be at the center of rebuilding the Ukrainian electricity system*. Joule.

MCDC. (2017). *MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare*. MCDC.

MCDC. (2019). *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare*. MCDC.

Mills, C. (2022). *Geopolitical implications of Nord Stream 2*. Hentet fra https://researchbriefings.files.parliament.uk/documents/CBP-9462/CBP-9462.pdf

NAOB. (2024). *Påvirkningsoperasjon*. Hentet fra Norsk Akademisk Ordbok: https://naob.no/ordbok/p%C3%A5virkningsoperasjon

NATO. (2021, 01 13). *Energy security in the era of hybrid warfare*. Hentet fra nato.int: https://www.nato.int/docu/review/articles/2021/01/13/energy-security-in-the-era-of-hybrid-warfare/index.html

NATO. (2024, 04 26). *Russia's hybrid war against the west*. Hentet fra nato.int:

https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html

Netsecurity. (2024). *Gjensidige avhengigheter av IT og OT i kraftforsyningen.* Oslo: NVE.

NKOM. (2024). Hentet fra https://nkom.no/aktuelt/betydelig-okning-gps-jamming-finnmark

NorSun. (2024, 12 17). *www.norsun.no*. Hentet fra https://www.norsun.no/artikler/norsun-as-avvikler-produksjonen-i-norge-pa-grunn-av-markedssvikt-i-europa

NRK. (2021). *www.nrk.no*. Hentet fra https://www.nrk.no/norge/pst_-har-etterretning-om-at-kinesisk-gruppe-stod-bak-dataangrep-mot-statsforvaltere-1.15540601

NRK. (2022). Hentet fra https://www.nrk.no/norge/russisk-hackergruppe-skal-ha-startet-angrep-mot-norge-1.16020947

NRK. (2022). Hentet fra https://www.nrk.no/nordland/xl/russiske-tralere-krysset-kabler-i-vesteralen-og-svalbard-for-brudd-1.16007084#:~:text=Gjennom%20AIS%2Ddata%20har%20NRK,Svalbard%20i%20januar%20i%20%C3%A5r.

NRK. (2024). Hentet fra https://www.nrk.no/nyheter/pst_-to-grupper-hacka-stortinget-1.16838862

NRK. (2024, 2 26). Hentet fra https://www.nrk.no/nordland/mistenker-at-sabotasje-forte-til-avsporing-pa-malmbanen-ved-svenskegrensen-1.16778977

NRK. (2024, 1 15). Hentet fra https://www.nrk.no/urix/hva-skjedde-da-gassrorledningen-i-ostersjoen-ble-revet-opp_-1.16706750

NRK. (2024, 1 15). Hentet fra https://www.nrk.no/urix/hva-skjedde-da-gassrorledningen-i-ostersjoen-ble-revet-opp_-1.16706750

NRK. (2024, 11 29). Hentet fra https://www.nrk.no/innlandet/ekspert-advarer-mot-kinesiske-elbiler-_-forsvaret-har-ingen-begrensninger-1.17138704

NSA, CIA og FBI. (2017). *Background to Assessing Russian Activities and Intentions.* Hentet fra https://www.dni.gov/files/documents/ICA_2017_01.pdf

NSM. (2020). *Temarapport Innsiderisiko.* Sandvika: Nasjonal Sikkerhetsmyndighet.

NSM. (2023). *Sikkerhetsfaglig råd. Et motstandsdyktig Norge.* Oslo: NSM.

NSM. (2024). *Risiko 2024: Nasjonal sikkerhet.* Sandvika: Nasjonal sikkerhetsmyndighet.

NUPI. (2016). Hentet fra https://www.nupi.no/skole/hvor-hender-det/2016/hybrid-krigfoering-hva-er-det

NVE. (2017). *Informasjonssikkerhetstilstanden i energiforsyningen.* Oslo: NVE.

NVE. (2024). Hentet fra https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/nve-strammer-inn-reglene-for-kraftsensitiv-informasjon/

NVE. (2024). *Energibruksrapporten 2024.* Oslo.

NVE. (2024). *Veileder i personnelsikkerhet i kraftforsyningen.* Oslo.

Politico. (2021). Hentet fra https://www.politico.eu/article/vladimir-putin-german-chancellors-nord-stream-russia-energy-angela-merkel/

Politiet. (2024). *Politiets trusselvurdering 2024.* Oslo: Politiet.

PST. (2022). *Nasjonal trusselvurdering 2022.*

PST. (2024). *Nasjonal Trusselvurdering 2024.* Oslo: PST.

PST. (2025). *Nasjonal trusselvurdering 2025.* Hentet fra https://www.pst.no/globalassets/2025/nasjonal-

trusselvurdering-2025/nasjonal-trusselvurdering-2025_no_web.pdf

PWC. (2024). *NVE Ekstern rapport 17/2024: Gjensidige avhengigheter IT og OT i kraftforsyningen.* Oslo: NVE.

RUSI. (2021). Hentet fra https://rusi.org/explore-our-research/publications/commentary/space-and-future-war-according-russia

Rusi. (2024). *Japan's Responses to China's Supply Chain Dominance*. Hentet fra Rusi: https://rusi.org/explore-our-research/publications/commentary/japans-responses-chinas-supply-chain-dominance

SINTEF. (2024). *Slik sikrer vi Norge mot nye energikriser*. Hentet fra https://www.sintef.no/siste-nytt/2024/slik-sikrer-vi-norge-mot-nye-energikriser/

Skeie, T. (2011). *Alv Erlingsson - fortellingen om en adelsmanns undergang.* Oslo: Spartacus.

