Kunnskapsgrunnlag for vurdering av sensitive teknologier (KVAST): Sluttrapport

Rapport fra Norges forskningsråd, Forsvarets forskningsinstitutt og Nasjonal sikkerhetsmyndighet

Innhold

Sammendrag

Dette prosjektet skal bidra til å etablere et mer helhetlig kunnskapsgrunnlag om hvilke teknologiområder og konkrete teknologier som til enhver tid vurderes som særlig sensitive for nasjonal sikkerhet, og hvordan forskningsfronten utvikler seg over tid.

Prosjektet gir for første gang en felles oversikt over sensitive teknologier tilpasset norske forhold. Denne oversikten inneholder 11 overordnede teknologiområder og total 48 underkategorier (teknologier). Prosjektet gir et statusbilde av Norges aktivitet og posisjon innenfor forskning på de sensitive teknologiene og hvordan vi samarbeider internasjonalt. Det er også utviklet en ny metodikk for risikovurderinger av sensitive teknologier, og det er gjennomført risikovurdering på utvalgte teknologier. Prosjektet bygger blant annet på sammenstilling og analyse av internasjonale teknologioversikter, spørreundersøkelser blant norske FoU-virksomheter, analyser av bibliometriske data og prosjektdata, fagevalueringer og åpne trusselvurderinger.

Blant hovedfunnene er at norske miljøer er aktive innenfor alle de sensitive teknologiområdene, men aktivitetsnivå og gjennomslag for de norske miljøene varierer sterkt mellom teknologiene. Kunstig intelligens og energiteknologier er Norges sterkeste områder blant de sensitive teknologiene, med høyt siterte artikler og høy total vitenskapelig produksjon. Norske miljøer henter inn betydelige midler fra EUs rammeprogram innenfor disse områdene. Enkelte områder har lavt volum, men er likevel høyt sitert og har høy prosjektdeltakelse. Det er imidlertid noen underkategorier med lite eller ingen aktivitet.

På de fleste teknologiområdene samarbeider Norge mest med allierte land – i hovedsak store europeiske forskningsnasjoner og USA. Men analysene viser også at samarbeidet med Kina, som både regnes som et samarbeidsland og en trusselaktør av norske myndigheter, er viktig for Norge på de fleste teknologiområdene og er av betydelig størrelse innenfor enkelte teknologiområder. Dette gjelder særlig kunstig intelligens og energiteknologier, som også er de to områdene hvor norske miljøer er sterkest.

Funnene indikerer at Norge har FoU-miljøer innenfor sensitive teknologier som står i en krevende spenning mellom åpenhet og viktigheten av internasjonalt samarbeid på den ene siden og hensynet til forskningssikkerhet og beskyttelse på den andre siden. Nasjonal sikkerhetsstrategi, som ble lagt frem av regjeringen i 2025, slår fast at internasjonalt samarbeid innenfor forskning og utdanning er en forutsetning for Norges konkurransekraft og vår evne til å løse nye utfordringer. I stortingsmeldingen om forskningssystemet (Meld. St. 14 (2024-2025)) er et større kapittel viet forskningssikkerhet og behovet for å styrke dette arbeidet for å ivareta internasjonalt samarbeid og åpen forskning i en mer usikker internasjonal situasjon. Resultatene fra KVAST-prosjektet gir et kunnskapsgrunnlag for videre arbeid i skjæringsfeltet mellom FoU og nasjonal sikkerhet, både for myndighetene, for ulike etater og i arbeidet med sikkerhet og ansvarlig forskningssamarbeid på institusjonsnivå.

Både teknologiene, forskningsfronten og den internasjonale sikkerhetssituasjonen er imidlertid i stadig endring. En teknologioversikt og et statusbilde vil derfor raskt kunne bli utdatert. I siste del av denne rapporten pekes det på nytten av kunnskapsgrunnlaget og hvordan behovet for systematisk oppdatering og videreutvikling av kunnskapen kan ivaretas fremover.

1. Innledning og bakgrunn

1.1. Om KVAST-prosjektet

Kunnskap, kompetanse og teknologi er avgjørende for internasjonal konkurranse og nasjonal sikkerhet, samtidig som geopolitiske endringer og spenninger gjør at kunnskapssektoren – som er basert på en grunnleggende åpenhet – blir mer sårbar. Denne utviklingen skaper særlige utfordringer for FoU-aktivitet innenfor sensitive teknologiområder knyttet til sikkerhet og regelverk, med gråsoner som kan være vanskelige å håndtere. Det kreves derfor bedre systematisk kunnskap for å identifisere behovet for beskyttende tiltak, samtidig som åpen forskning skal opprettholdes. Dette er bakgrunnen for at regjeringen ønsker å etablere et helhetlig kunnskapsgrunnlag om sensitive teknologier på tvers av sektorer og regelverk.

Oppdraget med å utvikle et kunnskapsgrunnlag for vurdering av sensitive teknologier (KVAST) ble gitt av Kunnskapsdepartementet, i samarbeid med Forsvarsdepartementet og Justis- og beredskapsdepartementet, til Forskningsrådet, Forsvarets forskningsinstitutt (FFI) og Nasjonal sikkerhetsmyndighet (NSM) 31. oktober 2024. Oppdraget hadde sluttdato 31. desember 2025.

Fullstendig oppdragsbeskrivelse finnes som Vedlegg 1 til denne rapporten.

Formålet med oppdraget er å bidra til å etablere et mer helhetlig kunnskapsgrunnlag om hvilke teknologiområder og konkrete teknologier som til enhver tid vurderes som særlig sensitive for nasjonal sikkerhet, og hvordan forskningsfronten utvikler seg over tid.

En felles forståelse av dette på tvers av ulike sektorer er en forutsetning for å kunne iverksette målrettede og proporsjonale risikoreduserende tiltak – dvs. tiltak som tilrettelegger for

- fortsatt åpenhet på områder hvor faglig samarbeid er ønskelig og viktig sett i lys av kunnskapspolitiske mål – inkludert Norges langsiktige kunnskaps- og kompetansebehov – og hvor eventuell risiko vurderes som håndterbar og dermed akseptabel.
- å redusere risiko til et akseptabelt nivå på områder som er i gråsonen.
- å unngå samarbeid på områder hvor risikoen vurderes som ikke-akseptabel.

Kunnskapsgrunnlaget skal bidra til å:

1. redusere risiko forbundet med sensitive teknologier (beskytte);
2. sikre tilstrekkelig norsk kunnskap og kompetanse på teknologiområder av betydning for nasjonal sikkerhet (fremme);
3. tilrettelegge for ansvarlig internasjonalt samarbeid, som sikrer trygge rammer for samarbeid, også med land vi ikke har et sikkerhetspolitisk samarbeid med (samarbeide).

1.2. KVAST-prosjektet i kontekst: FoU og nasjonal sikkerhet

KVAST-prosjektet skal etablere et felles kunnskapsgrunnlag om sensitive teknologier som skal bidra på tvers av sektorer og regelverk. Prosjektet er en av flere nasjonale og internasjonale prosesser som berører koblingen mellom FoU-systemet, nasjonal sikkerhet og økonomisk sikkerhet. I det følgende beskrives flere relevante prosesser og tiltak som danner en viktig kontekst for prosjektet, og som omfatter både politisk rammeverk, tiltak for bevisstgjøring og kunnskapsutvikling, regelverk og utviklingsprosjekter.

1.2.1. Nasjonal sikkerhet og økonomisk sikkerhet

Den skjerpede sikkerhetspolitiske situasjonen i Europa og globalt har aktualisert behovet for en samlet tilnærming til nasjonale sikkerhetsutfordringer, inkludert den rollen forskning og tilgang til kritisk kunnskap og teknologi spiller for nasjonal og økonomisk sikkerhet. I regjeringens Nasjonale sikkerhetsstrategi (2025) trekkes det frem tre strategiske hovedprioriteringer: 1) raskt styrke forsvarsevnen, 2) gjøre samfunnet mer motstandsdyktig og 3) styrke vår økonomiske sikkerhet. I strategien understrekes det at "Vår sikkerhet avhenger av at vi bevarer vår konkurransekraft og omstillingsevne", og at skillet mellom sikkerhet, økonomi og teknologi i økende grad viskes ut i møte med en kompleks internasjonal trusselsituasjon.[1]

Sensitive fagområder og teknologiområder vurderes i denne sammenhengen som både avgjørende for nasjonens kapasitet til å møte fremtidens sikkerhetsutfordringer og som mulige mål for spionasje, uønsket kunnskapsoverføring og påvirkning fra fremmede aktører. Særlig legges det vekt på teknologiområder med mulige både sivile og militære anvendelser (flerbrukspotensial), som IKT, kunstig intelligens, kvanteteknologi og bioteknologi.[2] EUs og NATOs arbeid med identifisering og beskyttelse av kritiske og sensitive teknologier danner et sentralt rammeverk for norske vurderinger av slike risikoer.

Økonomisk sikkerhet berører forskning både direkte og indirekte. Et åpent og innovativt forskningsmiljø er en nøkkel for en kunnskapsproduserende økonomi, og tilgang til infrastruktur, strategisk kunnskap og kompetanse er avgjørende for Norges evne til å forsvare interesser og opprettholde konkurranseevne. Samtidig innebærer økt stormaktrivalisering at risiko for uønsket kunnskapsoverføring og påvirkning på FoU øker, og dette skaper utfordringer for internasjonalt forskningssamarbeid, kunnskapsdeling og akademisk frihet.

Stortingsmeldingen om forskningssystemet (Meld. St. 14 (2024-2025)) fremhever at forskningssektoren må være "så åpen som mulig, og så sikker som nødvendig". Dette innebærer en balansegang mellom åpenhet, internasjonalt samarbeid, kritisk diskusjon og aktsomhet i møte med nye sikkerhetsutfordringer, hvor bevissthet om samarbeids-partnere og risikoreduserende tiltak må bygge på systematisk kunnskapsgrunnlag. I Nasjonal sikkerhetsstrategi understrekes det at Norge må identifisere og redusere risikoer i økonomisk samkvem – herunder forskningssamarbeid – spesielt i møte med land som Kina, hvor det presiseres at "på visse sensitive områder skal samarbeid unngås".

I Regjeringens plan for Norge 2025-2029, hvor en av prioriteringene er styrking av Norges økonomiske sikkerhet, fremheves det at «Norge må investere i bruk og utvikling av kvanteteknologi, forsvarsteknologi og undervannsteknologi, samtidig som vi styrker eksportkontrollen for å hindre at sikkerhetssensitiv teknologi og kunnskap deles med aktører som ikke deler våre sikkerhetsinteresser.»[3]

[1] Nasjonal sikkerhetsstrategi.
[2] St.meld. 14 (2024-2025): Sikker kunnskap i en usikker verden.
[3] Regjeringens plan for Norge 2025-2029, s. 13.

Samlet peker dokumentene på at forskning på sensitive og strategisk viktige teknologiområder må forstås som en integrert del av samfunnets totale beredskap, motstandskraft, og kapasitet til å møte både tradisjonelle og hybride trusler. Økonomisk sikkerhet er ikke en isolert disiplin, men et gjennomgående vilkår for at forskningsmiljøene, næringslivet og forvaltningen skal kunne forsvare, bevare og videreutvikle nasjonale interesser i et stadig mer usikkert verdensbilde.

1.2.2. Forskningssikkerhet

KVAST-prosjektet omfatter sensitive teknologiområder og teknologier hvor FoU-aktiviteten i noen tilfeller er underlagt klare begrensninger i regelverk, slik som eksportkontroll eller sikkerhetsloven. Men utenfor disse klart regulerte områdene vil det eksistere en rekke gråsoner, hvor det kan være uklart hvilken status og verdi forskning og teknologi har for nasjonale sikkerhetsinteresser og hvilken risiko som knytter seg til forskning og internasjonalt samarbeid. KVAST-prosjektet føyer seg inn i et pågående arbeid med å bygge nasjonal kunnskap og kompetanse innenfor forskningssikkerhet for å nettopp håndtere slike gråsoner og sette det norske kunnskapssystemet i stand til å operere «så åpent som mulig» og «så sikkert som nødvendig».

Forskningssikkerhet er i EU-sammenheng forstått som arbeidet med å identifisere og håndtere risiko relatert til 1) uønsket kunnskapsoverføring fra forskning og utvikling, 2) uønsket påvirkning og innblanding i forskning og utvikling og 3) brudd på forskningsetikk og -integritet hvor kunnskap og teknologi brukes til å underminere sentrale samfunnsverdier. Denne definisjonen av forskningssikkerhet legges også til grunn i stortingsmeldingen om forskningssystemet (Meld. St. 14) og i Nasjonal sikkerhetsstrategi.

Med EUs rådsanbefalinger[4] om styrket forskningssikkerhet (2024) og det påfølgende utviklingsarbeidet i EU-kontekst har det begynt å utkrystallisere seg en felles tilnærming til forskningssikkerhet. Det legges vekt på de akademiske institusjonenes autonomi og behovet for selvregulering og balansering av åpenhet og sikkerhet. En forutsetning for arbeidet på tvers av EU er at forskningen bygger på akademisk frihet og internasjonalt samarbeid. Forskningssikkerhet skal muliggjøre fortsatt samarbeid, heller enn å begrense det, samtidig som forskningssystemene må utvikle gode tilnærminger for å vurdere og sette inn tiltak der hvor dette er nødvendig av hensyn til nasjonal sikkerhet.

