Porteføljestyret for forskningssystemet

Dato	**Sted**
26. mars	Digitalt på teams
10:00 – 15:00	

Sak PS-FS 16/25	Godkjenning av sakslisten	10:00 – 10:02
Sak PS-FS 17/25	Godkjent møteprotokoll fra porteføljestyremøte 1/25	10:02 – 10:05
Sak PS-FS 18/25	Habilitet	10:05 – 10:10
Sak PS-FS 19/25	Søknadsbehandling nasjonale forskerskoler [U.off. § 14]	10:10 – 11:00
	Pause	11:00 – 11:10
Sak PS-FS 20/25	INTPART: Deltagelse fra HK-dir	11:10 – 11:30
Sak PS-FS 21/25	Internasjonal stimuleringspott: ytterligere kriterier for bruk og bevilgning [U.off. § 14]	11:30 – 12:00
	Lunsj og pause	12:00 – 13:00
Sak PS-FS 22/25	Refleksjonsnotat 2025 [U.off. § 14]	13:00 – 13:30
Sak PS-FS 23/25	Arbeidet med oppdatering av norsk veikart for infrastruktur og ny utlysning [U.off. § 14]	13:30 – 14:00
	Pause	14:00 – 14:15
Sak PS-FS 24/25	Forskningssikkerhet [U.off. § 14]	14:15 – 14:45
Sak PS-FS 25/25	Orienteringer	14:45 – 14:50
Sak PS-FS 26/25	Evaluering av møtet	14:50 – 14:55

Sak PS-FS 27/24	Godkjenning av møteprotokoll	14:55 – 15:00

Saksfremlegg
Porteføljestyremøte 2/25

Sak PS-Forskningssystemet
Spørsmål om habilitet

Til	**Ansvarlig Direktør**	**Saksbehandler**	**Vedlegg**
Porteføljestyret for forskningssystemet	Johannes W. Løvhaug	Lillian M. Baltzrud	1. Habilitet og tillit i Forskningsrådet

Fra

Områdedirektør

Benedicte Løseth

BESLUTNINGSSAK

Forslag til vedtak

I dette møtet skal porteføljestyret beslutte tildeling og avslag til søknader til nasjonale forskerskoler, PS-FS sak 19/25.

Forskningsrådets administrasjon har foretatt en habilitetsvurdering, og følgende porteføljestyremedlemmer er inhabile og fratrer derfor når sak 19/25 diskuteres i porteføljestyretstyret:

- Tanja Storsul, som er inhabil for behandling av søknadene 356538, 356534, 356488, 356464, 356560, 356599, 356490, 356427, 356390, 356423, 356569
- Tove Nilsen Klæboe, som er inhabil for behandling av søknadene 356499, 356550, 356464, 356520, 356488
- Ågot Aakre, som er inhabil for behandling av søknadene 356560, 356390
- Dagfinn Myhre, som er inhabil for behandling av søknadene 356462, 356560, 356569
- Astri Dankertsen, som er inhabil for behandling av søknaden 356499
- Rune Dahl Fitjar, som er inhabil for behandling av søknadene 356477 og 356560

For å sikre at porteføljestyret er beslutningsdyktig i saken er professor Barabara van Loon, ved Institutt for klinisk og molekylær medisin ved NTNU, oppnevnt som settemedlem. Van Loon er medlem i Porteføljestyret for banebrytende forskning og er valgt ut fordi hun har kompetanse om saken. Habilitet er kartlagt i forkant av oppnevningen.

Siden porteføljestyreleder Tanja Storsul er inhabil i saken, er porteføljestyremedlem Sven Stafström oppnevnt som setteleder under behandling av saken.

Kort bakgrunn

I henhold til Forskningsrådets bestemmelser om habilitet og tillit skal porteføljestyrets medlemmer vurdere sin habilitet i alle beslutningssaker. Eventuell inhabilitet og håndteringen av denne skal protokollføres. Usikkerhet om inhabilitet skal diskuteres åpent i styremøtet og skal også protokollføres. Styremedlemmer som blir vurdert inhabile, skal forlate styremøtet under behandlingen av den aktuelle saken. Styret er beslutningsdyktig når minst halvparten av styremedlemmene er habile og deltar i beslutningen.

Hvorfor saken fremmes til dette møtet

Porteføljestyret skal avklare styremedlemmenes habilitet i beslutningssakene i møtet.

Hovedpunkter	I dette møtet skal porteføljestyret beslutte tildeling og avslag i til søknader om nasjonale forskerskoleprosjekter, PS-FS sak 19/25. Bare habile styremedlemmer kan delta i diskusjonen om endelig tildeling. Det vil si at alle som skal delta i søknadsbehandlingen må være habile til alle søknadene som skal behandles i møtet. I forkant av møtet er porteføljestyrets medlemmer forelagt liste over alle prosjektdeltagere i søknadene og bedt om å vurdere egen habilitet. Tilbakemeldingene fra porteføljestyrets medlemmer er deretter vurdert av Forskningsrådets administrasjon. Som følge av vurderingene er seks av porteføljestyrets medlemmer inhabile og kan ikke delta under behandlingen av saken. Administrasjonen har også kartlagt egen mulig inhabilitet i de nevnte sakene. Det er ikke avdekket forhold som fører til inhabilitet for administrasjonen. Når seks av porteføljestyret medlemmer er inhabile, står det igjen syv habile medlemmer som kan delta under saken. For å sikre at styret er vedtaksdyktige, også om et av medlemmene skulle melde forfall til møtet, er professor Barbara van Loon ved Institutt for klinisk og molekylær medisin ved NTNU oppnevnt som settemedlem i porteføljestyret under saken. Siden porteføljestyrets leder er inhabil og ikke kan delta under behandling av saken, er medlem i porteføljestyret, professor Sven Stafström, oppnevnt som setteleder. Ingen andre saker krever habilitetsavklaring i dette møte.
Forberedelse / prosess	Administrasjonen har utviklet saken.
Videre saksgang	Administrasjonen har oppnevnt et settemedlem og en setteleder under porteføljestyrets behandling av sak PS-FS 19/25.

Bestemmelser om habilitet og tillit i Norges forskningsråd – kortversjon

Forskningsrådet er omfattet av habilitetsbestemmelsene i Forvaltningslovens kapittel II "Om ugildhet". Bestemmelsene gjelder også eksterne enkeltpersoner som bidrar i Forskningsrådets saksbehandling, som fageksperter. Forskningsrådet har i tillegg vedtatt egne bestemmelser om habilitet og tillit. Disse er på noen punkter strengere enn lovens regler. De viktigste bestemmelsene for vurdering av habilitet er følgende:

Fra bestemmelsene:

2 Definisjoner

I disse bestemmelsene menes med:

Part – person som en avgjørelse retter seg mot eller som saken ellers direkte gjelder, jf. forvaltningslovens § 2 e). Som part regnes normalt også enkeltperson som er direkte identifisert i en søknad og som har en sentral rolle i prosjektet.

3 Habilitetskrav og avgjørelse av habilitetsspørsmålet

3.1 Automatisk inhabilitet

Ansatt, ekspert eller medlem av styrende og rådgivende organer i Forskningsrådet samt enhver annen som utfører tjeneste eller arbeid for Forskningsrådet, er i alle tilfelle inhabil til å tilrettelegge grunnlaget for en avgjørelse, eller treffe avgjørelse i en sak

a) når han eller hun selv er part i saken
b) når han eller hun er i slekt eller svogerskap med en part i opp- eller nedstigende linje eller i sidelinje så nært som søsken
c) når han eller hun er eller har vært gift eller partner med eller er forlovet med, eller er samboer med, eller er fosterfar, fostermor eller fosterbarn til en part.
d) når han eller hun er verge eller fullmektig for en part i saken eller har vært verge eller fullmektig for en part etter at saken begynte
e) når han eller hun leder eller har en ledende stilling i, eller er medlem av styringsorgan eller bedriftsforsamling for en offentlig eller privat virksomhet, som er part i saken
f) når han eller hun er, eller for mindre enn 3 år siden har vært, veileder for en part med sikte på doktorgrad

3.2 Inhabilitet etter skjønn

Ansatt, ekspert eller medlem av styrende og rådgivende organer i Forskningsrådet samt enhver annen som utfører tjeneste eller arbeid for Forskningsrådet, er inhabil til å tilrettelegge grunnlaget for en avgjørelse, eller treffe avgjørelse i en sak når det foreligger særegne forhold som er egnet til å svekke tilliten til hans eller hennes upartiskhet.

Ved vurderingen skal det blant annet legges vekt på om avgjørelsen i saken kan innebære særlig fordel, tap eller ulempe for ham eller henne selv eller noen som han eller hun har nær personlig tilknytning til. Det skal også legges vekt på om ugildhetsinnsigelse er reist av en part.

Kommentar til 3.2:
I skjønnsvurderingen skal en særlig vurdere og vektlegge følgende:

- personlig interesse for utfallet av saken
- nært faglig samarbeid, herunder vurdere betydningen av samforfatterskap og veiledning
- nært vennskap
- personlig eller faglig motsetningsforhold
- personlig eierskap – aksjer e.l.

Fra veiledningen:

3. Generelt om habilitetsvurdering

Ved vurdering av habilitetsforhold vil det ofte være behov for å bruke skjønn. Ved vurdering av habilitet må følgende overordnede spørsmål stilles:

- Er det noen forhold i saken som kan svekke, eller kan antas å svekke, vedkommendes profesjonelle dømmekraft?
- Er det noen forhold i saken som kan svekke, eller kan antas å svekke, vedkommendes profesjonelle dømmekraft sett utenfra?
- Er vedkommendes opptreden egnet til å svekke tilliten til beslutningen?

Det skal legges vekt på muligheten for personlig fordel, tap eller ulempe som følge av utfallet av saken.

Nedenfor er det satt opp en oversikt over hvilke forhold som bør vurderes når man skal avgjøre om en person er inhabil.