SNL. (2022, 02 17). *Cyberkrigføring*. Hentet fra Store Norske Leksikon: https://snl.no/cyberkrigf%C3%B8ring

SNL. (2022, 07 28). *Sabotasje*. Hentet fra Store Norske Leksikon: https://snl.no/sabotasje

SNL. (2023). *trussel (risiko)*. Hentet fra Store Norske leksikon.

Sokkeldirektoratet. (2022). Hentet fra https://www.sodir.no/aktuelt/publikasjoner/rapporter/ressursrapporter/ressursrapport-2022/5-energiomstillingen-gir-nye-muligheter/faktaboks-energiproduksjon-fra-ulike-kilder/#:~:text=Norge%20og%20Island%20er%20de,28%5D%20(Figur%205.1).

Sokkeldirektoratet. (2023). Hentet fra https://www.sodir.no/aktuelt/nyheter/generelle-nyheter/2023/norsk-gass-viktig-for-europas-energisikkerhet/

Statnett. (2021). Hentet fra https://www.statnett.no/om-statnett/Forskning-utvikling-og-innovasjon/vare-sentrale-prosjekter/cosectime-3-tidsnoyaktighet-og-sikkerhet2/

Statnett. (2024). Begrensninger i nasjonalitet og opphavsland. Statnett.

Statnett. (2024). *Trusselvurdering 2024 (internt dokument).* Oslo: Statnett.

Totalberedskapskommusjonen. (2023). *NOU: Nå er det alvor - Rustet for en usikker fremtid.* Oslo: Regjeringen.

TU. (2021). *https://www.tu.no/artikler/topphemmelig-norsk-spionskip-skal-vedlikeholdes-av-russere-etter-oppkjop/507251*. Hentet fra Teknisk Ukeblad: https://www.tu.no/artikler/topphemmelig-norsk-spionskip-skal-vedlikeholdes-av-russere-etter-oppkjop/507251

TU. (2021). *Russlands største produsent av krigsskip vil samarbeide med Bergen Engines-kjøper*. Hentet fra Teknsisk Ukeblad: https://www.tu.no/artikler/e24-russlands-storste-produsent-av-krigsskip-vil-samarbeide-med-bergen-engines-kjoper/507353

TV2. (2024). Hentet fra https://www.tv2.no/nyheter/utenriks/avis-russisk-etterretning-ba-kinesisk-lasteskip-om-a-kutte-kabler/17289146/

UiS, & NTNU. (2021). *Kraftbransjens leverandørkjeder – digital sikkerhet og sårbarhet i globaliseringens tidsalder.* Oslo: NVE.

VG. (2024). Hentet fra https://www.vg.no/nyheter/i/AvXJgA/eksperter-til-vg-nordmenn-maa-vaere-forberedt-paa-russisk-sabotasje

Warzaw Institute. (2024). *Russian Disinformation and its Influence on the Energy Sector in V4 Countries*. Hentet fra Warzawinstitute.org: https://warsawinstitute.org/russian-disinformation-and-its-influence-on-the-energy-sector-in-v4-countries/

Waage, K., Lindgren, P. Y., Kvalvik, S. N., Haukland, M., Isaksen, T. B., & Moe, O. D. (2021). *Økonomiske virkemidler for å oppnå strategiske mål – en oversikt.* Kjeller: FFI.

Disclaimer

Hvis ikke beskrevet ellers, er informasjon og anbefalinger i denne rapporten basert på offentlig tilgjengelig informasjon. Visse uttalelser i rapporten kan være uttalelser om fremtidige forventninger og andre fremtidsrettede uttalelser som er basert på THEMA Consulting Group AS (THEMA) sitt nåværende syn, modellering og antagelser og involverer kjente og ukjente risikoer og usikkerheter som kan forårsake at faktiske resultater, ytelser eller hendelser kan avvike vesentlig fra de som er uttrykt eller antydet i slike uttalelser. Enhver handling som gjennomføres på bakgrunn av vår rapport foretas på eget ansvar. Kunden har rett til å benytte informasjonen i denne rapporten i sin virksomhet, i samsvar med forretningsvilkårene i vårt engasjementsbrev. Rapporten og/eller informasjon fra rapporten skal ikke benyttes for andre formål eller distribueres til andre uten skriftlig samtykke fra THEMA. THEMA påtar seg ikke ansvar for eventuelle tap for Kunden eller en tredjepart som følge av rapporten eller noe utkast til rapport, distribueres, reproduseres eller brukes i strid med bestemmelsene i vårt engasjementsbrev med Kunden. THEMA beholder opphavsrett og alle andre immaterielle rettigheter til ideer, konsepter, modeller, informasjon og ”know-how” som er utviklet i forbindelse med vårt arbeid.

Om THEMA

THEMA Consulting Group tilbyr rådgivning og analyser for omstillingen av energisystemet basert på dybdekunnskap om energimarkedene, bred samfunnsforståelse, lang rådgivningserfaring og solid faglig kompetanse innen samfunns- og bedriftsøkonomi og teknologi.

THEMA Consulting Group
Øvre Vollgate 6
0158 Oslo, Norway

www.thema.no

Berlin-kontor
Albrechtstraße 22
10117 Berlin, Germany

NVE

Norges vassdrags- og energidirektorat

Middelthuns gate 29
Postboks 5091 Majorstuen
0301 Oslo
Telefon: (+47) 22 95 95 95