Rådsanbefalingene og stortingsmeldingen om forskningssystemet er også tydelige når det gjelder ansvarsdeling: De forskningsutførende virksomhetene har det grunnleggende ansvaret for å ivareta ansvarlighet og sikkerhet i forskningen. Samtidig pekes det på sentrale aktører som forventes å spille en rolle. De forskningsfinansierende organisasjoner har en særlig rolle i å fremme forskningssikkerhet gjennom sine finansieringsmekanismer, samt bidra til kunnskapsutvikling og bevisstgjøring. Andre aktører som trekkes frem i Norsk sammenheng er EOS-tjenestene, som bidrar med trussel og risikovurderinger og har dialog med de utførende virksomhetene om trusselbildet mot deres virksomhet, og Direktoratet for eksportkontroll og sanksjoner (DEKSA), som behandler søknader om eksportlisens og tilbyr veiledning for kunnskapssektoren og næringsliv knyttet til eksportkontroll og sanksjoner.

Internasjonalt pågår det mye samarbeid om forskningssikkerhet gjennom organisasjoner som Science Europe (i hovedsak forskningsfinansiører i EU/EØS), OECD og EU-kommisjonen. Kommisjonen vil

[4] EU Council Recommendations on enhancing research security (2024)

fremover utvikle flere konkrete tiltak som oppfølging av rådsanbefalingene, blant annet et Centre of Expertise og verktøy og ressurser for bakgrunnssjekk og risikovurderinger. Det forventes at EU-kommisjonen vil utarbeide nye krav og retningslinjer for forskningssikkerhet for FoU-prosjekter med det neste rammeprogrammet for forskning og innovasjon (2028-2034), både i form av tiltak for risikovurdering i enkeltprosjekter, og tiltak på program- og utlysningsnivå, hvor enkelte temaer og utlysninger har begrensninger med hensyn til hvilke land som kan delta.

1.2.3. Trussel- og risikovurderinger om teknologier og FoU

De siste årene har norske sikkerhetsmyndigheter rapportert om et økende og komplekst trusselbilde mot teknologi og FoU, særlig fra aktører i Russland, Kina og Iran.[5] Trusselaktørene bruker metoder som inkluderer etterretning, rekruttering, digitale angrep og samarbeid for å få tilgang til norsk kompetanse og teknologi. FoU-sektoren har en stor grad av åpenhet og internasjonalt samarbeid, noe som gir risiko for uønsket kunnskapsoverføring. Spesielt utsatt er teknologier med militær, sikkerhetsmessig eller økonomisk betydning, som halvlederteknologi, kunstig intelligens (KI), kvanteteknologi og avanserte sensorer.

Sikkerhetstjenestene peker på at trusselaktørenes metoder har blitt mer avanserte, blant annet gjennom bruk av KI og målrettede digitale angrep. Sivil og militær teknologi flyter stadig mer sammen, og det gir større utfordringer knyttet til forskningssamarbeid og kontroll over leverandørkjeder. Vurderingene peker også på at FoU-sektoren er sårbar med tanke på digitalisering, bruk av skytjenester og åpne delingsplattformer.

1.2.4. Sikkerhetsloven og grunnleggende nasjonale funksjoner

Virksomheter som ligger under Kunnskapsdepartementet, som statlige universiteter og høgskoler, er underlagt Lov om nasjonal sikkerhet (Sikkerhetsloven). Også enkelte forskningsinstitutter er underlagt, eller er i prosess med å bli underlagt sikkerhetsloven. Dette innebærer krav om at virksomhetenes forebyggende sikkerhetsarbeid er del av virksomhetenes styringssystem, regelmessig kontroll av sikkerhetstilstanden og forsvarlig sikkerhetsnivå for skjermingsverdige verdier ved virksomhetene.

Sikkerhetsloven omhandler også beskyttelse av grunnleggende nasjonale funksjoner (GNF), definert som «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser». Eksempler på GNF er kommando og kontroll over militære styrker, kritiske samfunnsfunksjoner (kraftforsyning, telekommunikasjon, helseberedskap), gjennomføring av frie valg, osv.

I delrapport 4 (Risikovurdering) er det i noen tilfeller pekt på risiko der hvor enkelte teknologier er knyttet til eksisterende GNF i Norge, for eksempel teknologier som muliggjør og understøtter grunnleggende nasjonale funksjoner som digital infrastruktur, eller generell risiko knyttet til at teknologiske løsninger kan brukes til å skade nasjonale sikkerhetsinteresser eller grunnleggende nasjonale funksjoner.

[5] For eksempel fra 2025: Fokus 2025 - Etterretningstjenesten, Nasjonal trusselvurdering 2025 og Risiko 2025 - Nasjonal sikkerhetsmyndighet. Vi har sett på trusselvurderingene de siste seks år (2020-2025)

Regjeringen har besluttet å etablere en grunnleggende nasjonal funksjon innenfor forskning og utvikling (FoU). Dette innebærer at enkelte deler av forskning og utvikling anses å ha betydning for nasjonale sikkerhetsinteresser. Arbeidet med å etablere en GNF for forskning og utvikling innebærer å identifisere og avgrense de delene av FoU som anses å ha en slik betydning. Dette gjøres gjennom verdikartlegginger i tråd med krav som stilles i sikkerhetsloven. Arbeidet ledes av kunnskapsdepartementet. Regjeringen har omtalt arbeidet med en GNF i stortingsmeldingen om forskningssystemet (Meld. St. 14 (2024-2025)), og presiserer her at de skjermingsverdige verdiene i forskningssystemet antas å utgjøre en svært begrenset del av den samlede forskningsaktiviteten i Norge.

KVAST-prosjektet skal gi et avgrenset kunnskapsgrunnlag om sensitive teknologier i Norge. Arbeidet vil gi et felles kunnskapsgrunnlag for sektoren og på tvers av departement, men det ligger ikke i oppdraget å identifisere eller avgrense verdier innenfor en ny GNF for forskning og utvikling.

1.2.5. Eksportkontroll

Eksportkontroll har gjennom de siste årene fått mye oppmerksomhet i kunnskapssektoren. Dette har kommet som følge av nye krav i eksportkontrollforskriften når det gjelder lisensplikt for teknologioverføring til utenlandske aktører, noe som har betydning for deler av forskningssystemet. Det har også kommet viktige presiseringer om unntak for lisensplikt for grunnleggende forskning (lav TRL). Disse endringene har praktiske konsekvenser for kunnskapssektoren og har tydeliggjort at institusjonene har et ansvar for å gjøre vurderinger om forskningen faller inn under eksportkontrollen.

I 2025 ble Direktorat for eksportkontroll og sanksjoner (DEKSA) opprettet under Utenriksdepartementet. DEKSA har ansvar for å forvalte regelverket, behandle søknader om eksportlisenser samt tilby veiledning i spørsmål om eksportkontroll, inkludert til kunnskapssektoren.

Den norske eksportkontrollen er basert på varelister som er fremforhandlet internasjonalt med nøye angitte teknologier som har potensiale for militær anvendelse. Disse varelistene inngår som vedlegg til eksportkontrollforskriften.[6] Eksportkontrollen retter seg i hovedsak mot spesifikk teknologi og «know-how» knyttet til design, produksjon eller bruk av varer (forsvarsmateriell og flerbruksvarer/dual-use varer) fra disse listene.

Regelverket for eksportkontroll er en viktig, men begrenset del av arbeidet med nasjonal sikkerhet, og lisensplikten treffer en relativt liten del av den samlede FoU-aktiviteten i Norge. Teknologioversikten og kunnskapsgrunnlaget som etableres med KVAST-prosjektet peker derimot på teknologier som i praksis er brede forskningsfelt med stor variasjon og kompleksitet når det gjelder teknologimodenhet og risiko. En stor del av FoU-aktiviteten innenfor sensitive teknologier vil ikke være direkte berørt av regelverket for eksportkontroll, men vil kreve løpende aktsomhetsvurderinger og tiltak som ivaretar hensynet til både åpenhet og beskyttelse.

1.2.6. Investeringskontroll

Utredningen «NOU 2023: 28 Investeringskontroll – En åpen økonomi i en usikker tid», foreslo at det etableres en ny lov om investeringskontroll, der siktemålet er å kontrollere utenlandske investeringer

[6] Mens vareliste I gjelder rent militære produkter, er det vareliste II (flerbruksvarer) og vareliste III (fremvoksende teknologier) som i noen grad har relevans for FoU-sektoren. For nærmere beskrivelse av varelistene, se Varelister – DEKSA

i selskaper som ikke er underlagt sikkerhetsloven.[7] Utredningen følger den europeiske trenden ved å revidere nasjonale regelverk som følge av EUs forordning om kontroll av utenlandske direkteinvesteringer. Selv om Norge tradisjonelt har hatt en åpen og liberal økonomi der utenlandske investeringer har vært ønsket velkommen, krever den geopolitiske situasjonen tiltak for å både redusere og håndtere sårbarheter og risiko. Summen av investeringer og oppkjøp kan medføre at kontrollen over kritiske verdier havner hos stater Norge ikke har et sikkerhetspolitisk samarbeid med. Samtidig er utenlandske investeringer viktig for norsk økonomi. Legges det for store begrensninger på utenlandsk kapital til Norge vil dette kunne vanskeliggjøre tilgangen til globale konkurransemarkeder, hvilket vil kunne ha negative konsekvenser for verdiskapning, arbeidsplasser og innovasjon. Utvalget foreslår blant annet at det etableres en meldeordning for utenlandske direkteinvesteringer i sikkerhetssensitive sektorer og at det utarbeides en ny lov for investeringskontroll. Utvalget anbefalte å se hen til EUs liste over kritiske teknologier, selv om den er for overordnet til å fungere som en avgrensing for en meldeplikt i fremvoksende teknologier. Ifølge utvalget bør nasjonale myndigheter i størst mulig grad etablere en felles forståelse for hvilke teknologier og typer kunnskap som er sensitive for nasjonale sikkerhetsinteresser. Nærings- og handelsdepartementet følger opp arbeidet, og KVAST-prosjektet har hatt dialog om hvordan kunnskapsgrunnlaget fra KVAST kan bidra.

1.2.7. Felles datasystem for forsvarsrelevant forskning

Forsvarsdepartementet har gitt et oppdrag til Forskningsrådet og FFI om å utvikle et system som kan samle data om forsvarsrelevant forskning, og som kan understøtte bedre styring og samarbeid på tvers av sektorer. Formålet er å styrke strategisk styring, ressursutnyttelse og samarbeid mellom aktører i forsvarssektoren og det sivile forskningsmiljøet, og få bedre oversikt over forskningsaktivitet og tilgang til forskningsresultater på tvers av graderingsnivåer. Systemet skal gi helhetlig innsikt i forsvarsrelevant forskning, inkludert både sivil og militær sektor, og legge til rette for analyser, samarbeid og risikovurderinger. Gjennom KVAST-prosjektet har det blitt tydelig at det ikke er mulig å gi en fullstendig oversikt over nasjonal aktivitet og kompetanse på sensitive teknologier, ettersom det er en del forskning på og utvikling av teknologiene som ikke synliggjøres gjennom publiserings- og prosjektdata. Det gjelder en del oppdragsforskning i og for næringslivet samt forskning som er gradert. Dette omfatter blant annet en stor del av forskningen som gjøres ved FFI. Et felles system vil kunne bidra til å gi et mer helhetlig kunnskapsgrunnlag.

1.3. Gjennomføring og avgrensing av prosjektet

1.3.1. Tre hovedspor i gjennomføringen av KVAST-prosjektet

KVAST-prosjektet har tre hovedspor: For å møte behovet for en mer helhetlig og felles tilnærming på tvers av sektorer og institusjoner er det behov for et felles referansepunkt og en forståelse av hvilke teknologiområder og teknologier som til enhver tid oppfattes som sensitive. Den første hovedleveransen i prosjektet er en **oversikt over sensitive teknologier for norske forhold**. Arbeidet med denne oversikten er basert på en sammenstilling og sammenligning av tilsvarende internasjonale lister (EU/NATO-land). Videre er det behov for et bedre **kunnskapsgrunnlag om Norges aktivitet og posisjon** innenfor disse teknologiene og hvordan vi samarbeider internasjonalt. Arbeidet med å kartlegge Norges status og posisjon innenfor de sensitive teknologiene bygger på en spørreundersøkelse, fagevalueringer, prosjektdata og bibliometriske analyser. I tillegg er det behov

[7] NOU 2023: 28 Investeringskontroll – En åpen økonomi i en usikker tid

for kunnskap og metoder for å vurdere risiko knyttet til de ulike teknologiene. I prosjektet er det utviklet en metode for **risikovurdering av sensitive teknologier** og gjennomført en risikovurdering 14 utvalgte teknologier.

Alle deler av prosjektet er utført i tett samarbeid mellom Norges forskningsråd, Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets forskningsinstitutt (FFI).