Sjekkpunkter	**Nærmere beskrivelse**
a) Automatisk inhabilitet	Se bestemmelsene om automatisk inhabilitet
b) Nær personlig/faglig tilknytning	Nært personlig vennskap (det må være mer enn bare bekjentskap), faglig fellesskap, for eksempel samarbeid eller samforfatterskap av nyere dato etc. Både omfang og nærhet i tid er elementer i vurderingen av nærhet i samarbeid/-samforfatterskap (se kapittel 4.1 om faglig samarbeid). Ved vurdering av om nære personlige eller faglige forhold fører til inhabilitet, må det vurderes om avgjørelsen av den aktuelle saken har betydning for den man har et nært forhold til (jf. punkt c).
c) Mulighet for personlig vinning/tap/ulempe	For å bli inhabil skal man selv, eller noen man har et nært forhold til (punkt b), ha noen grad av personlig interesse av utfallet av en sak. I Forskningsrådet vil det normalt dreie seg

	om utfallet av en prosjektbevilgningssak. Den personlige interessen kan være av faglig og/eller økonomisk art. For universitetsansatte kan egeninteressen ofte være av faglig art. Man kan ha en egeninteresse av at ens fagmiljø blir styrket, får økt anerkjennelse, eller får finansiert nytt utstyr, selv om man ikke selv er direkte involvert i det aktuelle prosjektet, fordi dette kan øke ens egne muligheter for fremtidig støtte. For en bedriftsansatt, spesielt fra en liten bedrift, kan egeninteressen være av økonomisk art, det kan trygge arbeidsplassen for alle om bedriften får en bevilgning. For ansatte ved forskningsinstitutter kan begge forhold være aktuelle, avhengig av instituttets størrelse og mangfold (se kapittel 5).
d) Andre særegne forhold som er egnet til å svekke tilliten til en beslutning hvis vedkommende deltar	Er det noen forhold som kan svekke, eller kan antas å svekke, den profesjonelle dømmekraften sett utenfra, for eksempel knyttet til kravet om forsvarlig saksbehandling, likebehandling eller saklighet? Kontrollspørsmålet må være: Hvordan tar dette seg ut utenfra? Det må være en vurdering som bygger på mer enn løse antagelser og spekulasjoner. Man må vurdere det slik at det er overveiende sannsynlig, at noen vil reise spørsmål ved en persons upartiskhet, og at dette vil svekke tilliten til den aktuelle beslutningen.

Det er viktig at alle aktuelle momenter vurderes i hvert enkelt tilfelle. Hvis flere momenter gjør seg gjeldende samtidig, kan det lettere føre til inhabilitet.

4. Vurdering av inhabilitet etter skjønn

Når det ikke foreligger automatisk inhabilitet, er det viktig å vurdere inhabilitet ut fra reglene om skjønn. Det er ulike faktorer som må vurderes under denne kategorien. Vurderingstemaene er om det foreligger andre særegne forhold som er egnet til å svekke tilliten til en beslutning dersom vedkommende deltar i saksbehandlingen. Det skal bl.a. legges vekt på om avgjørelsen i saken kan innebære en mulighet for fordel, tap eller ulempe for vedkommende selv eller noen han eller hun har nær personlig tilknytning til.

Habilitetskravene kan bli noe strengere jo vanskeligere, viktigere og mer skjønnspreget en sak er, og også når den enkeltes mulighet for å påvirke den endelige avgjørelse i en sak er stor. Det er viktig at det ikke skapes tvil om vedkommendes tilknytning til saken eller partene.

Nedenfor drøftes en del typiske situasjoner som er aktuelle i Forskningsrådet

4.1 Nært faglig samarbeid, herunder samforfatterskap og veiledning

Den som har, eller inntil nylig har hatt, et nært faglig samarbeid med en person eller institusjon som er part i saken vil kunne bli inhabil fordi et nært faglig samarbeid kan påvirke evnen til upartisk vurdering.

Generelt skal det mye til for at samarbeid i tjeneste skal medføre inhabilitet. Det er først hvis samarbeidet er særlig nært og omfattende at det kan bli spørsmål om inhabilitet av den grunn alene.

Vanlig samarbeid i tjeneste og kontakt grunnet i arbeid innen samme fagfelt vil normalt ikke føre til inhabilitet. Forvaltningsloven åpner for en bred skjønnsmessig vurdering der det avgjørende er om det er konstatert et «særegent forhold» og om det er «egnet til å svekke tilliten» til upartisk vurdering. Forskning kan imidlertid ha særtrekk som skiller det fra annet samarbeid i tjeneste, fordi forskning er en mer personlig virksomhet.

Der kriteriene for rettmessig forfatterskap er oppfylt (jfr. definisjonen i etikkom.no) vil det foreligge et samarbeid, men det er ikke gitt at det medfører inhabilitet. Antall bidragsytere til en publikasjon, og rollen vedkommende har hatt, kan si noe om sannsynligheten for at samarbeidet er så nært at det vil medføre inhabilitet. Antall sampublikasjoner og utgivelseshyppigheten er også faktorer som må vurderes.

Samforfatterskap som ikke fyller vilkårene for rettmessig forfatterskap, vil ikke føre til inhabilitet med mindre det også foreligger samarbeid ut over samforfatterskapet som er av en slik karakter at det fører til inhabilitet.

- Redaktøransvar vil normalt ikke medføre inhabilitet.
- Ved rettmessig samforfatterskap som ligger nær 3 år tilbake i tid kan det være aktuelt å undersøke når samarbeidet fant sted, fordi det kan ha gått en tid før publikasjonen kom på trykk.

Veiledning
En person som har vært veileder for en part med sikte på doktorgrad for mer enn tre år siden (jf. bestemmelsenes punkt 3.1 f) må vurdere sin habilitet ut fra spørsmålene i de tre kulepunktene i kapittel 3 i veiledningen. Det samme gjelder for den som er, eller har vært, veileder for en part med sikte på andre eksamener enn doktorgrad.

5. Inhabilitet for ansatt ved samme institusjon (kollega-inhabilitet)

Når det gjelder kollegainhabilitet, kan både reglene om automatisk inhabilitet og inhabilitet etter skjønn komme til anvendelse.

Flere momenter må vurderes når en person skal være med på å fatte vedtak som gjelder søknader fra den institusjonen der vedkommende er ansatt.

- Hvilken posisjon har vedkommende i institusjonen?
  - Under ellers like forhold vil inhabilitet kunne oppstå oftere når vedkommende har en sentral posisjon i den virksomhet der vedkommende er ansatt.
- Eierrettigheter i form av aksjer eller lignende i den institusjonen hvor vedkommende er ansatt, må vurderes.
  - Høy stilling ved institusjonen kan medføre at selv en mindre aksjepost vil kunne utløse inhabilitet. Omvendt vil en stor aksjepost kunne bidra til å utløse inhabilitet også for en vanlig ansatt i vedkommende institusjon.

Vurdering av inhabilitet vil kunne påvirkes av hvilken sektor (universitetssektoren, instituttsektoren eller næringslivet) vedkommende er tilknyttet.

Under følger noen momenter som kan brukes ved habilitetsvurderingen basert på vedkommendes tilknytning til de ulike sektorene:

Universitetssektoren

Den som er rektor, dekan eller instituttleder vil være inhabil til å behandle søknader fra egen enhet i henhold til bestemmelsenes punkt 3.1 e). Det samme gjelder den som sitter i styret for universitetet, fakultetet eller instituttet.

Forsker/professor vil ofte kunne være inhabil for søknader der forskere fra egen forskergruppe, eller nære faglige samarbeidspartnere, er sentrale. Det at man kommer fra samme institutt, behøver ikke å medføre inhabilitet. Dette vil være avhengig av instituttets størrelse (antall forskere) og den faglige relasjonen mellom søker og vedkommende forsker/professor. Dette må vurderes konkret i hvert enkelt tilfelle.

Instituttsektoren

Den som er leder, eller har ledende stilling, ved et institutt vil være inhabil i henhold til bestemmelsenes punkt 3.1.e). Det samme gjelder den som sitter i styret for instituttet.

Forsker-/professorstilling vil, på samme måte som for universitetssektoren, ofte kunne medføre inhabilitet for søknader der forskere fra egen forskergruppe eller nære faglige samarbeidspartnere er sentrale. I tillegg må det vurderes hvilken betydning det har for den ansatte at en søknad fra instituttet blir innvilget. I denne vurderingen må det legges særlig vekt på prosjektets betydning for instituttets økonomi og renommé.

Næringslivet

Den som er leder, eller har ledende stilling, i et selskap vil være inhabil i henhold til bestemmelsenes punkt 3.1.e). Det samme gjelder den som sitter i styret for selskapet.

Ansatte i et selskap som søker om forskningsmidler, vil, på samme måte som for universitets- og instituttsektoren, ofte kunne være inhabile for søknader der personer fra eget fagmiljø eller nære faglige samarbeidspartnere er sentrale. I tillegg må det vurderes hvilken betydning det har for de ansatte at en søknad fra selskapet blir innvilget. I denne vurderingen må det legges særlig vekt på prosjektets betydning for selskapets økonomi og renommé.

Saksfremlegg
Porteføljestyremøte 2/25

Sak PS-Forskningssystemet 24/25
Forskningssikkerhet

Til	Ansvarlig direktør	Saksbehandler	Vedlegg
Porteføljestyret	Johannes W. Løvhaug	Heidi Dybesland / Jon Flæten / Bjørn Tore Kjellemo	KVAST Delleveranse 1 KVAST Delleveranse 2

Fra

Områdedirektør

Benedicte Løseth

DRØFTINGSSAK

Forslag til vedtak

Porteføljestyret tar orienteringen om arbeidet med forskningssikkerhet, ny portefølje for forsvar og sikkerhet og utarbeidelsen av et kunnskapsgrunnlag for vurdering av sensitive teknologiområder (KVAST) til etterretning. Administrasjonen tar med seg innspill fra porteføljestyret i det videre arbeidet.

Kort bakgrunn

En endret sikkerhetspolitisk situasjon har økt behovet for tiltak, både for å beskytte forskningens verdier og for å fremme forskning og innovasjon på områder som er viktige for nasjonal sikkerhet. Forskningsrådet har derfor gjennom det siste året intensivert arbeidet med forskningssikkerhet, sensitive teknologier og forskning for forsvar, sikkerhet og beredskap. Arbeidet er organisert i tre prosjekter:

1) Etablering av nye rutiner og tiltak for forskningssikkerhet.
2) Arbeid med å etablere en ny portefølje for forsvar, sikkerhet og beredskap.
3) Oppdrag fra kunnskapsdepartementet til Forskningsrådet, Forsvarets forskningsinstitutt og Nasjonal sikkerhetsmyndighet om å utarbeide et kunnskapsgrunnlag for vurdering av sensitive teknologier (KVAST).

Hvorfor saken fremmes til dette møtet

Porteføljestyret orienteres om pågående arbeid med forskningssikkerhet, og inviteres til å:

A. Kommentere Forskningsrådets rolle i arbeidet med forskningssikkerhet og etableringen av en ny portefølje for forsvar, sikkerhet og beredskap, samt delleveransene 1 og 2 i KVAST-oppdraget.
B. Gi innspill til det videre arbeidet med forskningssikkerhet i Forskningsrådet.

Hovedpunkter

1. **Forskningsrådets arbeid med forskningssikkerhet**

Forskningsrådet har i flere år jobbet med spørsmål relatert til forskningssikkerhet og ansvarlig internasjonalt kunnskapssamarbeid. Det siste året har forskningssikkerhet blitt tydeligere definert og kommet høyt på agendaen både internasjonalt og nasjonalt. Det europeiske rådets anbefalinger til medlemslandene om å styrke arbeidet med forskningssikkerhet fra 2024 peker blant annet på at finansierende organisasjoner bør utvikle risikovurdering som del av søknadsprosessene, oppfordre søkere til å identifisere risiko i forkant av prosjekter og etablere tiltak for å redusere risiko i prosjekter med høy risiko.

Høsten 2024 etablerte Forskningsrådet en tverrgående gruppe med ansvar for forskningssikkerhet, Gruppen jobber med interne prosesser, kompetanseheving og utvikling av Forskningsrådets rolle i forskningssektoren. Gruppen er i løpende kontakt med institusjoner både i UH- og instituttsektor, og med andre aktører på feltet, som HK-dir og Direktoratet for eksportkontroll og sanksjoner (DEKSA). Forskningsrådet

deltar i flere internasjonale grupper dedikerte til forskningssikkerhet, i regi av OECD GSF, EU-kommisjonen/ERA-arbeidet og Science Europe, og vi har bilateral kontakt med andre finansiører internasjonalt om denne tematikken.

Et viktig delprosjekt i 2025 er å utvikle en løsning for risikovurdering i søknadsbehandlingen. Denne løsningen skal bidra til å avdekke problematiske forhold i prosjekter og sikre at institusjonene har nødvendige rutiner og tiltak til at prosjekter kan gjennomføres der hvor det er identifisert risiko. Det legges vekt på å utvikle en enkel rutine/spørsmål til søkere basert på utprøvde tilnærminger blant annet inspirert av Horisont Europa og UK Research and Innovation (UKRI), og å finne en god balanse mellom institusjonenes ansvar for sikkerhet og Forskningsrådets ansvar som finansiør. Arbeidet med forskningssikkerhet skjer i tett samarbeid med arbeidet med å etablere en ny portefølje for forsvar, sikkerhet og beredskap (punkt 2) og KVAST-prosjektet (punkt 3).

2. Ny portefølje for forsvar, sikkerhet og beredskap

Forskningsrådets, FFIs og NSM leverte i fjor en felles rapport om *Et helhetlig forskningssystem for forsvar, sikkerhet og beredskap*, hvor en av anbefalingene var at det ble etablert en egen portefølje for dette i Forskningsrådet. Etter at Forskningsrådets styre sluttet seg til rapporten og anbefalingene på septembermøtet i fjor, har administrasjonen arbeidet langs flere spor. Dels har en løftet denne saken i dialogen med forskningssektoren, dels har en hatt en løpende dialog med relevante departement, og dels har en gjort en intern utredning av ulike spørsmål knyttet til en ev ny portefølje.

Forskningsrådets styre ble på møtet 13. mars orientert om status for arbeidet, og videre planer, og styret sluttet seg til arbeidet som er gjort så langt for å etablere en ny portefølje. Administrasjonen vil følge opp med å legge fram en beslutningssak om etablering av ny portefølje på styremøte 23. april. Dersom styret slutter seg til administrasjonens anbefaling, vil en deretter gå videre med rekruttering og oppnevning av nytt porteføljestyre og annet som må på plass for en ny portefølje.

3. Utarbeide et kunnskapsgrunnlag for vurdering av sensitive teknologier (KVAST)

Oppdraget fra Kunnskapsdepartementet 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.

Den første av delleveransene ble sendt til Kunnskapsdepartementet 15. januar (vedlegg 1). Det er en beskrivelse av

a. valg av metode
b. videre fremdriftsplan, som angir tidspunkt for øvrige delleveranser og tilhørende statusmøter med oppdragsgiver.
c. hvem som i utgangspunktet vurderes som de mest relevante aktørene på hvert av de aktuelle teknologiområdene, hvordan vi vil gå frem for å identifisere flere aktuelle bidragsytere og hvordan man vil involvere disse aktørene i videre arbeid.

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 oversikt over sensitive teknologier med hensyn til nasjonal sikkerhet. Forslaget er i stor grad overlappende med EUs liste over kritiske teknologier, men med noen tillegg.

	Det er utarbeidet en plan for å kvalitetssikre oversikten gjennom involvering av UH-institusjoner, institutter og forsvarsindustri. Det vil settes ut et oppdrag for å få gjennomført en kartlegging av hvordan oversikten samsvarer med miljøer som forsker på, anvender eller finansierer disse teknologiene. I tillegg vil vurdering av forhold knyttet til sårbarhet, risiko, mangler og komparative fortrinn kartlegges.
Forberedelse / prosess	Administrasjonen har utviklet saken.

Forskningsrådet

Kunnskapsdepartementet
Att: Mette Lending
Postboks 8119 Dep,
0032 Oslo

Vår saksbehandler / tlf.	Vår ref.	Deres ref.	Sted
Heidi Dybesland/98406052	24/6019	[Ref.]	Oslo 15.01.2025

Kunnskapsgrunnlag for vurdering av sensitive teknologier - delleveranse 1: beskrivelse av gjennomføring

Vi viser til oppdrag fra Kunnskapsdepartementet, Forsvarsdepartementet og Justisdepartementet av 31. oktober 2024. Norges forskningsråd, Forsvarets forskningsinstitutt og Nasjonal sikkerhetsmyndighet har sammen utarbeidet delleveranse 1, og kommer til å jobbe sammen på de ulike delleveransene.

I delleveranse 1 er vi bedt om å beskrive hvordan arbeidet i delleveransene 2-5 i oppdraget er tenkt gjennomført med tanke på:

a. valg av metode
b. fremdriftsplan, inkludert tidspunkt for delleveranser og tilhørende statusmøter med oppdragsgiver
c. identifisering og involvering av relevante aktører i arbeidet

Håndteringen av eventuell gradert informasjon og resultater fra kunnskapsgrunnlaget vil vurderes løpende.

Delleveranse 2

Fra oppdragsbeskrivelsen:

Utarbeide en systematisk sammenstilling av relevant eksisterende kunnskap / oversikter / lister som omhandler sensitive teknologier, på tvers av ulike land og sektorer, og identifisere eventuelle kunnskapshull av betydning for norske forhold og behov, samt gi anbefalinger om hvordan disse hullene eventuelt kan tettes.

Vi har valgt å dele utarbeidelsen av denne leveransen i tre trinn:

1. Sammenligne den systematiske sammenstillingen fra EU med tilsvarende lister f.eks. fra USA, Storbritannia, Canada, Australia og NATO.
2. Med utgangspunkt i EUs liste over kritiske teknologier, utarbeide en systematisk sammenstilling med relevante norske dokumenter som omhandler kritiske/sensitive teknologier med betydning for nasjonal og alliert sikkerhet.
3. Basert på den systematiske sammenstillingen, identifisere eventuelle kunnskapshull som kan ha betydning for nasjonale sikkerhetsinteresser.

Operasjonalisering og begrepsavklaring

Oppdragsbeskrivelsen påpeker behovet for en felles forståelse om hvilke teknologiområder og konkrete teknologier som vurderes som kritiske/sensitive. Vi forutsetter at det skal vurderes som kritisk/sensitivt opp mot nasjonal sikkerhet, forskning, utvikling og innovasjon – og dermed en sentral forutsetning for å kunne iverksette målrettede og proporsjonale risikoreduserende tiltak.

Etableringen av en felles begrepsforståelse av hva som er kritisk og/eller sensitive teknologier anses nødvendig. Dette forslås gjennomført ved å oversette EUs kritiske teknologiområder for økonomisk sikkerhet (Critical Technology Areas for the EU's economic security) til norsk, tilpasset norsk kontekst og behov, kvalifisert av relevant fagekspertise. Videre vil det, for å sikre et presist begrepsapparat, fremmes en omforent definisjon for påfølgende risikovurdering av kritiske/sensitive teknologier.

En foreløpig arbeidende definisjon er at sensitive teknologier kan være:

> *Avanserte og fremvoksende teknologier viktige for norsk sikkerhet, forskning, utvikling og innovasjon, som ved tilegnelse fra utenlandske statlige, statlig støttede, eller ikke-statlige aktører vil kunne medføre skadefølger for nasjonal og alliert sikkerhet, økonomisk konkurranseevne og/eller samfunnskritiske områder.*

Systematisk sammenstilling (trinnene 1 og 2)

EUs liste over kritiske teknologier legges til grunn for sammenstillingen og ses opp mot andre relevante lister, oversikter og kunnskap knyttet til kritiske/sensitive teknologier av strategisk betydning for nasjonal sikkerhet. Utgangspunktet for datainnsamlingen er de dokumenter som henvises til i *Vedlegg B: Vurdering av fag- og teknologiområder* i rapporten *Et helhetlig forskningssystem for åpen, skjermet og gradert forskning.*.

Ved å se EUs liste over kritiske teknologier opp mot andre relevante lister vil vi, innenfor hvert enkelt teknologiområde, kunne identifisere manglende eller svak omtale på tvers av de ulike listene/dokumentene. Dette gjøres ved å undersøke om det finnes kritiske/sensitive teknologier som omtales i nasjonale og allierte dokument eller i dokumenter fra sentrale allierte utenfor EU som ikke er på EUs lister og motsatt.

I etterkant vil vi kvalitetssikre den tilgjengelige kunnskapen som omhandler kritiske/sensitive teknologier for å avdekke eventuelle hull eller mangler. Dette vil blant annet gjøres gjennom dialog med eierne av de ulike dokumentene og relevante miljøer (se også delleveranse 3).