Både de aktuelle teknologiene, den internasjonale sikkerhetssituasjonen og kunnskapsfronten er i stadig utvikling, og det er behov for å sikre at kunnskapen om sensitive teknologier og risikoen som er forbundet med dem oppdateres jevnlig. Videre arbeid med oppdatering av kunnskapsgrunnlaget er omtalt i kapittel 5 nedenfor.

1.3.2. Avgrensninger

Prosjektet baserer seg på åpent tilgjengelig informasjon om forskningsvirksomhet, som prosjektdata og publikasjonsdata. Innretningen på oppdraget og innhentet kunnskapsgrunnlag gjør at deler av aktiviteten knyttet til de aktuelle teknologiene ikke er belyst. Dette gjelder særlig anvendt teknologiutvikling i deler av næringslivet hvor det i liten grad publiseres vitenskapelig knyttet til de aktuelle teknologiene. Noe fanges imidlertid opp der næringslivet har deltatt i prosjekter i regi av Forskningsrådet, Horisont Europa eller European Defence Fund.

Prosjektets innretning og kildetilfang gjør også at det vil være FoU-aktivitet knyttet til sensitive teknologier hvor informasjonen er sikkerhetsgradert og som ikke er dekket av prosjektet. Dette gjelder for eksempel FoU knyttet til forsvarssektoren som foregår på et høyt teknologimodenhetsnivå, og hvor resultater og informasjon om samarbeid ikke er åpent tilgjengelig. Et av formålene med KVAST-prosjektet er etablere et kunnskapsgrunnlag for å vurdere behov for eventuelle risikoreduserende tiltak knyttet til FoU-aktivitet på sensitive teknologier. Behovet for tiltak for sikkerhetsgradert FoU ligger utenfor formålet med KVAST-prosjektet.

Teknologioversikten og tilhørende vurderinger fra dette prosjektet dekker svært bredt og berører mye av teknologiforskningen i Norge. I prosjektet brukes et detaljnivå som svarer til de internasjonale teknologioversiktene, med 11 hovedkategorier (teknologiområder) og 48 underkategorier (teknologier). Samtidig bemerkes det at all forskning er svært spesialisert, og i flere tilfeller vil selv underkategoriene som er benyttet i dette prosjektet i praksis være brede kategorier med stor intern variasjon, både med hensyn til sensitivitet, risiko og anvendelse/teknologimodenhet. Dette forholdet er presisert i risikovurderingene som er gjort i del 4 av prosjektet.

1.4. Introduksjon til kapittel 2-5

Hovedkapitlene i denne sluttrapporten gir beskrivelser og sammendrag av arbeidet som er utført under de ulike delprosjektene i KVAST.

Delleveranse 1 i prosjektet har bestått i å beskrive metode og tidsplan for prosjektet.[8]

Kapittel 2 i denne sluttrapporten beskriver den andre delleveransen i prosjektet, en **oversikt over sensitive teknologier for norske forhold**.

[8] Vedlegg 1: KVAST delleveranse 1: Beskrivelse av gjennomføring (Januar 2025)

I kapittel 3 beskrives arbeidet med å **kartlegge Norges posisjon innenfor de sensitive teknologiene** gjennom bruk av spørreundersøkelser, fagevalueringer, analyser av prosjektdata og bibliometriske analyser.

I kapittel 4 beskriver vi en metode for **risikovurdering** av sensitive teknologier og viser til risikovurdering som er gjennomført på utvalgte teknologier.

I kapittel 5 gir vi en oppsummering av dialog og reaksjoner fra FoU-institusjoner og departement, og anbefalinger for det videre arbeidet med KVAST.

Kapitlene 2-4 i gir beskrivelser og sammendrag av arbeidet som er utført. De ulike delleveransene i prosjektet, slik som grunnlaget for en norsk teknologioversikt, kartlegging av Norges posisjon, og risikovurdering av utvalgte teknologier, er tilgjengelig som selvstendige rapporter som utgjør vedlegg til denne sluttrapporten.

2. Oversikt over sensitive teknologier for norske forhold

2.1. Om arbeidet med en norsk teknologioversikt

I oppdragsbrevet forventes prosjektet å utarbeide en systematisk sammenstilling av relevant eksisterende kunnskap / oversikter / lister som omhandler sensitive teknologier, på tvers av ulike land og sektorer. Dette arbeidet har resultert i en rapport hvor FFI utførte det meste av arbeidet (delleveranse 2).

I tillegg skulle prosjektet identifisere eventuelle kunnskapshull av betydning for norske forhold og behov, samt gi anbefalinger om hvordan disse hullene eventuelt kan tettes. Dette spørsmålet er tatt opp i prosjektets delleveranse 3 (se neste kapittel).

Sensitive, kritiske og strategiske teknologier er begreper som ofte brukes om hverandre og som kan overlappe. Arbeidet med delleveranse 2 bygger på en forståelse av disse begrepene hvor *sensitive* teknologier er teknologier som må skjermes på grunn av risiko for misbruk, *kritiske* teknologier er teknologier som er avgjørende for en nasjons sikkerhet og samfunnsfunksjoner, mens *strategiske* teknologier er teknologier som gir et land komparative fortrinn. Sensitive teknologier kan være kritiske for nasjonal sikkerhet og kan også være strategiske fordi det er behov for og må overvåkes for å sikre kompetanse og internasjonalt samarbeid.

En del av arbeidet med delleveranse 2 har vært en gjennomgang av hvordan begrepene brukes internasjonalt, og følgende definisjon av sensitive teknologier er lagt til grunn for arbeidet:

> *Sensitive teknologier: Teknologier som ved tilegnelse fra uønskede aktører, vil kunne påvirke norske sikkerhetsinteresser og teknologisk konkurranseevne negativt.*

Delleveranse 2 sammenstiller eksisterende kunnskap om kritisk, sensitiv og strategisk teknologi mellom forskjellige land og sektorer, med et mål om å lage et videre kunnskapsgrunnlag og forslag til en norsk liste over sensitive teknologier med hensyn til nasjonal sikkerhet. Videre fremhever delleveranse 2 viktigheten av å definere og oversette kritiske teknologiområder for norsk kontekst, og understreker åpenhet og samarbeid mellom ulike aktører for ytterligere utvikling og beskyttelse av nasjonale sikkerhetsinteresser.

Delleveranse 2 diskuterer også viktigheten av teknologi i dagens hurtig utviklende landskap, særlig i forhold til nasjonal sikkerhet. Notatet fremhever den geopolitiske konkurransen om teknologisk dominans, der fremvoksende og disruptive teknologier ikke bare skaper muligheter, men også nye risikoer og trusler. Konseptet om den fjerde industrielle revolusjon, der teknologi er intelligent, sammenkoblet, desentralisert og digital, utfordrer skillet mellom sivil og militær teknologi. Det understreker behovet for samarbeid mellom offentlige myndigheter, akademia og næringslivet for å møte kravene til forskningssikkerhet.

Delleveranse 2 beskriver EUs innsats for å identifisere og prioritere teknologier av strategisk betydning for den økonomiske sikkerheten. Listen fra EU fremhever ti kritiske teknologiområder: avanserte halvlederteknologier, kunstig intelligens, kvanteteknologier, bioteknologier, avansert samband og navigasjon, avanserte sensorteknologier, romfartsteknologier, energiteknologier, robotikk og autonome systemer, samt avanserte materialer og produksjonsteknologier. Her diskuteres også EU-kommisjonens prioritet til fire teknologiområder—avanserte halvledere, kunstig

intelligens, kvanteteknologi og bioteknologi—på grunn av deres høye risiko for teknologilekkasje og potensial for flerbruk (dual-use). EU ser det som avgjørende å redusere avhengigheten av eksterne leverandører, styrke teknologisk lederskap og beskytte avanserte forsknings- og utviklingsarbeider. Bransjeforeningen DIGITALEUROPE fremhever også EUs nåværende teknologiske posisjon og identifiserer hull i konkurranseevnen sammenlignet med globale ledere som USA og Kina, og oppfordrer til politiske tiltak for å forbedre EUs teknologiske konkurranseevne.[9]

Videre i notatet sammenlignes EUs liste over kritiske teknologier med tilsvarende lister fra NATO og flere land, inkludert USA, Storbritannia, Canada, Australia, Danmark, Sverige, Finland og Nederland. Hensikten er å kort vurdere hvilke teknologiområder disse landene prioriterer for å styrke nasjonal sikkerhet og økonomisk konkurranseevne.

- NATO fokuserer mer på militære teknologier som hypersoniske våpen og energivåpen, mens EU legger vekt på økonomisk sikkerhet og teknologisk suverenitet.
- USA har en bredere tilnærming med detaljerte teknologier som avansert databehandling og våpenteknologier, mens EU fokuserer på teknologisk autonomi.
- Storbritannia fremhever bredere teknologier som 6G og energiteknologier, i kontrast til EUs fokus på avanserte halvledere og KI.
- Canada inkluderer avanserte sensorer og våpenteknologier som ikke er nevnt i EUs liste.
- Australia har mange flere kritiske teknologier og vektlegger spesielt energiteknologier og militære anvendelser.
- Danmark legger vekt på grønne teknologier og digital innovasjon, koblet til bærekraft innen EUs ramme.
- Sverige vektlegger energiteknologi for en grønnere samfunnsstruktur, mens EU har en bredere sikkerhetstilnærming.
- Finland fremhever cybersikkerhet i tråd med NATOs krav, i større grad enn EUs fokus på teknologisk uavhengighet.
- Nederland prioriterer spesifikke teknologier som integrert fotonikk, med fokus på nasjonale styrker innen kommunikasjon.

Analysen, sammendraget og oppsummeringen i kapittel fire av notatet uthever hvordan hver nasjon tilpasser sine teknologiske prioriteringer for å møte sine unike nasjonale mål, i motsetning til EUs mer generelle strategi for økonomisk sikkerhet og teknologisk autonomi.

Notatets kapittel fem bygger på EUs liste over kritiske teknologier og analyser av andre lands lister for å utarbeide et forslag til en norsk liste over kritiske teknologier. Det norske forslaget tar utgangspunkt i EUs ti teknologiområder, men inkluderer også enkelte teknologier som er fremhevet i andre lands lister. Forslaget innebærer dermed i noen tilfeller utvidelse av eksisterende teknologiområder i EUs liste. I tillegg introduseres en egen kategori kalt "Undervannsteknologi", som ikke finnes i EUs liste. Denne kategorien omfatter spesielt teknologi for navigasjon, kommunikasjon og (miljø)sensorer under vann.

[9] "The EU's Critical Tech Gap: Rethinking economic security to put Europe back on the map", DIGITALEUROPE (2024).

Kapittelet legger spesielt vekt på at de fire første teknologiområdene i forslaget, som avanserte halvledere og kunstig intelligens, har stort flerbruks-potensial og er gjensidig avhengig med øvrige teknologiområder.

Avslutningsvis vises det en utvidet norsk oversikt (sammenlignet med EUs liste), basert på nasjonale behov og globale teknologitrender. Det ble understreket at denne oversikten ikke var endelig, men dannet grunnlag for det videre arbeidet. Oversikten kunne bli endret som følge av funn eller innspill i de neste delleveransene.

2.2. Anbefalt oversikt over sensitive teknologier for norske forhold

Etter at delleveranse 2 var ferdigstilt og offentliggjort, ble det gjennomført en større undersøkelse rettet mot UH- og instituttsektor, helseforetak og relevant industri. Denne undersøkelsen inngår i delleveranse 3 (se kapittel 3 under) og i kartleggingen av Norges aktivitet og posisjon innenfor sensitive teknologier.

Undersøkelsen tok utgangspunkt i den foreslåtte oversikten i delleveranse 2, og har tjent til å kvalitetssikre denne oversikten og avdekke eventuelle mangler eller feil ved den foreslåtte oversikten, samt få kommentarer på norske oversettelser av begreper som benyttes i internasjonale teknologioversikter. Undersøkelsen har også være viktig for å belyse om det er særlige norske forhold som bør fremheves i en slik oversikt.

Resultatet fra dette arbeidet er en oversikt som ligger tett på EUs oversikt «Critical Technology Areas». De viktigste forskjellene fra EUs oversikt er at det er tilføyd en teknologi, «maskinlæring og dyplæring», under kategorien Teknologier for kunstig intelligens, og at det er lagt til en egen hovedkategori for «Undervannsteknologier». I tillegg er det oversatt fra EUs oversikt til norske teknologibenevnelser.

Med utgangspunkt i delleveranse 2 og påfølgende justeringer etter innspill fra sektoren, anbefales følgende oversikt over sensitive teknologier for norske forhold:

Advanced Semiconductors Technologies	**Avanserte halvlederteknologier**
Microelectronics, including processors	Mikroelektronikk, inkludert prosessorer
Photonics (including high energy laser) technologies	Fotonikkteknologier, inkludert høyenergilaser
High frequency chips	Databrikker med høyfrekvensegenskaper
Semiconductor manufacturing equipment at very advanced node sizes	Utstyr for produksjon av halvledere med svært små nodestørrelser
Artificial Intelligence Technologies	**Teknologier med kunstig intelligens**
High Performance Computing	Tungregning
Cloud and edge computing	Skytjenester og kantprosessering

Data analytics technologies	Dataanalytiske teknologier
Computer vision, language processing, object recognition	Datamaskinsyn, språkbehandling og objektgjenkjenning
Machine learning and deep learning	Maskinlæring og dyplæring
Quantum Technologies	**Kvanteteknologier**
Quantum computing	Kvanteberegning
Quantum cryptography	Kvantekryptografi
Quantum communications	Kvantekommunikasjon
Quantum sensing and radar	Kvantesensorer og -radar
Biotechnologies	**Bioteknologier**
Techniques of genetic modification	Genmodifiseringsteknikker
New genomic techniques	Nye genomiske teknikker
Gene-drive	Gendrivere
Synthetic biology	Syntetisk biologi
Advanced connectivity, Navigation and digital Technologies	**Avansert samband, navigasjon og digitale teknologier**
Secure digital communications and connectivity, such as RAN & Open RAN (Radio Access Network) and 6G	Sikker forbindelse og digital kommunikasjon, som RAN (Radio Access Network), Open RAN og 6G
Cyber security technologies incl. cyber-surveillance, security and intrusion systems, digital forensics	Cybersikkerhetsteknologier, inkludert cyberovervåkning og sikkerhets- og inntrengningssystemer, og digital etterforskning.
Internet of Things and Virtual Reality	Tingenes internett og virtuell virkelighet
Distributed ledger and digital identity technologies	Distribuerte regnskapsbøker, som blokkjedeteknologi, og distribuert digital identitetsteknologi
Guidance, navigation and control technologies, including avionics and marine positioning	Styrings-, navigasjons- og kontrollteknologier, inkludert avionikk og maritim posisjonering
Human–Machine Interaction, including AR and VR	Menneske–maskin-interaksjon, inkludert AR og VR

Advanced sensing Technologies	**Avanserte sensorteknologier**
Electro-optical, radar, chemical, biological, radiation and distributed sensing	Elektrooptiske, kjemiske, biologiske og distribuerte sensorer, radar- og strålingssensorer.
Magnetometers, magnetic gradiometers	Magnetometre og magnetiske gradiometre
Gravity meters and gradiometers	Gravimetre og gradiometre
Space & propulsion technologies	**Romfarts- og fremdriftsteknologier**
Dedicated space-focused technologies, ranging from component to system level	Dedikert romrettet teknologi, fra komponent- til systemnivå
Space surveillance and Earth observation technologies	Romovervåknings- og jordobservasjonsteknologier
Space positioning, navigation and timing (PNT)	Posisjonsbestemmelse, navigasjon og tidsbestemmelse (PNT)
Secure communications including Low Earth Orbit (LEO) connectivity	Sikker kommunikasjon, inkludert kommunikasjon via lav jordbane (LEO)
Propulsion technologies, including hypersonics and components for military use	Hypersoniske kapabiliteter og komponenter for militært bruk
Energy technologies	**Energiteknologier**
Nuclear fusion technologies, reactors and power generation, radiological conversion/enrichment/recycling technologies	Fusjonskraftteknologi, reaktorer og kraftproduksjon, og teknologier for konvertering, anrikning og resirkulering av radioaktive materialer
Hydrogen and new fuels	Hydrogen og nye drivstoff
Net-zero technologies, including photovoltaics	Netto-null-teknologier, inkludert solenergi
Smart grids and energy storage, batteries	Kraftteknologier, inkludert smarte strømnett, energilagring og batterier
Robotics and autonomous systems	**Robotikk og autonome systemer**
Drones and vehicles (air, land, surface and underwater)	Ubemannede farkoster (i lufta, på land, på overflaten og under vann)
Robots and robot-controlled precision systems	Roboter og robotstyrte presisjonssystemer
Exoskeletons	Eksoskjeletter

AI-enabled systems	KI-drevne systemer
Advanced materials, manufaturing and recycling technologies	**Avanserte materialer, produksjons- og resirkuleringsteknologier**
Technologies for nanomaterials, smart materials, advanced ceramic materials, stealth materials, safe and sustainable by design materials	Teknologier for nanomaterialer, smarte materialer, avanserte keramiske materialer, lavsignaturmaterialer og trygge materialer utformet med tanke på sikkerhet og bærekraft
Additive manufacturing, including in the field	Additiv produksjon, inkludert i felt
Digital controlled micro-precision manufacturing and small-scale laser machining/welding	Digitalt kontrollert mikropresisjonsproduksjon og småskala laserbearbeiding og -sveising
Technologies for extraction, processing and recycling of critical raw materials (including hydrometallurgical extraction, bioleaching, nanotechnology-based filtration, electrochemical processing and black mass)	Teknologier for utvinning, prosessering og gjenvinning av kritiske råmaterialer, inkludert hydrometallurgisk utvinning, bioutluting, nanoteknologibasert filtrering, elektrokjemisk prosessering og svart masse
Underwater Technologies	**Undervannsteknologier**
Underwater positioning and navigation, including sonar-based navigation, terrain correlation, and inertial navigation.	Undervannsposisjonering og -navigasjon, inkludert sonarbasert navigasjon, terrengkorrelering og treghetsnavigasjon
Underwater communication, including the use of sound waves, low-frequency radio waves, or lasers.	Undervannskommunikasjon, inkludert ved bruk av lydbølger, lavfrekvente radiobølger eller laser.
Underwater sensors, including sonars and synthetic aperture sonar (SAS), sensors for electric fields, and electro-optical sensors.	Undervannssensorer, inkludert sonarer og syntetisk apertursonar (SAS), sensorer for elektriske felt og elektrooptiske sensorer.
Technologies for underwater vehicles, including design, propulsion, and power supply.	Teknologier for undervannsfarkoster, inkludert utforming, fremdrift og energiforsyning.
Technologies for underwater installations and infrastructure, including power supply and other technologies that enable underwater infrastructure.	Teknologier for undervannsinstallasjoner og -infrastruktur, inkludert energiforsyning og andre teknologier som muliggjør infrastruktur under vann.

3. Aktører, kompetanse og samarbeid innenfor sensitive teknologier

Delrapport 3 omhandler Norges posisjon innenfor sensitive teknologiene per i dag (status). Noen sentrale spørsmål oppdraget skulle besvare var:

- Hvem er sentrale nøkkelaktører og hvor finnes de viktigste fagmiljøene innenfor hvert teknologiområde?
- På hvilke av de aktuelle teknologiområdene er Norge per i dag ledende?
- På hvilke områder mangler Norge nasjonal kunnskap/kompetanse som vi bør ha?
- Hvem samarbeider Norge med på hvilke områder?
- På hvilke områder er Norge avhengig av samarbeid med hhv. allierte og ikke-allierte?

Teknologiområdene som undersøkes er de som er definert som sensitive teknologier for norske forhold i delleveranse 2.

Spørsmålene ovenfor er relevante både med hensyn til nasjonal sikkerhet og økonomisk sikkerhet. I Nasjonal sikkerhetsstrategi fra mai i år, understrekes det at Norge skal være blant de beste til å forstå og anvende ny teknologi, og at det er avgjørende for norsk sikkerhet og økonomi.[10] Kunnskap om hvor Norge har sterke forskningsmiljøer er viktig for bevisstgjøring om hvilke miljøer som er attraktive for utenlandske aktører. Tilsvarende gir kunnskap om hvor Norge har svak kompetanse innsikt i mulige sårbarheter når det gjelder økonomisk sikkerhet. Kartlegging av samarbeidsrelasjoner gir nyttig kunnskap om hvilke land Norge samarbeider mye og lite med innenfor de ulike teknologiene. Ikke-allierte er her definert som land som nevnes i åpne trusselvurderinger, Kina, Russland, Iran og Nord-Korea.

3.1. Metode

Tre hovedkilder ble brukt for å besvare spørsmålene:

- Spørreundersøkelse rettet mot aktuelle forskningsaktører om sensitive teknologier.
- Forskningsrådets fagevalueringer om biovitenskap, naturfag og matematikk, IKT og teknologi.
- Analyse utført av Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU) basert på publikasjoner og prosjektdata.

3.2. Spørreundersøkelse og dialog med forskningsaktører

Spørreundersøkelsen rettet seg mot forskningsaktører i universitets- og høgskolesektoren, instituttsektoren, helseforetak/sykehus og forsvarsindustrien i Norge.

Spørreundersøkelsen har vært viktig for å forankre og kvalitetssikre den foreslåtte teknologioversikten i norsk forskningssektor, samt bidra til å identifisere eventuelle mangler eller uklare områder i den foreslåtte oversikten. I undersøkelsen har forskningsmiljøene også gjort egenevalueringer av forskningsaktiviteten innenfor de aktuelle teknologiene, vurderinger av sensitivitet og militær relevans, rekrutteringssituasjon og samarbeidsflater. Undersøkelsen har

[10] Nasjonal sikkerhetsstrategi (s. 28)

dermed bidratt til å besvare både del 2 (teknologioversikt for norske forhold) og del 3 (kartlegging av aktører og aktivitet) av KVAST-prosjektet.

Som en videreføring av undersøkelsen har prosjektgruppen høsten 2025 gjennomført dialogmøter med de miljøene som har høyest aktivitet innenfor teknologiene. I tillegg til å utdype institusjonenes svar i spørreundersøkelsen, har disse dialogmøtene gitt viktige innspill til det videre arbeidet med sensitive teknologier og forskningssikkerhet (se også kap. 5 Anbefalinger og veien videre).

Undersøkelsen som ble gjennomført i mai-juni 2025 har bestått av flere hoveddeler:

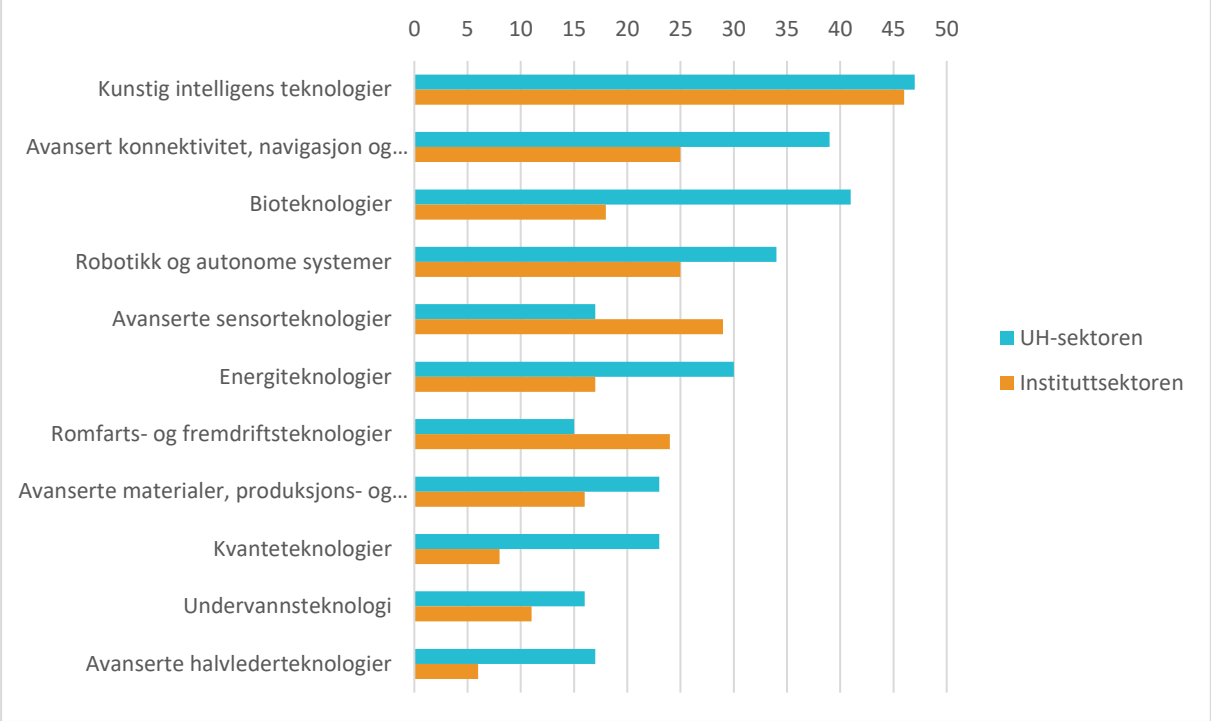
1. **Kvalitetssikring av oversikten over sensitive teknologier**:
    - Deltakerne bes vurdere om foreslåtte teknologiområder og underkategorier er relevante for norske forhold, om det mangler viktige teknologier, samt om begrepsbruken er dekkende.
2. **Kartlegging av forskningsaktivitet**:
    - Aktørene skal oppgi hvilke sensitive teknologiområder det forskes på hos dem, samt omfanget av aktiviteten.
3. **Vurdering av sensitivitet**:
    - Institusjonene bes vurdere hvor sensitive teknologiområdene er for norsk sikkerhet eller konkurranseevne.
4. **Militær relevans**:
    - Deltakerne vurderer sannsynligheten for at teknologien kan ha militær bruk.
5. **Rekrutteringssituasjonen**:
    - Spørsmål om hvor lett/vanskelig det er å rekruttere søkere fra NATO-land til relevante stillinger.
6. **Samarbeidsflater**:
    - Kartlegging av samarbeid mellom forskningsmiljøer og industri, spesielt for FSi-medlemmer.