Utvide horisonten (trinn 3)

I de foregående trinnene benyttes eksisterende dokumenter for å etablere et kunnskapsgrunnlag og identifisere gap. Det er hensiktsmessig å kvalitetssikre og utfordre dette kunnskapsgrunnlaget med flere kilder, herunder å gjøre vurderinger og få innspill på hvilke teknologiområder som er spesielt viktige for Norge. Det foreslås for eksempel å gjennomføre en undersøkelse til medlemmene i Forsvars- og Sikkerhetsindustriens forening (FSi). Grunnen til at FSi er relevant her, er at særskilte norske kunnskapsbehov vil være knyttet til forsvarsmateriell som utvikles og produseres i Norge. Mulige aktører er EOS-tjenestene, DEKSA og aktører i UH- og instituttsektoren, med flere.

Trinn 3 skal gjennomføres i samspill med delleveranse 3. Det gjelder informasjonsmøte, undersøkelse/survey, dialogrunder og uavhengig vurdering av eksperter.

Frist for trinn 1: **7. mars 2025.**
Frist for trinn 2 og 3: **19. september 2025.**

Delleveranse 3

Fra oppdragsbeskrivelsen:

Kartlegge hva som er Norges posisjon innenfor disse sensitive teknologiene per i dag. Noen sentrale spørsmål med tanke på videre politikkutvikling er:

- 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?

Eksisterende kilder

Spørsmålene over vil delvis kunne besvares gjennom eksisterende kilder:

- Evaluering av matematikk, IKT og teknologi (kommer mars/april 2024). Spørsmål om Norges posisjon innenfor sensitive teknologier skal besvares av den nasjonale komiteen for hovedrapporten.
- Evaluering av naturvitenskap 2022–2024. Evalueringen vurderte blant annet Norges posisjon innen energiteknologi og kvanteteknologi.
- Forskningsrådets oversikt over prosjekter og samarbeidspartnere.
- Norske prosjekter i Horisont Europa, European Defence Fund (EDF) og Digital Europe.

- Samarbeidsmønstre via Web of science.
- NIFU-oppdraget «Kunnskap og sikkerhet i en ny geopolitisk tid».

Involvering av aktuelle miljøer

I tillegg til eksisterende kilder vil vi foreta eller bestille en kartlegging i aktuelle miljøer i UH-sektoren, instituttsektoren og forsvarsindustrien for å besvare spørsmålene som er skissert i oppdraget. Vi vil også vurdere om det er andre spørsmål kan være aktuelle.

Vi ser for oss fire trinn:

1. Møte med institusjons-/organisasjonsledere og andre aktuelle aktører som UHR, FFA og FSi i slutten av februar for å kommunisere hva oppdraget består i og hvordan det er tenkt gjennomført. Formålet er både å sikre at alle får det samme budskapet og at vi får tilbakemelding på forslag til prosess og involvering.
2. Undersøkelse/survey til aktuelle UH-institusjoner/institutter/industri med spørsmål om hvordan forslaget til liste over sensitive teknologier faller sammen med miljøenes, hvilke konkrete teknologier de forholder seg til, hvem de samarbeider med innenfor teknologiene, hvor Norge har konkurransefortrinn, risikovurdering m.m.
3. I etterkant av undersøkelsen legges det opp til dialog med enkeltmiljøer som forsker på, anvender eller finansierer sensitive teknologier.
4. Mulig innhenting av en samlet vurdering av spørsmålene som skal vurderes i delleveranse 3 fra uavhengige eksperter.

Resultatene fra delleveranse 3 vil være særlig relevant i oppfølgingen av rapporten *Et helhetlig forskningssystem for åpen, skjermet og gradert forskning*.

Frist for leveranse: **19. september 2025.**

Delleveranse 4

Fra oppdragsbeskrivelsen:

Analysere konkrete teknologiområder/ev. underkategorier både med tanke på risikonivå og hvilken type risiko som er forbundet med hvert enkelt område, bl.a. med henblikk på

- teknologiens muliggjørende potensial
- sannsynligheten for at flerbrukspotensialet realiseres til militær bruk
- risiko for misbruk til menneskerettighetsbrudd mv.

Samle resultatet av analysene i en oversikt som skal kunne deles bredest mulig.

Delleveranse 4 skal ta utgangspunkt i oversikt og lister over sensitive teknologier i delleveranse 2 og gjennomføre en analyse av teknologiområder med eventuelle underkategorier. Analysen skal ta utgangspunkt i teknologiens egenart og mulige bruksområder med tanke på risikonivå og hvilken type risiko som er forbundet med hvert enkelt område.

- Teknologiområdets potensielle bruksområder for å ivareta nasjonal sikkerhet og samfunnssikkerhetsinteresser
- Teknologiområdets potensielle bruk hos trusselaktører
- Sannsynligheten for at flerbrukspotensialet realiseres til militær bruk eller på andre måter som kan skade nasjonale sikkerhetsinteresser
- Behovet for skjerming av informasjon

Følgende kilder er så langt identifisert:

- Delleveranse 2 og 3.
- Trussel- og risikovurderinger fra EOS-tjenestene og Nasjonalt etterretnings- og sikkerhetssenter (NESS).
- NIFU-oppdraget «Kunnskap og sikkerhet i en ny geopolitisk tid».
- Input fra samtaler med sentrale aktører i kunnskapssektoren og industrien
- Skriftlige vurderinger fra EU og andre nordiske land.
- På områder NSM har aktiviteter eller interesse for kan vi gjenbruke eller utarbeide tilpassede vurderinger.

Avhengig av både delleveranse 2 og omfanget av arbeidet kan det vurderes å anmode om informasjon fra:

- Samarbeidende tjenester nasjonalt og internasjonalt.
- Internasjonale organisasjoner der NSM representerer sikkerhetsmyndighetene eller deltar i sikkerhetsarbeid.
- Relevante deler av forsvarsindustrien og forsvarssektoren.

Om det skulle bli aktuelt, vil det være naturlig at FFI og NSM samarbeider om de to siste kulepunktene.

Vurderinger knyttet til Norges nåværende posisjon innenfor de ulike områdene er ikke en del av denne delleveransen, men det vil gjøres en overordnet vurdering av risiko knyttet til nåværende internasjonalt samarbeid om de ulike kategoriene der det er kjent.

Resultatet skal samles i et dokument som viser en oversikt som skal deles bredest mulig.

Frist for leveranse: **31. oktober 2025.**

Forskningsrådet

Delleveranse 5

Fra oppdragsbeskrivelsen:

Foreslå mulig system for håndtering av relevant kunnskap etter at oppdraget er fullført:

- 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 mv.
- Basert på dette, foreslå en egnet rigg for løpende drift og oppdatering av kunnskapsgrunnlaget etter at oppdraget er fullført (dvs. fra og med 2026).

Besvarelsen vil avhenge av det kunnskapsgrunnlaget som utvikles. Det vil bli tydeligere underveis i prosjektet hvilken metode og involvering som kreves.

Frist for leveranse: **31. desember 2025.**

Delleveranse 6

Fra oppdragsbeskrivelsen:

Levere en sluttrapport fra arbeidet som sammenfatter sentrale hovedfunn og erfaringer fra gjennomføring av oppdraget.

Forskningsrådet, NSM og FFI skal sammen utarbeide sluttrapporten. Vi vil vurdere å opprette en referansegruppe for å sikre kvaliteten på rapporten.

Frist for leveranse: **31. desember 2025.**

Oversikt over statusmøter og leveranser

	Statusmøte	**Leveranse**
Delleveranse 1	31. januar	15. januar
Delleveranse 2	4. mars	7. mars
Oppdatering	23. mai	
Delleveranse 3	12. september	19. september
Delleveranse 4	24. oktober	31. oktober
Delleveranse 5 og 6	5. desember	31. desember

Vi tar gjerne et møte med oppdragsgiver i januar 2026 etter at alle leveransene er levert.

Forskningsrådet

Vi ser frem til dialog om forslaget på møtet 31. januar.

Med vennlig hilsen
Norges forskningsråd

Benedicte Løseth
Områdedirektør
Forskningssystemet og internasjonalisering

Johannes W. Løvhaug
Avdelingsdirektør
Forsknings- og innovasjonssystemet

Brevet er elektronisk signert

FFI Forsvarets forskningsinstitutt

Forskningsrådet | NASJONAL SIKKERHETSMYNDIGHET

FFI-NOTAT

Eksternnotat 25/00521

Kunnskapsgrunnlag for vurdering av sensitive teknologier (KVAST)

– delleveranse 2: Norske teknologiområder av strategisk betydning for nasjonal sikkerhet

Forfattere
Frank Brundtland Steder og Tord Apalvik
Prosjektnummer 1619
7. mars 2025

Godkjenner
Jan Erik Torp, *assisterende direktør*

Dokumentet er elektronisk godkjent og har derfor ikke håndskreven signatur.

Emneord
Teknologisk utvikling, Avanserte halvlederteknologier, Kunstig intelligens, Kvanteteknologier, Bioteknologier, EU

Sammendrag
I notatet gjøres en analyse og vurdering av sensitive teknologiområder med strategisk betydning for økonomisk konkurranseevne, nasjonal sikkerhet og militær relevans. Med utgangspunkt i EUs liste over kritiske teknologier for økonomisk sikkerhet og en sammenligning med tilsvarende lister fra andre land og organisasjoner gir dokumentet et kunnskapsgrunnlag for å utvikle en oversikt over sensitive teknologier som reflekterer både globale trender og spesifikke norske behov. Herunder understrekes viktigheten av samarbeid mellom offentlige myndigheter, akademia og næringslivet for å beskytte og fremme Norges teknologiske interesser. Listen som foreslås er ikke endelig, men danner grunnlaget for det videre arbeid i KVAST og kan bli justert som følge av dette.

E

Innhold

1 Innledning

Dette notatet er delleveranse 2 i oppdraget fra Kunnskapsdepartementet av 31. oktober 2024, hvor det skal utarbeides et *kunnskapsgrunnlag for vurdering av sensitive teknologier* (KVAST). Det er satt ned en arbeidsgruppe med representanter fra Norges forskningsråd (NFR), Forsvarets forskningsinstitutt (FFI) og Nasjonal sikkerhetsmyndighet (NSM) som skal jobbe sammen på de ulike delleveransene. Notatet er utarbeidet av FFI, i tett dialog med arbeidsgruppen.