3.3. Fordeling på teknologiområder

Vår vurdering er at de fleste relevante aktørene i UH- og instituttsektoren har besvart undersøkelsen. Store institusjoner kunne velge å svare på fakultets- eller avdelingsnivå. Det er få svar fra helseforetak/sykehus og forsvarsindustri. Se delleveranse 3 for fullstendig oversikt over hvem som har svart. På spørsmålet om aktivitetsnivå på de ulike teknologiområdene var det tre hovedalternativer, i tillegg til «vet ikke»:

- Stor aktivitet: Stort volum når det gjelder prosjekter og investeringer.
- Noe aktivitet: En viss aktivitet, men det er begrenset til et mindre antall prosjekter og initiativer.
- Liten aktivitet: Svært liten aktivitet, med minimal investering.

Figuren under viser fordelingen på teknologiområder i henholdsvis UH-sektoren og instituttsektoren. Figurene viser teknologiområder hvor det er rapportert om «stor» eller «noe» aktivitet. Hvert teknologiområde består av flere underkategorier, så en institusjon kan for eksempel ha oppgitt stor aktivitet på fire ulike kunstig intelligens teknologier. Derfor blir antall svar høyere enn antall respondenter (41).



Figur 1. Antall som har svart «stor» eller «noe» aktivitet på teknologiområder innenfor UH- og instituttsektoren

3.4. Dialog med forskningsaktører

Som en videreføring av spørreundersøkelsen gjennomførte prosjektet høsten 2025 dialogmøter med et utvalg av institusjonene som har deltatt. Dette er institusjoner som rapporterte særlig høy aktivitet innen ett eller flere av de definerte sensitive teknologiområdene, og som derfor er sentrale når det gjelder forskning og utvikling på de definerte sensitive teknologiene.

Formålet med dialogmøtene er å gå dypere inn i temaene som har kommet frem i undersøkelsen, og få bedre innsikt i institusjonenes vurderinger av teknologienes sensitivitet, konkrete bruksområder, flerbrukspotensial og eventuelle utfordringer knyttet til rekruttering, samarbeid og kunnskapsdeling. Gjennom samtaler mellom prosjektgruppen og institusjonenes fagmiljøer ønsket vi å utfylle og nyansere det bilde spørreundersøkelsen har gitt, og samtidig få frem institusjonenes egne synspunkter og behov knyttet til kunnskapsgrunnlag. Dette er ikke minst viktig for videre arbeid med KVAST-prosjektet (se kapittel 5 under).

Samtalene ble gjennomført digitalt med: Forsvarets forskningsinstitutt (FFI), Institutt for Energiteknikk (IFE), NTNU - Fakultet for informasjonsteknologi og elektroteknikk, Fakultet for medisin og helsevitenskap og Fakultet for naturvitenskap, SINTEF, UiB- Fakultet for naturvitenskap og teknologi og UiO Det matematisk-naturvitenskapelige fakultet. Deltakerne har i hovedsak vært fakultetsansatte, instituttledere, forskningssjefer, sikkerhetspersonell, samt deltakere fra KVAST-prosjektet. I tillegg hadde prosjektet samtale med Kongsberg Gruppen.

Samtalene gir viktige tilbakemeldinger om institusjonenes erfaringer med KVAST-undersøkelsen og et inntrykk av hvordan ulike fagmiljøer opplever og håndterer forskningssikkerhet, med søkelys på

utfordringer, behov og forslag til videre prosess etter KVAST. Dialogen med institusjonene gir dermed viktige perspektiver til det videre arbeidet med løpende oppdatering og videreutvikling av kunnskapsgrunnlaget.

3.5. Forskningsrådets fagevalueringer om biovitenskap, naturfag og matematikk, IKT og teknologi

Forskningsrådet gjennomfører fagevalueringer av alle vitenskapelige disipliner ca. hvert tiende år. Hovedmålet med evalueringene er å identifisere og bekrefte kvaliteten og relevansen av forskningen som utføres ved UH-institusjoner og i instituttsektoren. Evalueringene utføres av internasjonale fageksperter, og evalueringsrapportene gir en samlet vurdering av forskningsstatus for en tiårsperiode, i tillegg til anbefalinger for videre utvikling av forskningsdisiplinene. I perioden 2022–2025 er det gjennomført tre evalueringer der ulike teknologier er sentrale: én innen biovitenskap (EVALBIOVIT), én innen naturvitenskap (EVALNAT) og én innen matematikk, IKT og teknologi (EVALMIT).

Fagevalueringene i regi av Forskningsrådet er ikke innrettet med det formål å evaluere de sensitive teknologiene spesielt. For fagevalueringen av matematikk, IKT og teknologi (EVALMIT) ble det likevel skrevet en tilleggsrapport som baserer seg på evalueringen for øvrig, og det ble ikke gjort en egen analyse. Fagevalueringene gir imidlertid god kunnskap om hvor Norge regnes som gode eller svake innenfor enkelte av teknologiene.

3.6. Norges posisjon innenfor sensitive teknologier

Etter en anbudsrunde juni 2025 fikk Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU) oppdraget med å bistå med å besvare hovedspørsmålene i delleveranse 3. Oppdraget ble utført i perioden 18.08.2025 – 15.10.2025 og resultatet er rapporten «Kartlegging av norsk forskning på sensitive teknologier» (NIFU Rapport 2025:17). Formålet var å identifisere FoU-aktivitet innenfor sensitive teknologiområder og NIFU utviklet en metode for å kartlegge FoU-omfanget spesielt for KVAST-prosjektet. NIFU har videre analysert publikasjonsdata fra Web of Science for perioden 2015-20024 og prosjekta fra Norges forskningsråd og EUs rammeprogram for perioden 2020-2024 og European Defence Fund for perioden 2021-2024.

3.6.1. På hvilke av teknologiområder har Norge relativt sterke eller svake fagmiljøer?

Basert på fagevalueringer, publikasjons- og prosjektdataene kan vi indikere på hvilke teknologiområder Norge synes å ha relativt sterke og relativt svake fagmiljøer sett i forhold til sammenlignbare fagmiljøer i utlandet. Å foreta en vurdering av hvorvidt norske fagmiljøer er (internasjonalt) ledende på noen av de aktuelle teknologiområdene ville krevd langt større ressurser.

Kunstig intelligens skiller seg ut som Norges sterkeste forskningsområde innenfor de sensitive teknologiene. Norske artikler er høyt sitert og den totale produksjonen av artikler er relativt høy for perioden 2015-2024. Selv om antallet kun utgjør en marginal andel av verdensproduksjonen i samme periode, er tallet høyt sammenlignet med norsk produksjon på andre teknologiområder, og veksten har vært kraftig de siste ti årene. I tillegg er antallet artikler produsert totalt sett høyt, noe som er et tegn på kontinuitet i både produksjon og siteringer.

Det er også på *kunstig intelligens* at Norge mottar klart mest midler fra EU-prosjekter. I tillegg er andelen prosjekter som Norge koordinerer høy. På *energiteknologier* henter Norge nest mest penger

fra EU-prosjekter. På begge områdene henter Norge betydelig mer penger enn forventet gitt fordelingen i EUs totale prosjektportefølje. Det er flere indikatorer i prosjektdataene som NIFU har analysert som taler for at *energiteknologi* er et enda sterkere felt for Norge enn *kunstig intelligens*, til tross for at det er på kunstig intelligens det er mottatt flest midler.

Robotikk og autonome systemer og *romfart og fremdriftsteknologier* har relativt høye siteringstall. Disse områdene har imidlertid mye lavere total produksjon. Mens norsk forskning på *kunstig intelligens* produserte om lag 2500 artikler i løpet av perioden, produserte *robotikk og autonome systemer* og *romfart og fremdriftsteknologier* henholdsvis 405 og 184 artikler.

Avanserte materialer, produksjons- og resirkulasjonsteknologier er også et område hvor norsk forskning er relativt sterk. På samme måte som for de to ovennevnte områdene er *avanserte materialer* et område hvor norsk forskning henter inn mer midler enn forventet og har høy grad av koordinering i prosjekter. Også *robotikk og autonome systemer* skiller seg ut med særlig høy koordineringsgrad. Dette er også et område hvor Norge henter mer penger enn forventet og som skårer relativt høyt på den folketallsjusterte indikatoren for innhentede EU-midler.

Romfarts- og fremdriftsteknologier og *undervannsteknologier* er områder hvor Norge henter inn langt mindre penger enn forventet gitt fordelingen i EUs budsjettportefølje. Norge kommer litt bedre ut etter folketallsjusteringen, men er fortsatt lite deltakende. Videre koordinerer Norge ingen prosjekter på disse områdene. For *undervannsteknologier* henger dette sammen med at dette er et lite felt i europeisk sammenheng som det lyses ut få midler på, mens for *romfarts- og fremdriftsteknologier* – som er et stort felt i europeisk sammenheng – kan ikke svakheten forklares på samme måte. Kontrasten er også stor til de ekstremt gode siteringstallene Norge har på dette området.

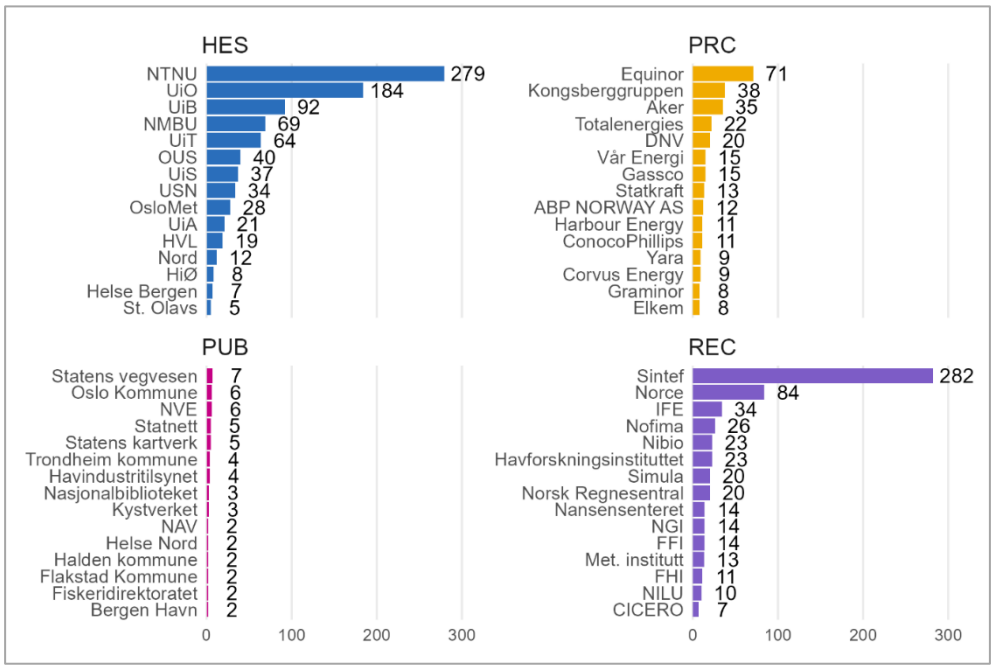
Undervannsteknologier er et litt spesielt område fordi volumet (og siteringstallene) er svært lave. Dette er imidlertid et veldig lite område internasjonalt, og relativt sett har Norge sterk publiseringsaktivitet på dette området[11]. Nettopp fordi Norge er relativt sterke på undervannsteknologier, kan det være et område andre aktører ønsker tilgang til, jf. saken om at norsk undervannsteknologi er særlig ettertraktet for Russland ettersom de ikke har denne teknologien selv[12]. Risikovurderinger av teknologiområder og enkeltteknologier er nærmere omtalt i kapittel 4.

3.6.2. Hvor er de mest sentrale fagmiljøene innenfor hvert teknologiområde?

NTNU er den norske aktøren med høyest antall publikasjoner og høyest prosentandel forfatterandeler på alle de sensitive teknologiområdene i perioden 2015-2024, bortsett fra ett. Innenfor bioteknologier har Universitetet i Bergen størst produksjon. På flere av teknologiområdene er NTNUs bidrag (minst) dobbelt så stort som nest største institusjon. For eksempel når det gjelder energiteknologier har NTNU 2,9 ganger så mange publikasjoner som SINTEF og 3,7 ganger så mange publikasjoner som Universitetet i Oslo.

[11] Blant annet har NTNU AMOS som var et senter for fremragende forskning (2013-2023) bidratt til dette.
[12] Kongsberg-utstyr videresolgt til Russland – kan bidra til beskyttelse av atomvåpen i Russland – Troms og Finnmark

Figuren under viser de mest aktive norske aktørene innen de fire sektorene høyere utdanning (HES), instituttsektor (REC), privat næringsliv (PRC) og offentlig sektor (PUB) når prosjektdeltakelse i Forskningsrådsprosjekter, Horisont Europa og European Defence Fund slås sammen.



Figur 2. De 15 mest aktive norske institusjonene i prosjekter innen sensitive teknologier - totalt antall prosjektdeltakelser 2020-2024 (Horisont Europa, EDF og Forskningsrådet)

3.6.3. På hvilke områder mangler Norge nasjonal kunnskap som vi burde ha?

NIFU presiserer i sin rapport at spørsmålet om hva slags kunnskap/kompetanse Norge *bør* ha er et politisk spørsmål som deres data og analysemetoder ikke egner seg til å besvare. Likevel kan svarene på de andre spørsmålene som ble stilt i oppdraget benyttes til å belyse også dette spørsmålet.