KVAST består av seks delleveranser hvor delleveranse 1 handler om å beskrive gjennomføringen av de påfølgende delleveransene inkludert metodevalg, fremdriftsplan og involvering av relevante aktører. I delleveranse 2 sammenstilles eksisterende kunnskap om sensitive teknologier mellom ulike land og sektorer. Delleveranse 3 innebærer kartlegging av Norges posisjon innen sensitive teknologier, inkludert nøkkelaktører og essensielle fagmiljøer. Delleveranse 4 er en analyse av teknologiområdene med hensyn til risikonivå og type risiko, samt en vurdering av teknologienes mulige bruksområder og behov for informasjonsbeskyttelse. Delleveranse 5 skal vurdere hvilke produkter som krever kontinuerlig oppdatering, og foreslå et system for håndtering av kunnskapen etter prosjektets fullføring. Til slutt, i delleveranse 6, utarbeides en sluttrapport med hovedfunn og erfaringer fra gjennomføringen av hele oppdraget.

Dette notatet vil med utgangspunkt i EUs liste over kritiske teknologiområder[1] sammenligne EUs teknologiområder opp mot tilsvarende lister fra andre land og NATO. Basert på denne sammenligningen etableres et kunnskapsgrunnlag for å utarbeide et omforent forslag til sensitive teknologier i Norge, med vekt på nasjonal sikkerhet. Utgangspunktet for datainnsamlingen er de dokumenter som henvises til i vedlegg B i publikasjonen *Et helhetlig forskningssystem for åpen, skjermet og gradert forskning.*[2]

Det er viktig å etablere en felles begrepsforståelse av de sensitive teknologiene. Dette gjøres blant annet ved å oversette og beskrive EUs kritiske teknologiområder for økonomisk sikkerhet til norsk, tilpasset norsk kontekst og behov. Videre foreslås det i kapittel 2 en definisjon av «sensitive teknologier for nasjonal sikkerhet» for å sikre et mer presist begrepsapparat i påfølgende presentasjon og analyse av tilsvarende lister med teknologier i kapittel 3 og 4.

Delleveranse 2 brukes som et utgangspunkt for innspill fra relevante aktører innen universitets- og høgskolesektoren, instituttsektoren, industrien og andre interessenter. Mer overordnet vil et omforent begrepsapparat legge til rette for tydelige initiativ og satsninger for å utbedre eventuelle svakheter og å styrke eksisterende fortrinn. Vi vurderer det spesielt viktig å sammenligne EUs liste med kritiske teknologier med tilsvarende lister fra et ikke-tilfeldig utvalg av nære allierte samt NATO som organisasjon.

[1] Europakommisjonen. (2023). *Annex to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States*.
[2] Forskningsrådet, Forsvarets forskningsinstitutt, & Nasjonal sikkerhetsmyndighet. (2024). *Et helhetlig forskningssystem for åpen, skjermet og gradert forskning.*

2 Sensitive teknologier for nasjonal sikkerhet

Utviklingen på ulike teknologiområder akselererer hurtig og har konsekvenser på tvers av politikkområder.[3] I sikkerhetsfaglig råd påpeker NSM at det foregår en geopolitisk konkurranse om teknologisk herredømme, og at utviklingen innenfor fremvoksende og banebrytende teknologier (emerging and disruptive technologies; EDT'er) samtidig som det gir verdiskapende muligheter, også er en kime til nye sårbarheter og trusler.[4] På samme måte trekker langtidsplanen for forsvarssektoren frem at slike teknologier vil kunne påvirke samfunn, internasjonale makt-forhold, gjensidige avhengigheter, verdikjeder, produksjonssystemer og måten militærmakt anvendes på.[5]

Å forstå hvorfor de ulike teknologiene alene eller i kombinasjon utgjør et problem eller en mulighet, hvordan de forventes å utvikle seg, og hva dette vil bety for nasjonal sikkerhet er nødvendig for å bevare norsk sikkerhet, økonomiske konkurranseevne og samfunnskritiske funksjoner.

2.1 Den fjerde industrielle revolusjon

Fellesnevnerne for teknologiene i den såkalte fjerde industrielle revolusjon er at de er intelligente, sammenkoblede (interconnected), desentraliserte og digitale (I2D2).[6] Dette understreker mulighetene som ligger i konvergensen av ulike teknologier, eksempelvis koblingen mellom kunstig intelligens, stordata og autonomi. De fleste av I2D2-teknologiene har bred anvendelse og er i økende grad integrert i både sivil og militær virksomhet.

Den teknologiske utviklingen og investeringer i ny teknologi foregår i større grad i det privatkommersielle markedet, spesielt innenfor kvanteteknologi, kunstig intelligens og elektronikk.[7] Imidlertid er virkemiddelapparatet i offentlig sektor vesentlig for risikokapital til nisjeteknologier og forskning på lavere TRL-nivå[8] (1-3) avhenger fortsatt i stor grad offentlig finansiert forskning.[9] Likevel medfører økende teknologiske kommersialisering at skillet mellom militær og sivil teknologi blir stadig mindre og vanskeligere å skille fra hverandre.[10]

Dette reiser en rekke problemstillinger i skjæringsfeltet kunnskapspolitikk, sikkerhetspolitikk og nasjonal sikkerhet og stiller nye krav til forskningssikkerhet. Dette tydeliggjør et nødvendig samspill mellom offentlige myndigheter, akademia og næringsliv for å treffe løsninger som tilrettelegger for forskning, utvikling og innovasjon som både fremmer og beskytter norske sikkerhetsinteresser og konkurransekraft. Et strukturert, funksjonelt og dynamisk sikkerhets-

[3] Forsvarsdepartementet. (2021). *Meld. St. 17 (2020–2021): Samarbeid for sikkerhet*. s. 12.
[4] Nasjonal sikkerhetsmyndighet. (2023). *Sikkerhetsfaglig råd - Et motstandsdyktig Norge*. s. 19; 35.
[5] Forsvarsdepartementet. (2024). *Prop. 87 S (2023–2024): Forsvarsløftet – for Norges trygghet. Langtidsplan for forsvarssektoren 2025–2036*. s. 138
[6] NATO STO. Science & Technology Trends 2023-2043. s. 10-12
[7] NATO STO. Science & Technology Trends 2023-2043. s. 9
[8] Technology Readiness Level
[9] NATO STO. Science & Technology Trends 2023-2024. s. 88-90
[10] Nasjonal sikkerhetsmyndighet. (2023), s. 35.

arbeid gir Norge strategiske fortrinn i en krevende tid hvor omstillingsevne og kompetansebehov er fremtredende. Målet må være at åpen forskning fortsatt skal være normen for vitenskapelig aktivitet, men samtidig må behovet for å iverksette beskyttende tiltak vurderes når dette er nødvendig.

I møte med en hurtigere teknologisk utvikling og økende stormaktsrivalisering har flere nasjoner og internasjonale organisasjoner utviklet ulike kunnskapsgrunnlag, teknologistrategier og lister for å fremme forskning, utvikling og innovasjon og samtidig styrke nasjonal sikkerhet og økonomisk konkurransekraft. En gjennomgang av relevant litteratur gir ingen omforent terminologi, men begreper som kritisk teknologi, sensitiv teknologi, strategisk teknologi, prioriterte teknologiområder, nøkkelteknologier og fremvoksende og banebrytende teknologier går igjen. I det neste delkapittelet gjøres det rede for hvordan teknologibegrepet forstås i dette oppdraget.

2.2 Definisjon av kritiske, sensitive og strategiske teknologier

I dette notatet benyttes begrepene kritiske teknologier, sensitive teknologier og strategiske teknologier. *Kritiske teknologier* gir den bredeste tilnærmingen og forstås som teknologier som er avgjørende for en nasjons sikkerhet, samfunnsfunksjoner, økonomiske vekst og teknologiske konkurranseevne. *Sensitive teknologier* forsås som teknologier som må skjermes på grunn av risiko for misbruk, konfidensialitet eller mulig skade hvis de kommer på avveie. *Strategiske teknologier* forstås som teknologier utpekt basert på et lands komparative fortrinn eller behov og som gir grunnlag for prioritering og påfølgende satsning. Kritisk blir dermed overbygningen, sensitivt ses i sammenheng med konsekvenser av kunnskap og teknologi som kommer på avveie og strategisk i sammenheng med nasjonale behov og muligheter. Med disse definisjonene blir strategiske teknologier en delmengde av sensitive teknologier, og sensitive teknologier en delmengde av kritiske teknologier. Det er hva som tillegges av betydning for sensitiv teknologi som er mest sentralt i dette arbeidet. I listene som er gjennomgått fra de ulike nasjonene og organisasjonene er sensitiv teknologi gjennomgående tett koblet opp mot nasjonal sikkerhet og behovet for beskyttelses- og kontrolltiltak for å forhindre misbruk og uautorisert tilgang.

Samtidig varierer definisjonene; noen legger større vekt på teknologiens innvirkning på samfunns- og økonomisk stabilitet, mens andre fokuserer mer på teknologisikkerhet og beskyttelse av immaterielle rettigheter. Enkelte definisjoner fremhever viktigheten av internasjonal regulering og samarbeid, mens andre vektlegger teknologiens rolle i forsknings- og utviklingsprosesser og behovet for å balansere sikkerhet med innovasjon. Til tross for disse variasjonene, er behovet for beskyttelse og regulering av sensitiv teknologi en fellesnevner.

Ifølge oppdragsbeskrivelsen er hensikten med KVAST-oppdraget å etablere et mer helhetlig kunnskapsgrunnlag om hvilke teknologiområder og konkrete teknologier som er særlig sensitive for nasjonal sikkerhet for å sikre:

1) Fortsatt åpenhet på områder hvor faglig samarbeid er ønskelig og viktig i lys av kunnskapspolitiske mål – inkludert Norges langsiktige kunnskaps- og kompetansebehov – og hvor eventuell risiko vurderes som håndterbar og dermed akseptabel.
2) Å redusere risiko til et akseptabelt nivå på områder som er i gråsonen.

3) Å unngå samarbeid på områder hvor risikoen vurderes som ikke-akseptabel.