NIFUs analyse viser til at *avanserte halvledere*, *avanserte sensorer* og *kvanteteknologier* skiller seg ut som områdene der Norge er svakest. Samtlige er svake fordi de har en kombinasjon av relativt lav andel topp 10% mest siterte artikler og lav total produksjon, og lav andel av global produksjon. De øvrige nordiske landene har betydelig mer aktivitet innen disse teknologiområdene når det gjelder innvilgede EU-midler.

Avanserte halvlederteknologier var blant teknologiområdene hvor det ble rapportert om lav aktivitet i spørreundersøkelsen. For UH-sektoren ble det oppgitt tredje lavest aktivitet på dette teknologiområdet og det var det laveste for instituttsektoren. Det er særlig innen *høyfrekvente databrikker* og *utstyr for produksjon av halvledere på svært avanserte node-størrelser* at aktiviteten oppgis som lav. EVALMIT viste som tidligere beskrevet et variert bilde når det gjelder *avanserte halvledere*, med noen miljøer og underkategorier med sterk ekspertise. Samtidig ble det påpekt at samarbeid med nasjonale industrier innen dette teknologiområdet er noe begrenset da det ikke finnes noen stor mikro-elektronisk industri eller utstyrsprodusent.

Når det gjelder *avanserte sensorteknologier* ble det oppgitt høy aktivitet på én underkategori (elektro-optisk, radar, kjemisk, biologisk, stråling og distribuert sensorer) og lav aktivitet på andre

underkategorier (*magnetometre, magnetiske gradiometre, undervanns elektriske felt sensorer og gravimeter og gradiometre*). Som teknologiområde var dette det nest største området for instituttsektoren når det gjelder aktivitet, men det fjerde laveste for UH-sektoren. EVALMIT påpekte at «datavitenskap-komponenten» kunne vært sterkere i Norge, og det anbefales å igangsette synergiprosjekter hvor dataspesialister og domeneeksperter samarbeider.

Den svake norske posisjonen innen kvantevitenskap og -teknologi ble også fremhevet i fagevalueringen EVALNAT. Den nasjonale satsingen på kvanteteknologi og det nordiske samarbeidet som er beskrevet tidligere, vil kunne endre dette bildet i årene som kommer.

En underkategori som ble fremhevet som relativt svakt i EVALMIT var *6G-kommunikasjonssystemer* (under *avansert samband*). Det ble påpekt at Norge historisk sett har vært sterk innen trådløs kommunikasjon, men mangler nå ledende forskning på feltet. Vår undersøkelse viste at 12 miljøer hadde stor eller noe aktivitet på området, mens NIFUs publiseringsdata viser at det er svært lite publisering på sikker digital kommunikasjon i perioden 2015-2024. Avansert samband som teknologiområde skårer lavt når det gjelder mottatte EU-midler og i grad av norsk koordinering. De andre nordiske landene gjør det bedre enn Norge.

Det er tre underkategorier hvor det ikke er noen norske artikler i Web of Science i perioden i det hele tatt. De tre er *gendrivere* (under *bioteknologi*), *kjernekraftsfusjonsteknologier* (under *energiteknologier*) og *undervanns elektriske felt sensorer* (under *sensorteknologier*).

3.6.4. Hvem samarbeider Norge med på hvilke områder og på hvilke områder er Norge avhengig av samarbeid med hhv. allierte og ikke-allierte?

Norge samarbeider mest med allierte land på de fleste teknologiområdene. Det nordiske samarbeidet er relativt lavt, noe som indikerer at Norges i stor grad samarbeider med de store europeiske forskningsnasjonene, i tillegg til USA. Samarbeid med identifiserte trusselaktører, og da særlig Kina, er av betydelig størrelse særlig på *kunstig intelligens* og *energiteknologier*. Dette samarbeidet har økt samtidig som norsk og internasjonal forskning på disse feltene generelt har økt i omfang. NIFUs analyse indikerer også at Norge over tid har samarbeidet med færre land på *kunstig intelligens*, og i stigende grad konsentrert samarbeidet om Kina. Dette kan være et tegn på en viss avhengighet av Kina innenfor nettopp dette teknologiområdet.

Videre er Kina også største samarbeidsland i 2024 på *robotikk og autonome systemer*, blant de ti viktigste samarbeidslandene på alle områder unntatt to (*romfart og fremdriftsteknologier* og *undervannsteknologier*) og blant de fem viktigste på fem av områdene. Verken Iran, Russland eller Nord-Korea figurerer på listene over Norges ti viktigste samarbeidsland på noen av teknologiområdene.

Inntrykket av at Kina er blant Norges viktigste samarbeidsland underbygges av siteringsanalysen. *Avansert samband, kunstig intelligens og robotikk og autonome systemer* skiller seg ut som områder der samarbeidet med Kina er ekstra sterkt målt i siteringsgjennomslag. På disse områdene sampubliserer norske og kinesiske forskere omfattende og med høy kvalitet (målt i andel artikler som er blant de 10% og 1% mest siterte i verden ila. et år).

Når det gjelder underkategoriene, er også bildet at Norge samarbeider mest med allierte, men at Norge har utstrakt samarbeid særlig med Kina. USA, Storbritannia og Tyskland, men også Kina og

India, er viktige samarbeidspartnere på underkategorier innenfor kunstig intelligens og energiteknologier. Det er noe variasjon innenfor de ulike underkategoriene. Norges samarbeid med Kina på kunstig intelligens er for eksempel konsentrert om *maskin- og dyplæring og sky- og kantdata*, mens Norges samarbeid med India på kunstig intelligens er konsentrert om *datamaskinsyn og språkbehandling*. På *energiteknologier* er Norges samarbeid med Kina og India konsentrert om underkategoriene *smarte nett og energilagring*, samt *nullutslipp*.

Norges samarbeid med Russland er ganske ubetydelig og spredt. Iran har et mer betydelig samarbeid med Norge, både i den forstand at de bidrar i flere artikler, og at artiklene de bidrar i er konsentrert på færre områder. Mest omfattende er norsk samarbeid med Iran på *kunstig intelligens* innenfor underkategorien *maskin- og dyplæring*. Deretter følger energiteknologier med underkategorien *smarte nett og energilagring*, *avanserte halvledere* med *fotonikk* og *avanserte materialer* med *additiv produksjon*. Men det er viktig å påpeke at volumet på samarbeidet med Iran er svært beskjedent.

Antall forfatterandeler iranske forskere har i artikler der Norge også er med som samarbeidspartner er svært lave, noe som indikerer at artikkelsamarbeid som omfatter både norske og iranske forskere ofte involverer flere forskere fra forskjellige land. Dette reflekteres også i siteringsanalysen, hvor Iran ikke figurerer på noen av listene over land Norge publiserer mest med når det gjelder høyt siterte artikler.

3.7. Deltakelse i European Defence Fund (EDF)

NIFU-rapporten omtaler i liten grad norsk deltakelse i EDF, ettersom data om EDF-prosjekter generelt er lite tilgjengelige. Derfor er det lagt til en egen omtale i delleveranse 3 av norsk deltakelse basert på rapporter fra Fondation pour la recherche stratégique (FRS).[13] Oversikten viser at Norge gjør det bra i EDF, og er den 9. mest aktive nasjonen, basert på antall deltakelser. Norge har høy deltakelse av forskningsinstitutter (31 prosent av antallet norske deltakelser). FFI er det mest aktive norske forskningsinstituttet i EDF, målt i antall deltakelser og mottatt støtte. SINTEF har også en betydelig deltakelse i EDF. Ut over disser er IFE det eneste øvrige norske forskningsinstituttet med aktivitet i EDF. Universitetene i Norge har lav deltakelse (4 prosent av antallet norske deltakelser). NTNU er det eneste universitetet som har deltatt, men gjør det til gjengjeld svært godt med fire prosjektdeltakelser og en høy rangering blant de europeiske universitetene. Norge har 39 prosent av antall deltakelser fra industrien, mens små og mellomstore bedrifter (SME) utgjør 26 prosent. Industrideltakelsen er relativt stor for en liten nasjon, mens SME-andelen er litt mindre enn man kunne forvente av en nasjon på Norges størrelse. Kongsberg i en klasse for seg, og er blant topp-25 av industriaktørene i EDF.

Gjennomgangen av norske prosjektdeltakelser viser at disse er jevnt fordelt på ulike sensitive teknologiområder, med høyest deltakelse innen avansert samband, navigasjon og digitale teknologier. Dette reflekterer både EDFs prioriteringer og norsk industris kompetanse, særlig innen militære kampsystemer og cybersikkerhet. Samtidig påpekes det at verken FFI eller SINTEF har deltatt i EDF-prosjekter innenfor robotikk og autonome systemer, til tross for betydelig nasjonal aktivitet på disse feltene.

Det bemerkes at det er liten eller ingen norsk deltakelse i prosjekter knyttet til kvanteteknologi og bioteknologi. Dette kan skyldes både lavere nasjonal aktivitet og begrensede utlysninger i EDF

[13] Fondation pour la Recherche Stratégique :: FRS

innenfor disse teknologiene. Samlet sett tyder funnene på at norsk forsvarsindustri og forskningsmiljø har bred faglig dekning på de fleste sensitive teknologiområder, men antyder også at det fortsatt finnes kunnskapshull, for eksempel innenfor bio- og kvanteteknologi.

3.8. Særskilt om rekruttering

Rekruttering er også et sentralt tema knyttet til økonomisk sikkerhet og kompetansebehov, og det er en spenning mellom samfunnets behov for kunnskap og hensynet til nasjonal sikkerhet. I spørreundersøkelsen ble virksomhetene bedt om å vurdere rekrutteringssituasjonen innenfor de sensitive teknologiområdene. Gjennom undersøkelsen og de påfølgende dialogmøtene er inntrykket at det for mange teknologiområder er stadig vanskeligere å rekruttere faglige ansatte og doktorgradsstudenter. Det er en reell fare for at Norge går glipp av talenter, ettersom kompetansen innen mange teknologiområder ofte finnes hos forskere eller studenter fra land utenfor NATO eller Europa. Det gjelder særlig teknologiområder som er underlagt sikkerhetsmessige restriksjoner og som berøres av eksportkontroll. Rekruttering av forskere og studenter fra såkalte høyrisikoland er utfordrende med tanke på sikkerhetsklarering, men også for prosjektsamarbeid med institutter eller land med strengere føringer.

Den samlede produksjonen av doktorgrader innenfor matematikk, naturfag og teknologi (MNT) i Norge økt betydelig de siste 15 årene. I løpet av denne perioden ble det levert totalt 8 147 doktorgradsavhandlinger innen MNT-fagene, med et årlig gjennomsnitt på 543 avhandlinger. Siden 2010 har det vært en økning på hele 67 prosent i antall innleverte MNT-doktorgrader. Basert på titler og tilgjengelige sammendrag av avleverte doktorgradsavhandlinger har prosjektet forsøkt å identifisere avhandlinger innenfor sensitive teknologiområder. Tallene viser at det har vært en særlig sterk vekst i antall doktorgrader innenfor sensitive teknologiområder de to siste årene. Teknologier innenfor kunstig intelligens står for en stor andel av denne veksten. Det er noe usikkerhet knyttet til kartleggingen. Det skyldes at de fleste MNT-avhandlingene dekker eller berører flere teknologiområder. Prosjektet har kun indeksert hver avhandling med ett teknologiområde i denne kartleggingen. I tillegg er det usikkert om prosjektet har funnet frem den riktige kategoriseringen basert på tittelen alene, og i noen tilfeller sammendraget fra avhandlingen. Prosjektet vil anbefale at fremtidige MNT-avhandlinger bør merkes (av kandidaten/forfatteren) med 1-3 teknologiområder som oppgaven omhandler – på lik linje med dagens praksis for bruk av emneord[14] slik at det blir enklere å følge med på utviklingen fremover.

[14] I dag er det ikke et nasjonalt, lovpålagt krav, men emneord kreves normalt av universitetene i Norge for doktorgradsavhandlinger innen MNT-fag.

4. Risikovurdering av sensitive teknologier

KVAST-prosjektet var bedt om å analysere konkrete teknologiområder/ev. underkategorier både med tanke på risikonivå og hvilken type risiko som er forbundet med hvert enkelt område. Analysen skulle blant annet baseres på funn fra delleveranse 2 og delleveranse 3. Oppdraget presiserte at det var ønskelig å dele resultatet av disse analysene bredest mulig.

Risikovurderingen er i hovedsak utført av Nasjonal sikkerhetsmyndighet (NSM), med bidrag fra Forsvarets forskningsinstitutt (FFI) og Norges forskningsråd. Analysen bygger på et sammensatt grunnlag: åpne trussel- og risikovurderinger fra norske myndigheter (PST, NSM og Etterretningstjenesten) for å beskrive trusselaktørers kapasitet, modus og intensjon; KVAST-prosjektets egne delleveranser for metode, datagrunnlag og sektorspesifikke funn; samt relevante lov- og regelverk, herunder eksportkontroll (DEKSA-listene) og annet nasjonalt og internasjonalt regelverk som rammer teknologibruk, samarbeid og kunnskapsoverføring. I tillegg er NIFUs rapport (2025:17) brukt for å belyse forskningstrender, samarbeid, mobilitet og kompetansesituasjon på tvers av teknologiområder. Svarene fra forskningsaktørene på spørsmålene i spørreundersøkelsen om teknologienes grad av sensitivitet og flerbrukspotensial har i noen grad blitt brukt som grunnlag. Dialogmøtene med forskningsaktørene har ikke blitt brukt som input til risikovurdering, da de har foregått parallelt.