Kunnskapsgrunnlaget vil inngå i arbeidet med å vurdere sensitive teknologier med utgangspunkt i norske forhold og interesser med sikte på å:

1) Redusere risiko forbundet med sensitive teknologier (beskytte)
2) Sikre tilstrekkelig norsk kunnskap og kompetanse på teknologiområder 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)

I denne leveransen er det innhentet informasjon fra et bredt dokumentgrunnlag, i antall og omfang. Selv om dokumentene som er analysert i denne leveransen i det store har et sammenhengende rasjonale; å utpeke viktige teknologier, er det det nyanser i hva som vektlegges med hensyn til bredde, tematikk og utgiver. De fleste lister er utgitt fra nasjonale myndigheter eller på oppdrag fra disse, mens enkelte dokumenter er mer selvstendige initiativ. Noen lister er rettet mot den bredere betegnelsen kritiske teknologier, mens andre benytter betegnelsene sensitive eller strategiske teknologier. Noen lister er rettet mot nasjonal sikkerhet, mens andre mer overordnet omtaler teknologier som er sentrale for et samfunns omstillingsevne, teknologiske konkurransekraft og lignende. Det er ikke enkelt å gjøre klare skiller her, og det er muligens heller ikke hensiktsmessig. Men, det er viktig å ha med seg i det videre arbeidet at listene ikke er direkte sammenlignbare, legger ulike begreper til grunn, er produsert på ulike tidspunkt og med noe ulike ambisjoner.

Tatt i betraktning oppdragets intensjon og føringen om å innhente informasjon fra et bredt dokumentgrunnlag, i antall og omfang, foreslås benyttet terminologien kritiske teknologier for nasjonal sikkerhet. I dette notatet benyttes følgende definisjoner for kritiske, sensitive og strategiske teknologier for nasjonal sikkerhet:

Kritiske teknologier: Teknologier som er avgjørende for en nasjons sikkerhet, samfunnsfunksjoner, økonomiske vekst eller teknologiske konkurranseevne.

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

Strategiske teknologier er teknologier som er viktige for framtidig norsk forskning, utvikling og innovasjon (FUI), økonomisk sikkerhet, norske sikkerhetsinteresser og bærekraftig utvikling.

Teknologier kan overordnet forstås som den praktiske anvendelsen av vitenskapelig kunnskap med formålet å skape verktøy, maskiner og systemer for å løse problemer og oppnå spesifikke mål. I tillegg til selve teknologien inkluderer vi også teknologisk *kompetanse* i vår forståelse, som inkluderer evnen til å utvikle, produsere og anvende disse teknologiene i praksis. I arbeidet med å ferdigstille endringer i eksportkontrollforskriften påpeker Utenriksdepartementet at

definisjon av begrepet «teknologi» er under arbeid. [11] Teknologibegrepet slik det benyttes i dette notatet vil justeres opp mot den endelige definisjonen i eksportkontrollforskriften.

Med tilgang menes evnen til enten å produsere eller anskaffe relevante teknologier og komponenter, samt tilstrekkelig beskyttelse mot uønsket utenlandsk avhengighet. Med kontroll menes evnen til å beskytte, regulere og sikre teknologien fra uautorisert bruk og overføring, lekkasje eller påvirkning fra aktører som kan utgjøre en trussel mot nasjonale sikkerhets-interesser. Disse teknologiene vil ofte kategoriseres som fremvoksende og banebrytende (disruptiv), men ikke all sensitiv teknologi som er sensitiv for nasjonal sikkerhet faller inn under den kategorien, og alle fremvoksende og banebrytende teknologier er ikke sensitive. Åpen og samarbeidsorientert *forskning* muliggjør *utvikling og innovasjon* og er en forutsetning for å kunne håndtere mange av samfunnets økonomiske og samfunnsmessige utfordringer.

Med nasjonale sikkerhetsinteresser legges forståelsen i sikkerhetslovens § 1-5 til grunn og forstås som «Landets suverenitet, territorielle integritet, demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til (a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet, (b) forsvar, sikkerhet og beredskap, (c) forholdet til andre stater og internasjonale organisasjoner, (d) økonomisk stabilitet og handlefrihet og e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet.».[12] Eksempler på dette er blant annet behovet for å ivareta beredskap og forsyningssikkerhet, skjerme sensitiv informasjon, sikre særlig følsom teknologi, ivareta særlige behov knyttet til nasjonale forhold og kunne operere sammen med allierte, inkludert evne til å nyttiggjøre seg alliert teknologi.[13]

2.3 Sensitiv teknologi og militær relevans

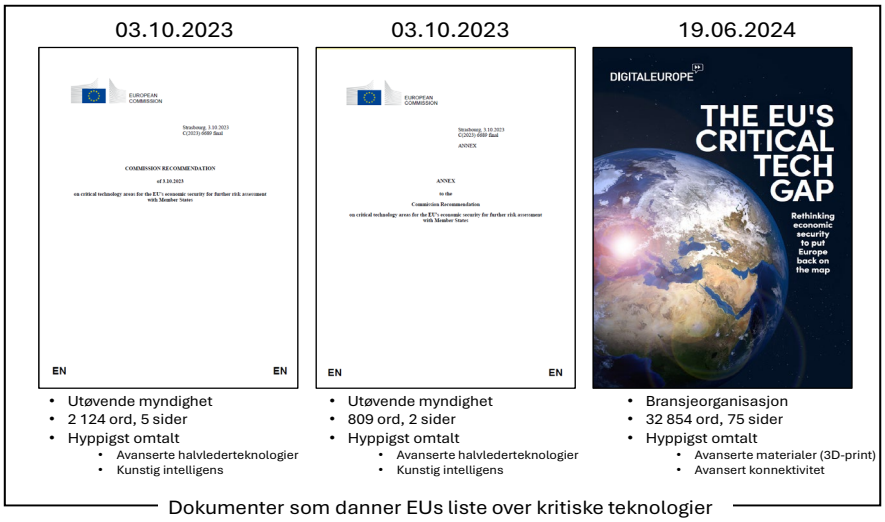
Norske høyere utdannings- og forskningsinstitusjoner holder et høyt internasjonalt nivå innenfor fagfelt med militær relevans, og norske miljøer er derfor sannsynlige mål for fordekte forsøk på å anskaffe kunnskap og teknologi som kan anvendes til militær bruk. I Etterretningstjenestens åpne trusselvurdering *Fokus 2025* påpekes det at fremmede aktører benytter en rekke metoder for å anskaffe og utnytte sivil, vestlig teknologi til militære formål, blant annet ved å delta i internasjonale teknisk-naturvitenskapelige forskningssamarbeid. Videre gjør «demokratisering» av teknologi (at den blir billigere og lettere tilgjengelig) at statlig støttede og ikke-statlige aktører kan spille en disproporsjonal rolle. Å knytte sensitiv teknologi til militær relevans bli derfor essensielt i dette notatet. Det å forstå den militære relevansen av sensitiv teknologi bidrar til å beskytte nasjonale interesser, kritisk kompetanse og norsk infrastruktur samtidig som det fremmer trygt internasjonalt samarbeid og alliansebygging. Dessuten gir det en ramme for den påfølgende risikovurderingen (delleveranse 4 i KVAST-oppdraget) og en videre helhets-vurdering av norsk teknologi og teknologisk kompetanse.

[11] Utenriksdepartementet. (2024). *Arbeidet med å ferdigstille endringer i eksportkontrollforskriften er i sluttfasen*.
[12] Justis- og beredskapsdepartementet. (2018). *Lov om nasjonal sikkerhet (sikkerhetsloven)*.
[13] (Meld. St. 17 (2020-2021), s. 6).

3 EUs liste over kritiske teknologier

EU-dokumentene er utgitt av Europakommisjonen, som er den utøvende delen av EU. Kommisjonen er ansvarlig for å fremme lovforslag for EU-parlamentet, administrere den daglige virksomheten og spiller en nøkkelrolle i å utvikle og implementere politikk og strategier i samråd med medlemslandene. Argumentene EU-kommisjonen bruker for å fremme kritiske teknologier baseres primært på å beskytte og fremme EUs økonomiske sikkerhet. Ved å styrke noen kritiske teknologier kan EU redusere avhengigheten av eksterne leverandører og dermed redusere risikoen for økonomisk tap ved geopolitiske spenninger. Publikasjonene fra EU understreker viktigheten av å holde tritt i det globale teknologiløpet, spesielt mot konkurrenter som USA og Kina.

Ved å forstå hvilke teknologier som er kritiske, kan EU «styre» investeringer og utvikling for å opprettholde eller oppnå teknologisk lederskap. Enkelte teknologier er såkalt flerbruksteknologi (dual-use), det vil si de kan brukes både sivilt og militært, og EU anser det nødvendig å vurdere hvordan slike teknologier kan misbrukes for å undergrave nasjonal sikkerhet, eller resultere i brudd på menneskerettigheter. Listen fra EU gir en struktur for å vurdere risiko for teknologi-lekkasje til aktører som ikke nødvendigvis har samme verdier eller sikkerhetsinteresser som EU-landene. Dette er viktig for å beskytte avansert forsknings- og utviklingsarbeid. Listen fungerer som en veileder for samarbeid mellom medlemslandene i EU og styrker rammeverket for et felles europeisk marked for teknologiutvikling. Ved å klargjøre hvilke teknologier som er kritiske, kan EU og medlemsstatene prioritere ressurser, drive frem forskning og utvikling samt styrke kompetansen innenfor disse områdene. Dette notatet vil presenterer EUs liste over kritiske teknologier som et produkt av tre dokumenter, som illustrert i figur 3.1.



Figur 3.1 Presentasjonen av EUs kritiske teknologier baseres de tre dokumenter, hvorav to kommer fra EU-kommisjonen. DIGITALEUROPE er en bransjeorganisasjon som representerer over 45,000 bedrifter i Europa som representerer et digitalt omforent Europa.

Det er spesielt det midterste dokumentet[14] i figur 3.1 og vedlegget til EU-kommisjonens anbefaling (til venstre), som lister EUs kritiske teknologier. Dokumentet fra bransjeorganisasjonen DIGITALEUROPE presenterer noen av mulige forskjeller i fokus og prioritet av kritisk teknologi mellom kommisjonen og bransjeforeningen. Vedlegget til EU-kommisjonens lister opp ti kritiske teknologi områder som er viktige for EUs økonomiske sikkerhet, og beskriver kort de spesifikke teknologiene som anbefales tatt videre til en risikovurdering. Gitt oppdraget (se innledning) vil dette notatet ta utgangspunkt i disse ti teknologiområdene for videre vurdering opp mot andre lands lister (se kapittel 4).