4.1. Metode for risikovurdering

Delleveranse 4 innleder med definisjoner av risiko og risikovurdering. For sensitive teknologier er risiko definert som samspillet mellom teknologiens verdi, teknologiens sårbarheter og det eksterne trusselbildet.

- **Teknologiens verdi** beskriver hvor strategisk viktig teknologien er for nasjonale sikkerhetsinteresser og grunnleggende nasjonale funksjoner. Høy verdi innebærer at misbruk vil ha større konsekvenser for nasjonale sikkerhetsinteresser.
- **Teknologiens sårbarheter** beskriver de interne svakhetene ved teknologien som gir muligheter for skade eller misbruk. Dette omfatter både tekniske, operasjonelle eller regulatoriske svakheter.
- **Det eksterne trusselbildet** beskriver de eksterne faktorene som føre til misbruk, både knyttet til hvilke aktører som kan ha motiv og evne til å skaffe seg kontroll over teknologien, og hvordan geopolitiske forhold påvirker sannsynligheten for innhenting, påvirkning eller sabotasje.

Metodikken måler risiko med seks kriterier:

1. Eksponering for utenlandske aktører
2. Regulatorisk kontroll og etterlevelse
3. Potensiell militær eller strategisk utnyttelse
4. Konsekvenser for kritisk infrastruktur
5. Økonomisk sikkerhet
6. Respekt for menneskeverd

Kriteriene måles på en skala fra **lav til svært høy**. Deretter gjøres en totalvurdering av risiko, basert på utfallet av vurderingene for hvert kriterium. Resultatene fremstilles grafisk i slutten av

risikovurderingen for hver teknologi. Metoden er basert på en kvalitativ tilnærming til risikoanalyse der sannsynligheter og konsekvenser blir bestemt rent kvalitativt, og der det benyttes ord for å beskrive frekvens og alvorlighetsgrad.

Kriteriene som brukes i risikovurderingen tar høyde for både interne og eksterne faktorer og dette gjør at den samlede analysen på et teknologiområde er relativt kompleks. For eksempel gir en høy grad av eksponering for utenlandske aktører eller et stort potensial for militær bruk høy risiko i vurderingen av en teknologi, samtidig som lav nasjonal aktivitet på et teknologiområde kan innebære en sårbarhet i seg selv og dermed risiko knyttet til mangel på strategisk viktig kunnskap og kompetanse. Forslaget til oversikt over sensitive teknologier for norske forhold omfatter 48 teknologier, fordelt på 11 hovedkategorier. Ut ifra tilgjengelig tid og ressurser var det ikke mulig å gjennomføre risikovurderinger for alle teknologiene. Prosjektet valgte derfor minst én teknologi fra hver av de 11 hovedkategoriene i oversikten for å sikre tilstrekkelig bredde i vurderingene. Videre så prosjektet hen til svar fra spørreundersøkelsen om teknologier hvor det var rapportert stor forskningsaktivitet. I tillegg så vi på teknologier hvor institusjonene selv vurderte høy grad av sensitivitet eller høyt potensiale for militær anvendelse. På denne bakgrunn, og ut fra kapasitetshensyn, ble 14 teknologier valgt ut til risikovurdering.

4.2. Drøfting av risikovurderingen

Risikovurderingene av de 14 teknologiene viser at sensitive teknologier favner både komplekse og sammensatte risikoer, ikke bare knyttet til mulig misbruk, men også til avhengigheter og kunnskapsbehov. Hovedbildet er at de fleste teknologiene havner i kategoriene «høy» og «svært høy» risiko, både når det gjelder risikovurderingen for hvert av de seks kriteriene, og når det gjelder samlet vurdering for den enkelte teknologi. Dette er ikke et overraskende resultat, ettersom utvalget er fra en oversikt over teknologier som i utgangspunktet er definert som sensitive. Vi kan derfor anta at de øvrige teknologiene i oversikten også ville blitt vurdert å ha relativt høy risiko.

Risiko for en gitt teknologi vil variere på bruksområde, verdikjede, regulatorisk kontroll, samarbeidspartnere og trusselutvikling. Dagens situasjonsbilde, med rask teknologisk utvikling, geopolitisk usikkerhet og fragmentert regulatorisk kontroll, gjør risikoen både dynamisk og vanskelig å fastsette presist. Vurderingene er øyeblikksbilder, og samlet vurdering av en bredere teknologi kan fange opp ytterpunkter, mens flere teknologier bærer med seg latente risikoer som først materialiseres under visse forutsetninger.

For enkelte kriterier er vurderingen gjennomgående at det er høy risiko for alle teknologiene som ble risikovurdert. Dette gjelder særlig for «potensiell militær eller strategisk utnyttelse». Kriteriet fanger opp potensialet for militær og strategisk bruk i en tid der veldig mange teknologier er flerbruks-orienterte, og resultatet uttrykker et øvre risikonivå innenfor kategoriene. Dermed blir nyansene i underliggende delteknologier ikke fullt ut synlige (eksempelvis innenfor fotonikk, som både omfatter rettede energivåpen og lasere til bruk i medisinsk behandling). I praksis vil storparten av de mest sensitive delene av teknologiområdene allerede være underlagt nasjonale graderings- og kontrollregimer. Metoden synliggjør toppnivået av risiko i brede kategorier, men erstatter ikke mer finmasket vurdering.

Risikovurderingene bør dermed ikke oppfattes som endelige «fasitsvar», men som et verktøy for bevisstgjøring, prioritering og løpende revurdering på ulike nivåer og på tvers av sektorer – med

utgangspunkt i faktiske trusselbilder, nasjonale kompetansebehov og vår evne til å balansere hensynet til sikkerhet og kunnskapsutvikling. Metodikken som er utarbeidet i prosjektet gir et strukturert rammeverk for slike vurderinger, men det forutsetter fortsatt uavhengig kvalitativ analyse og dialog mellom berørte aktører og miljøer.

Risikohåndtering av sensitive teknologiområder handler om å finne balansen mellom å beskytte norske sikkerhetsinteresser og å fremme nødvendig teknologiutvikling og internasjonalt samarbeid. Behovet for kontinuerlig kompetansebygging, nasjonal kontroll og oppdatert styring vil bare bli viktigere i tiden fremover – og risikovurderinger må fortsatt være sentrale bidrag til dette arbeidet.

Risikovurderingen er ment å bidra til bevisstgjøring om hvorfor teknologiene vurderes som sensitive og på hvilke måter de kan være sårbare. Det at mange av teknologiene kommer ut med en samlet vurdering som «høy» eller «svært høy», betyr ikke nødvendigvis at det er ønskelig å begrense samarbeid om disse. På noen områder kan samarbeid, spesielt med allierte, være avgjørende for å sikre posisjon og kompetanse, og på andre områder har vi mer å tjene på samarbeidet enn vi har å tape. Samtidig skiller metoden tydelig mellom samarbeid med allierte og samarbeid med ikke-allierte: både risiko for eksponering og risiko knyttet til økonomisk sikkerhet er tar inn over seg eksponering for- eller avhengigheter til ikke-allierte, mens det vanligvis ikke knyttes forhøyet risiko til samarbeid med allierte. Risikovurderingen har også en viktig strategisk dimensjon, ettersom risiko knyttet til økonomisk sikkerhet er basert på at det er grunnleggende viktig for norske sikkerhetsinteresser å tilegne seg kunnskap og kompetanse gjennom samarbeid. Hvor nyttig og risikofylt samarbeid er, avhenger av Norges posisjon på området: er vi svake på et område, kan vi ha mer å tjene på å samarbeide enn vi har å tape. Motsetningsvis, dersom Norge er ledende på et område, kan samarbeid koste mer enn det smaker. Vurderingene er dynamiske, og vil til enhver tid avhenge av faktorer som sikkerhetsbildet og nasjonal posisjon, og nasjonale og internasjonale satsinger og nyvinninger. I tilfeller der blant annet samarbeid med ikke-allierte vurderes som nødvendig, tross for en forhøyet risiko, er det viktig å være bevisst risikodimensjonen.

Dette er en viktig påminnelse om at målsetningen bak KVAST-prosjektet ikke er å begrense, men å legge til rette for internasjonalt samarbeid, også når det er identifisert risiko. Spenningen mellom å beskytte og fremme er noe som ulike aktører innenfor forskningssystemet må forholde seg til. Metoden som er utarbeidet i prosjektet kan være et bidrag til å øke denne bevisstheten og en hjelp til å navigere i dette landskapet.

5. Oppsummering og veien videre

5.1. Dialog med FoU-aktører og departementer

Gjennom arbeidet med KVAST har prosjektgruppen hatt stor nytte av dialog med de utførende virksomhetene, med departementene og andre aktører. KVAST er et nybrottsarbeid som må avstemmes med forventinger og behov hos aktørene som skal bruke kunnskapsgrunnlaget i sitt videre arbeid med FoU og nasjonal sikkerhet.

De følgende avsnittene gir en oppsummering av hovedpunktene fra dialogen med aktørene, med vekt på erfaringer, reaksjoner og avveininger som blir viktige for det videre arbeidet med å utvikle en helhetlig og langsiktig plan for videre utvikling og oppdatering av kunnskapsgrunnlaget etablert i KVAST (se 5.2 nedenfor).

5.1.1. Institusjonenes tilbakemeldinger på spørreundersøkelsen

Dialogmøtene som ble gjennomført i forlengelse av spørreundersøkelsen (se kap. 3) har bidratt til enda bedre involvering av nøkkelaktørene og muligheten til å komme med synspunkter som ikke er lett å fange opp i et spørreskjema. I tillegg til samtaler med aktører i UH- og instituttsektor, gjennomførte prosjektgruppen et dialogmøte med Kongsberg Gruppen, ettersom få av nøkkelaktørene innen industrien besvarte spørreundersøkelsen.

Institusjonenes erfaringer med spørreundersøkelsen og tilbakemeldingene til prosjektet er en kombinasjon av positive holdninger til initiativet og faglige og praktiske utfordringer i besvarelsesprosessen.

Svært mange av aktørene som prosjektet hadde dialog med oppga at arbeidet med å fylle ut spørreskjemaet om sensitive teknologier hadde vært nyttig internt. I mange tilfeller førte det til diskusjoner om aktivitetsnivå, vurdering av sensitivitet og flerbruk og rekrutteringssituasjonen. Dette gjaldt også for virksomheter som har et høyt bevissthetsnivå rundt forskningssikkerhet og som oppga at selve prosessen ga økt modenhet og forståelse for sikkerhetsrisiko.

Samtidig har flere erfart at spørsmål knyttet til definisjoner av sensitivitet, omfang av aktivitetsnivå og grenseoppganger for flerbruksteknologier, har vært vanskelige å forstå og operasjonalisere. Noen av utfordringene som har blitt påpekt er:

- Begreper som «sensitiv teknologi», «militær bruk» og «stor aktivitet» samsvarer ikke alltid med institusjonenes interne kategorier og oppleves som utydelige, særlig på grunn av variasjon mellom fagmiljøer.
- Det etterlyses mer entydige definisjoner og tydeligere retningslinjer for begrepene "strategisk", "kritisk" og "sensitiv" teknologi.
- Innsamling og kvalitetssikring av svar har hovedsakelig vært sentralt koordinert av nøkkelpersoner, ofte konsolidert på ledelsesnivå. Det har gjort at institusjonene i noen tilfeller valgte den strengeste vurdering av risiko der hvor miljøer internt har svart ulikt.
- Det har vært en utfordring å sikre at besvarelsen dekker hele bredden av forskningsaktiviteten på de aktuelle teknologiområdene. Flere påpeker at svarene ofte kun reflekterer deler av virksomheten.
- Mange teknologikategorier og spørsmål i undersøkelsen opplevdes som generelle eller vage, noe som gjør det vanskelig å plassere egen aktivitet i kategoriene.

- Kompleksiteten og overlappet innen forskningsporteføljen gjør det utfordrende å gi presise svar, og det er behov for mer presise begreper og bedre verktøy.
- Institusjonene ønsker at fremtidige rammeverk tar hensyn til faglig kompleksitet og kontekst, og legger til rette for dialogbaserte løsninger.

Reaksjoner fra institusjonene på undersøkelsen peker på behovet for presise, relevante og kontekstilpassede spørsmål ved kartlegging av forskningssikkerhet og sensitive teknologier. Uklare eller generelle spørsmål gir liten verdi og kan føre til misforståelser i arbeidet med å besvare undersøkelsen. Det er viktig å balansere detaljeringsgrad med oversikt, samt inkludere fagevalueringer for bredere forståelse. Samtidig bør metodikken være fleksibel og gi rom for kvalitative utdypninger, spesielt i dynamiske og tverrfaglige miljøer. Kartleggingen bør være dialogbasert, med støtteverktøy og oppdaterte prosesser som er tilpasset institusjonenes organisering og arbeidsform.