Det blir understreket av EU-kommisjonen at listen ikke er uttømmende og i hoveddokumentet fra EU-kommisjonen (til venstre i figur 3.1) anbefales det å gjennomføre en risikovurdering på alle de 10 kritiske teknologiområdene. Hoveddokumentet er nært knyttet til vedlegget, men fremhever spesielt prioriteringen av å risikovurdere fire teknologiområder: avanserte halvledere, kunstig intelligens, kvanteteknologi og bioteknologi. I hoveddokumentet begrunnes valget av disse fire teknologiene med militær relevans, nødvendigheten av å ivareta en bred kunnskapsbase (kunnskapsberedskap[15]) og potensialet for flerbruksteknologi (dual-use). Det er spesielt disse fire teknologiområdene som representerer en umiddelbar og høyere risiko for (teknologi)lekkasje og uønsket kunnskapsoverføring til land og aktører som en ikke har formelt sikkerhetssamarbeid med. Basert på disse argumentene vil vi derfor i den påfølgende underkapittel (fra kapittel 3.1 til kapittel 3.10) tilføye tekst som omhandler teknologien i en militær kontekst.

Dokumentet fra bransjeforeningen DIGITALEUROPE gir en detaljert analyse av EUs nåværende posisjon innen kritiske teknologier, hvor de identifiserer hull i konkurranseevne og investeringer sammenlignet med globale ledere som USA og Kina. Dokumentet forsterker prioriteringen på de kritiske teknologiområdene ved å fremheve konkurransegapene, som for eksempel at EU ligger etter i kunstig intelligens og avanserte halvlederteknologier. Det gir en samtidskontekst for teknologiene ved å vurdere hvordan disse påvirker EUs globale posisjon. Det oppfordres til politiske tiltak for å forbedre EUs konkurranseevne gjennom regulatoriske utfordringer, investeringsmangler og rekruttering. Videre diskuteres mulige strategiske tilnærminger for å styrke EUs posisjon i det globale markedet, noe som resonnerer med teknologiene som er listet i vedlegget fra EU-kommisjonen. Dokumentet beskriver også den bredere strategiske rammen for EUs økonomiske sikkerhet og legger vekt på samarbeid med EU-medlemslandene, uten å pålegge landspesifikke risikovurderinger.

De er spesielt to teknologiområder som gjentas og fremheves i alle de tre dokumentene fra EU: avanserte halvlederteknologier og kunstig intelligens. Bransjeforeningen DIGITALEUROPE legger også stor vekt på additiv produksjon og avansert konnektivitet (*advanced connectivity)*, analyserer nåværende status, verdikjede, global konkurranseevne og gir anbefalinger for at EU skal opprettholde og styrke sin posisjon i denne sektoren.

[14] Europakommisjonen, 2023. *Annex to the Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States*
[15] https://www.pahoyden.no/margareth-hagen-rektorbloggen/kunnskapsberedskap-og-dobbelt-brukerpotensial-dual-usage/133096

I underkapitlene som følger vil EUs ti kritiske teknologier presenteres, basert på dokumentene illustrert i figur 3.1. Alle teknologiområdene presenteres med en anbefalt norsk oversettelse og kort forklaring. I tillegg vil hvert enkelt teknologiområde (kort) relateres til en militær kontekst for senere risikovurdering i oppdraget. Alle engelske ord og utrykk av teknologiområdene, brukt fra EU kommisjonen, vil stå i kursiv eller parentes. Avslutningsvis i hvert delkapittel gjøres en opplisting av teknologiene EU-kommisjonen har knyttet til de ulike teknologiområdene. I dette kapitlet gjøres ikke vurderinger om disse teknologiene er utfyllende for teknologiområdet. Slike vurderinger gjøres imidlertid i noen grad i kapittel 5 i dette notatet.

3.1 Avanserte halvlederteknologier

På norsk oversettes *Advanced Semiconductors Technologies* til Avanserte halvlederteknologier. Halvledere er materialer som har elektriske ledningsevner mellom ledere (som kobber) og isolatorer (som glass). Halvlederteknologien er grunnlaget for moderne elektronikk, inkludert datamaskiner, mobiltelefoner og andre digitale enheter.

Avanserte halvlederteknologier gir Forsvaret muligheten til å utvikle mer sofistikerte og effektive systemer, samtidig som de reduserer størrelse og strømforbruk. Dette muliggjør bedre ytelse og effektive løsninger i ulike forsvarsapplikasjoner. Halvledere kan brukes i avanserte sensorsystemer, inkludert radarer og infrarød teknologi, noe som forbedrer muligheten for deteksjon og overvåkning. De er også helt avgjørende i utviklingen og produksjon av høyenergi lasere som ventes å kunne bidra med viktige militære kapasiteter i nær fremtid. Videre kan avanserte halvledere benyttes i GPS-teknologi og andre navigasjonsverktøy, noe som gir mer presis posisjonsbestemmelse og navigasjon.

Avanserte halvlederteknologier inkluderer

- Mikroelektronikk, inkludert prosessorer (Microelectronics, including processors)
- Fotonikk teknologier, inkludert høyenergilaser (Photonics (including high energy laser) technologies)
- Høyfrekvente databrikker (High frequency chips)
- Utstyr for produksjon av halvledere på svært avanserte node-størrelser (Semiconductor manufacturing equipment at very advanced node sizes)

3.2 Kunstig intelligens teknologier

Artificial Intelligence oversettes til kunstig intelligens (KI) på norsk. Det finnes ingen klar autoritativ definisjon av hva som er kunstig intelligens. I forsvarssektorens KI-strategi defineres KI som «maskiners evne til å utføre oppgaver som tradisjonelt krever menneskelig intelligens». KI inngår typisk som en del av et produkt eller system. Det kan derfor være hensiktsmessig å tenke på systemer som bruker KI, heller enn kunstig intelligens isolert sett.

Grovt sett kan dagens kunstige intelligens deles i to grupper – grunnmodeller (foundation models) og spesifikke modeller. Grunnmodeller, for eksempel språk- og multimodalmodellene som ligger bak chatboter som OpenAIs ChatGPT, er laget for å dekke et svært bredt

anvendelsesområde. Det kreves enorme datamengder og beregningsressurser for å bygge slike modeller. Spesialiserte modeller, for eksempel KI som kan tolke innholdet i et bilde, er derimot spisset inn mot et spesifikt og smalt bruksområde, og dermed langt mindre ressurskrevende.

Bruk av KI-systemer gjør Forsvaret i stand til å utnytte store datamengder som ikke lar seg analysere manuelt eller som analyseres langt raskere automatisk, ved å detektere, klassifisere og identifisere interessante objekter eller signaler, eller ved å oppdage endringer. Forsvaret tar også i bruk KI-baserte systemer for språkbehandling, slik som oversettelse, informasjonssøk og automatisert innholdsproduksjon. FFIs forsvarsanalyse 2025 peker på etterretning, overvåking og rekognosering, cybersikkerhet og -operasjoner, samt logistikk og annen støttevirksomhet hvor KI har og vil kunne få stor betydning.[16]

Kunstig intelligens inkluderer

- Høyytelsesdatabehandling (High Performance Computing)
- Sky- og kantdatabehandling (Cloud and edge computing)
- Dataanalyseteknologier (Data analytics technologies)
- Datamaskinsyn, språkbehandling, objekt-gjenkjenning (Computer vision, language processing, object recognition)

3.3 Kvanteteknologier

Quantum Technologies oversettes til kvanteteknologier på norsk. Kvanteteknologier bygger på prinsippene fra kvantemekanikk, som er den delen av fysikken som beskriver oppførselen til svært små partikler som atomer og fotoner.

En kvantebit (*qubit)* er et kvantesystem som kan være i to ulike tilstander. Dette er den minste byggeklossen innen kvanteteknologi, og kan brukes i et bredt spekter av anvendelser.

Kvantedatamaskiner har potensial for eksponentielt høyere hastighet enn en tradisjonell datamaskin og antas på mellomlang sikt å kunne løse komplekse problemer som ikke er løsbare i dag. Dette inkluderer å knekke kryptografiske koder. En kvantedatamaskin må programmeres på en annen måte enn en tradisjonell datamaskin. Fagfeltet kvanteberegninger arbeider med å utvikle algoritmer for dette. Kvantekommunikasjon består både av å overføre informasjon mellom kvantesystemer og muligheten til å overføre kvantenøkler på en sikker måte (*quantum key distribution, QKD)* slik at en fremtidig kvantedatamaskin ikke vil være i stand til å knekke koden. Kvantebitene er normalt ekstremt følsomme for ytre påvirkning, noe som er en stor utfordring innen utvikling av kvantedatamaskiner, men som kan utnyttes i en kvantesensor. Sensorer basert på ulike kvantebiter kan måle en lang rekke forskjellige fysiske parametere, som elektrisk og magnetisk felt, trykk, temperatur og akselerasjon med ekstrem nøyaktighet. Kvantesensorer kan potensielt gi svært god GPS-uavhengig navigasjon og overlegen situasjonsforståelse.

[16] Skjelland et al, 2025. Forsvarsanalysen 2025. FFI-rapport 25/006

Kvanteteknologier inkluderer

- Kvanteberegning (Quantum computing)
- Kvantekryptografi (Quantum cryptography)
- Kvantkommunikasjon (Quantum communications)
- Kvantesensorer og radar (Quantum sensing and radar)

3.4 Bioteknologier

Biotechnologies oversettes til bioteknologi på norsk. Bioteknologi innebærer bruk av biologiske prosesser, organismer, vev, celler eller molekylære komponenter fra levende organismer til å påvirke andre levende organismer, eller ved å intervenere i cellers funksjon eller deres molekylære komponenter, inkludert deres genetiske materiale. Dette feltet spenner over alt fra områder som genteknologi, hvor organismer endres genetisk for å gi ønskede egenskaper, til bruk av mikroorganismer for å produsere kjemikalier og materialer.

Bioteknologi kan også benyttes til å oppdage, diagnostisere og behandle biologiske trusler. Dette inkluderer utvikling av sensorer og tester som kan identifisere biologiske agenter raskt, samt forskning på vaksiner og terapeutiske midler. Videre, ved å bruke genetiske teknikker kan man utvikle organismer som kan bryte ned eller nøytralisere farlige stoffer, noe som er nyttig for dekontaminering, for eksempel etter et bioterrorangrep. Avansert DNA-teknologi benyttes til identifikasjon av patogener og sporing av smitteveier, hvilket er kritisk for rask respons og kontroll ved biologiske hendelser. Bioteknologiske fremskritt gir også mulighet til å utvikle bedre verktøy for overvåkning og håndtering av biologiske agens, og dermed øke sikkerheten i håndteringen av biologiske våpen.