Andre temaer som ble tatt opp i samtalene og som kan følges opp i senere arbeid var:

- Institusjonenes strategiske vurderinger av sensitiv forskning og teknologiutvikling.
- Identifisering av konkrete risikoområder og behov for ytterligere kompetansebygging.
- Erfaringer knyttet til internasjonalt samarbeid - herunder eventuelle dilemmaer og utfordringer.
- Innspill til hvordan nasjonale myndigheter og relevante aktører kan tilrettelegge for bedre informasjonsflyt, støtte og avklaring for aktørene på tvers av sektorer.
- Utfordringer knyttet til rekruttering, og rekruttering fra såkalte høyrisikoland og behovet for styrking av insentiver/langsiktighet for nasjonal talentrekruttering til forskning på sensitive og strategisk viktige teknologiområder.
- Kobling mellom KVAST-prosjektet og institusjonenes arbeid med verdivurderinger.

5.1.2. Dialog med departementene

KVAST-prosjektet har høsten 2025 også gjennomført dialogmøter med flere departementer som har relevant sektoransvar, herunder Justis- og beredskapsdepartementet, Kunnskapsdepartementet, Forsvarsdepartementet, Nærings- og fiskeridepartementet og Helse- og omsorgsdepartementet. Det skal gjennomføres dialogmøter med flere departementer tidlig i 2026.

Departementene gir uttrykk for at KVAST-prosjektet er nyttig for deres arbeid på flere områder knyttet til nasjonal sikkerhet, økonomisk sikkerhet og forskningssikkerhet. Behovene knytter seg blant annet knyttet til praktisk veiledning, situasjonsforståelse og ressurser for risikovurderinger innenfor de ulike sektorene, håndtering av internasjonalt samarbeid, samordning av arbeidet med nasjonal sikkerhet og arbeidet med grunnleggende nasjonale funksjoner, arbeid med nasjonal satsing på kvanteteknologi og sektorvise prioriteringer, kompetanseutvikling og aktørforståelse.

5.2. Anbefalinger for videre arbeid med kunnskapsgrunnlaget

Med KVAST-prosjektet foreligger det for første gang en samlet norsk oversikt over sensitive teknologier. En rekke av våre nærmeste samarbeidsland har allerede slike oversikter, og det er viktig at også Norge etablerer en felles oversikt tilpasset norske forhold og etter modell fra de internasjonale oversiktene. Dette gir et felles referansegrunnlag som kan benyttes på tvers av sektorer i politikkutforming, forvaltning, forskning og næringsvirksomhet.

Kartleggingen av aktivitet og omfanget av samarbeid med allierte og ikke-allierte samarbeidsland innenfor de sensitive teknologiene vil danne et viktig grunnlag for videre arbeid med forskningssikkerhet og et underlag for strategiske diskusjoner om kapasitet og kompetansebehov på områder som blir viktige for Norge fremover.

Med risikovurderingen i prosjektet er det utviklet og anvendt en skreddersydd, sektorovergripende metodikk for risikovurdering av sensitive teknologier tilpasset dagens situasjonsbilde og behovene knyttet til nasjonal sikkerhet. Dette rammeverket kan brukes til å øke bevissthet i forskningsmiljøene om sensitive teknologier og være til hjelp for institusjonenes eget arbeid med å gjøre konkrete vurderinger knyttet til de enkelte prosjekter og samarbeid, men også bidra til vurderinger på myndighetsnivå gjennom å avdekke risiko knyttet til manglende kompetanse innenfor viktige teknologier.

En konkret anvendelse av teknologioversikten vil være i forbindelse med risikovurdering av prosjekter som finansieres av Forskningsrådet, hvor prosjektansvarlig organisasjon vil bli bedt om å oppgi hvilke vurderinger og tiltak som er gjort for å ivareta forskningssikkerheten for prosjekter som er innenfor de definerte sensitive teknologiene.

Kunnskapsgrunnlaget vil også være nyttig for videreutviklingen av retningslinjer for ansvarlig internasjonalt samarbeid og gir et supplement til dagens retningslinjer, som har en generell innretning. KVAST-prosjektet og videre arbeid med kunnskapsgrunnlag om andre sensitive fagområder blir nyttig for å videreutvikle råd og veiledning om ansvarlig praksis innenfor ulike fagområder i internasjonale forsknings- og utdanningssamarbeid.

5.2.1. Oppdateringer og videreutvikling av kunnskapsgrunnlaget

KVAST-prosjektet er et første skritt i et kontinuerlig arbeid. Både teknologiene, forskningsfronten og den sikkerhetspolitiske situasjonen internasjonalt er i stadig endring. Dette krever at kunnskapsgrunnlaget og risikovurderingene oppdateres jevnlig.

En del av KVAST-prosjektet har vært å foreslå mulig system for håndtering av relevant kunnskap etter at oppdraget er fullført. Dette innebærer å vurdere hvilke resultater/produkter fra oppdraget som vil kreve kontinuerlig oppdateringer blant annet som følge av teknologiutviklingen og hvor forskningsfronten til enhver tid befinner seg, og foreslå et opplegg for løpende drift og oppdatering av kunnskapsgrunnlaget. De tre departementene (KD, FD, JD) og prosjektgruppen har gjennom dialog underveis i prosjektet sett at det er behov for en videre prosjektfase etter at det første KVAST-prosjektet avsluttes i utgangen av 2025. Denne neste fasen av prosjektet skal gjennomføres i første halvdel av 2026, og formålet med den neste fasen vil være å utvikle en helhetlig og langsiktig plan for videre drift av kunnskapsgrunnlaget fra og med 2027.

Den neste fasen skal brukes til å videreutvikle både metodikk for utvikling og oppdatering av kunnskapsgrunnlaget og gi anbefalinger om hvordan KVAST kan bli brukt som en felles ressurs, både av institusjoner og myndighetsaktører fremover. Det skal også legges vekt på for hvordan KVAST kan sees i sammenheng med andre prosesser knyttet til FoU og nasjonal sikkerhet, herunder (listen er ikke uttømmende).

- Oppdrag gitt til Forskningsrådet og Forsvarets forskningsinstitutt om felles datasystem for FoU-prosjekter relatert til forsvarssektoren.

- Satsing på FoU gjennom Forskningsrådet for økt forsvarsevne sikkerhet og beredskap er vedtatt og aktualiserer en rekke problemstillinger knyttet til flerbruksforskning
- Etablering av et porteføljestyre for forsvarsevne, sikkerhet og beredskap som skal følge opp satsingen og bidra til økte synergier mellom sivil og militær forskning.
- Etablering av grunnleggende nasjonal funksjon for FoU.
- Oppdatering og videreutvikling av retningslinjer for Ansvarlig internasjonalt kunnskapssamarbeid (Forskningsrådet og HK-dir).
- Oppdrag om å vurdere andre fagområder med tanke på sensitivitet og risiko (Forskningsrådet og HK-dir).
- Videre arbeid med forskningssikkerhet på myndighetsnivå, på finansiør-nivå og ved de utførende institusjonene, i lys av internasjonale prosesser, herunder EU-kommisjonens arbeid og tiltak i forlengelse av EUs rådsanbefalinger om forskningssikkerhet.
- EUs planlagte konkurranseevnefond og det neste rammeprogrammet for forskning og innovasjon, hvor det legges opp til en betydelig satsing på forsvar, sikkerhet og beredskap og hvor det forventes at styrking av Unionens økonomiske sikkerhet blir tillagt stor vekt i det kommende langtidsbudsjettet.

For oppdateringer av kunnskapsgrunnlaget bør det legges vekt på regelmessighet og forutsigbarhet, for eksempel gjennom at det etableres en rutine for jevnlig revidering av den norske teknologioversikten. Tilsvarende bør det gjøres regelmessige statusoppdateringer av Norges posisjon innenfor de sensitive teknologiene. Her blir det viktig å ta hensyn til institusjonenes reaksjoner og erfaringer med spørreundersøkelsen (jf. over) og løpende vurderinger av institusjonenes arbeid med risikovurdering og nytte og bruk av metodikken for risikovurdering fra prosjektets første fase.

Teknologiområdene som er utgangspunkt for KVAST-prosjektet, dekker svært bredt. En tilbakemelding fra institusjonene er at selv underkategoriene i praksis er brede fagfelt med stor intern variasjon, og at det derfor er krevende å svare presist om teknologienes sensitivitet. Samtidig ville en mer detaljert inndeling av teknologier føre til et mer omfattende kartleggings- og vurderingsarbeid. Det videre arbeidet vil innebære vurderinger om hva som er et hensiktsmessig detaljnivå for videre nasjonale kartlegginger og risikovurderinger, og hva som er en god ansvarsdeling mellom institusjonenes eget vurderingsarbeid og nasjonale kartlegginger.

I arbeidet med risikovurderingen ble det vurdert flere andre kriterier utover dem som ble tatt med i modellen, blant annet teknologiens modenhetsnivå målt på TRL-skalaen, teknologiens muliggjørende potensiale, og sårbarhet for cyberangrep. Disse kriteriene ble av ulike grunner ikke benyttet i dette prosjektet, som forklart idelleveranse 4. I videre arbeid med kunnskapsgrunnlaget kan det være relevant å også se på andre kriterier, i tillegg til detaljeringsnivå for teknologiene

En av intensjonene med oppdraget har vært å belyse områder hvor Norge mangler nasjonal kunnskap som vi bør ha. Delleveranse 3, (se kapittel 3 over) gir en bred kartlegging og et utgangspunkt for en slik vurdering, og delleveranse 4 (risikovurdering) peker på sårbarheter knyttet til mangel på strategisk viktig kunnskap innenfor enkelte teknologier. Avgrensninger av KVAST-prosjektet når det gjelder kildetilfang og innretning, som nevnt over, har gjort at spørsmålet om strategisk svake områder kun delvis er belyst. Neste fase av KVAST bør se hen til begrensinger i nåværende prosjekt og vurdere om kunnskapsgrunnlaget bør utvides, også metodisk, for å omfatte andre deler av aktiviteten knyttet til sensitive teknologier. Dette gjelder for eksempel aktivitet i

næringslivet som ikke blir dokumentert gjennom vitenskapelige publikasjoner. Det gjelder også FoU-aktivitet som er sikkerhetsgradert. For å møte behovet for felles kunnskapsgrunnlag på tvers av åpen og skjermet forskning bør den videre utviklingen av kunnskapsgrunnlaget sees i sammenheng med annen informasjon, herunder gjennom videre samarbeid mellom Forskningsrådet og FFI om felles datafangst for FoU med relevans for forsvarssektoren. Dette vil bidra til å gi et mer samordnet kunnskapsgrunnlag også når det gjelder kunnskap- og kompetansebehov på strategisk viktige områder.

I videre arbeid bør det også gjøres vurderinger av hvordan sensitive teknologier kan monitoreres og om tilgjengelig statistikk og system for prosjektmerking gir tilstrekkelig informasjon. Aktører som bør involveres i vurderingen, er Forskningsrådet og SSB. Det finnes også andre aktører, f.eks. i instituttsektoren, som kan bidra.

Det videre arbeidet med KVAST bør sees i nær sammenheng med et utvidet kunnskapsgrunnlag for andre fagområder hvor resultater fra FoU kan ha betydning for nasjonal sikkerhet. Dette gjelder eksempelvis innenfor helseforskning (helsedata og persondata), ulike deler av samfunnsvitenskapene, marin og maritim forskning eller forskning knyttet til nordområdene.

I det videre arbeidet med KVAST, eventuelt parallelt med dette arbeidet, bør det gjøres en helhetlig kartlegging av arbeidet med forskningssikkerhet i norsk FoU-sektor.

Det bør også vurderes å gjøre en mer helhetlig kartlegging av hvilke kompetanseprofiler og utdanningsløp næringslivet og forsvarsindustrien har behov for fremover.

5.2.2. Videre samarbeid, dialog og samspill med departement og FoU-institusjoner

En erfaring fra prosjektet er at det tverretatlige samarbeidet i KVAST-prosjektet mellom NSM, FFI og Forskningsrådet har stor verdi og har bidratt til å gi bredde til vurderingene i prosjektet. Gjennom prosjektet er det lagt et godt grunnlag for videre samarbeid mellom de tre etatene.

Arbeidet med å oppdatere og videreutvikle kunnskapsgrunnlaget og vurderinger av dets rolle og funksjon som felles ressurs bør skje i nært samspill og dialog med berørte departement, andre myndighetsaktører og de utførende virksomhetene.

Gjennom prosjektet har det vært jevnlig og god dialog med oppdragsgiverne, og basert på dette kan det være hensiktsmessig med utvidede dialogmøter og hyppigere kontakt også med andre departement som har sektoransvar knyttet til de aktuelle teknologiene.

I dialog med institusjonene har det kommet frem at det er et stort behov for dialog, felles refleksjon og tilpasninger i takt med både teknologiutvikling og endrede trusselbilder. Det bør vurderes å etablere mer faste møtearenaer hvor det legges til rette for erfaringsdeling og utveksling mellom institusjoner og myndigheter.