Bioteknologi inkluderer

- Teknikker for genetisk modifikasjon (Techniques of genetic modification)
- Nye genomiske teknikker (New genomic techniques)
- Gen-driv (Gene-drive)
- Syntetisk biologi (Synthetic biology)

3.5 Avansert konnektivitet, navigasjon og digitale teknologier

Advanced connectivity oversettes til avansert tilkobling eller avansert konnektivitet på norsk. Begrepet refererer til moderne teknologier og systemer som gjør det mulig å koble enheter, nettverk og brukere sammen på mer effektive og kraftige måter. Dette omfatter teknologier som 5G-nettverk, som gir høyere hastigheter og lavere forsinkelser for mobilkommunikasjon, samt tingenes internett (IoT), som gjør det mulig for ulike enheter å kommunisere og dele data med hverandre. Avansert konnektivitet spiller en viktig rolle i hvordan samfunnet vårt håndterer informasjon og kommuniserer i en stadig mer digital verden.

Avansert konnektivitet gjør det mulig for militære enheter å kommunisere i sanntid, noe som forbedrer koordinasjon og respons i operasjoner. Ved å koble sammen forskjellige enheter og sensorer kan Forsvaret samle inn og dele informasjon fra flere kilder, noe som gir en omfattende

situasjonsforståelse og forbedrer beslutningsprosesser. Avansert konnektivitet innebærer også forbedrede teknologier for kryptering og sikkerhet som beskytter kommunikasjonen mot avlytting og cyberangrep.

Avansert konnektivitet inkluderer

- Sikker digital kommunikasjon og tilkobling, som RAN og Open RAN (Radio Access Network) og 6G (Secure digital communications and connectivity, such as RAN & Open RAN (Radio Access Network) and 6G)
- Cybersikkerhetsteknologier inkludert cyberovervåkning, sikkerhet og inntrengingssystemer, digital etterforskning (Cyber security technologies incl. cyber-surveillance, security and intrusion systems, digital forensics)
- Tingenes internett og virtuell virkelighet (Internet of Things and Virtual Reality)
- Distribuerte ledgers og digital identitetsteknologi (Distributed ledger and digital identity technologies)
- Veiledning, navigasjon og kontrollteknologier, inkludert avionikk og maritim posisjonering (Guidance, navigation and control technologies, including avionics and marine positioning)

3.6 Avanserte sensorteknologier

Advanced sensing oversettes til avansert sensorteknologi eller avanserte sensorer på norsk. Dette begrepet refererer til bruk av sofistikerte sensorer og teknologier som kan oppdage, måle og analysere ulike fysiske fenomener med høy presisjon og nøyaktighet. Avanserte sensorer benyttes i en rekke anvendelser, inkludert helseovervåking, miljøovervåking, industriell automasjon, sikkerhetssystemer, og autonome kjøretøy. Disse teknologiene muliggjør innsamling av omfattende og detaljerte data som kan brukes til å forbedre ytelsen, sikkerheten og effektiviteten i mange forskjellige systemer og prosesser.

Avanserte sensorteknologier spiller en kritisk rolle i moderne militære operasjoner ved å forbedre deteksjon, overvåking og beslutningstaking. Elektrooptiske, infrarøde og radarsensorer, gir mulighet til å overvåke store områder i sanntid og de kan nøyaktig identifisere og spore mål, noe som er essensielt for å sikre presisjon i Forsvarets operasjoner og minimere risikoen for utilsiktet skade. Avanserte sensorer kan også brukes til å oppdage kjemiske, biologiske, radiologiske og nukleære trusler (CBRN), så vel som eksplosive enheter. Dette bedrer beredskapen og responsen mot slike trusler. Videre kan integrerte avanserte sensorer i droner og andre ubemannede systemer gi bedre autonom kapasitet, slik at disse systemene kan operere effektivt uten direkte menneskelig styring.

Avanserte sensorteknologier inkluderer

- Elektro-optisk, radar, kjemisk, biologisk, stråling og distribuert sensorer (Electro-optical, radar, chemical, biological, radiation and distributed sensing)
- Magnetometre, magnetiske gradiometre (Magnetometers, magnetic gradiometers)
- Undervanns elektriske felt sensorer (Underwater electric field sensors)
- Gravimeter og gradiometre (Gravity meters and gradiometers)

3.7 Romfarts- og fremdriftsteknologier

Space & propulsion oversettes til romfart og fremdrift på norsk. Dette begrepet omfatter teknologier og vitenskap knyttet til utforskning av verdensrommet og metoder for å drive romfartøyer og satellitter. Romfart refererer til utvikling, bygging og bruk av romfartøy og systemer som muliggjør utforskning av det ytre rom, inkludert bemannede og ubemannede romferder. Fremdrift handler om de mekanismene og teknologiene som brukes for å drive romfartøyer, for eksempel rakettmotorer og ionemotorer. Dette feltet er avgjørende for fremtidig romutforskning og utvikling av nye muligheter for transport og forskning i rommet.

Romfart og fremdriftsteknologier har flere viktige anvendelser i Forsvaret, spesielt når det gjelder overvåkning, kommunikasjon og navigasjon. Forsvaret og Forsvarets allierte bruker satellittkommunikasjon for å sikre pålitelige og sikre kommunikasjonslinjer, spesielt i områder hvor tradisjonelle nettverk ikke er tilgjengelige eller er utsatt for forstyrrelser. GPS-satellitter gir nøyaktig posisjonering og navigasjon for militære enheter, noe som er avgjørende for effektiv manøvrering og drift i komplekse operasjoner. Satellitter kan oppdage oppskytning av fiendtlige missiler og spore deres bane, en kritisk evne for å gi tidlig varsling og aktivere forsvarssystemer som eventuelt skal avskjære innkommende trusler. Avanserte fremdriftssystemer er stadig mer avgjørende for fly og missilsystemer, da de gjør det mulig for dem å oppnå høye hastigheter og hurtig manøvrerbarhet, for eksempel banetilpasninger til missiler for å lykkes med å avskjære og nøytralisere innkommende trusler.

Romfarts- og fremdriftsteknologier inkluderer

- Dedikert rombasert teknologi, fra komponent- til systemnivå (Dedicated space-focused technologies, ranging from component to system level)
- Romovervåkning og jordobservasjonsteknologier (Space surveillance and Earth observation technologies)
- Romposisjonering, navigasjon og tidssynkronisering (PNT) (Space positioning, navigation and timing (PNT))
- Sikre kommunikasjoner inkludert konnektivitet i lav jordbane (LEO) (Secure communications including Low Earth Orbit (LEO) connectivity)
- Fremdriftsteknologier, inkludert hypersoniske og komponenter for militært bruk (Propulsion technologies, including hypersonics and components for military use)

3.8 Energiteknologier

*Energy technologi*es oversettes til energiteknologier på norsk. Dette begrepet refererer til de ulike teknologiske systemene som brukes for å produsere, lagre, distribuere og forbruke energi på en effektiv og bærekraftig måte. Energiteknologier omfatter et bredt spekter av områder, inkludert fornybare energikilder som solenergi, vindkraft og vannkraft, samt forbedringer i tradisjonelle energikilder som fossile brensler. Det inkluderer også teknologier for energi-optimalisering, energilagring, som batteriteknologi, og smarte energinett (smart grids) som bidrar til å styre energiforbruk og -fordeling mer effektivt. Målet med energiteknologier er ofte

å redusere miljøpåvirkningen av energibruk og å fremme en overgang til et mer bærekraftig energisystem.

Ved å benytte avanserte energiteknologier kan Forsvaret oppnå større operasjonell fleksibilitet, redusere logistiske utfordringer og styrke sine generelle strategiske kapasiteter i en rekke (strids)miljøer og scenarier. Implementering av fornybare energikilder som sol- og vindkraft kan redusere avhengigheten av tradisjonelle drivstoff-forsyninger, lette logistikkbyrden og gi strøm i avsidesliggende områder. Dette er spesielt nyttig for fremskutte baser og isolerte utposter. Avanserte batteriteknologier og energilagringsløsninger er essensielle for å sikre pålitelig strømtilførsel til ulike militære anvendelser, inkludert bærbar elektronikk, kjøretøy og kommunikasjonssystemer. Utvikling av lette, bærbare strømsystemer gjør det mulig å generere strøm i felt, og sikrer tilgang til essensielt elektronisk utstyr uten å være avhengig av stor infrastruktur. Militære installasjoner kan bruke mikronetteknologi for å forbedre energisikkerhet og opprettholde tilgangen til energi (resiliens). Mikronettverk tillater integrasjon av ulike energikilder og kan operere uavhengig av det sentrale strømnettet og kan dermed gi mer pålitelig energiforsyning under konflikter eller naturkatastrofer.

Energiteknologier kan også integreres i utviklingen av strålevåpen, som laser- og mikrobølge-systemer. Disse våpnene kan gi nye kapasiteter for målretting og engasjement uten å være avhengig av tradisjonelle ammunisjonstyper. Små modulære reaktorer eller andre kjernefysiske teknologier kan gi en stabil og langvarig energikilde for marinefartøy eller avsidesliggende installasjoner, og reduserer behovet for hyppig drivstoffylling. Elektrifisering av militære kjøretøy, inkludert bakkekjøretøy og droner, kan øke operasjonell fleksibilitet, redusere støy og redusere varmesignaturer, og dermed tilby taktiske fordeler i ulike oppdrag.

Energiteknologier inkluderer

- Kjernekraftfusjonsteknologier, reaktorer og kraftproduksjon, radiologisk konvertering/anrikning/resirkulerings-teknologier (Nuclear fusion technologies, reactors and power generation, radiological conversion/enrichment/recycling technologies)
- Hydrogen og nye drivstoff (Hydrogen and new fuels)
- Nullutslippsteknologier, inkludert solenergi (Net-zero technologies, including photovoltaics)
- Smarte nett og energilagring, batterier (Smart grids and energy storage, batteries)

3.9 Robotikk og autonome systemer

Robotics and autonomous systems oversettes til robotikk og autonome systemer på norsk. Robotikk er feltet som omhandler design, konstruksjon, drift, styring og bruk av roboter. Roboter kan være maskiner som utfører oppgaver autonomt eller semi-autonomt og brukes i mange sektorer som industri, helsevesen, tjenester og underholdning. Autonome systemer er systemer som effektivt kan utnytte informasjon fra egne sensorer til å utføre oppgaver de har

fått, gjerne i samarbeid med andre.[17] Systemene kan bruke kunstig intelligens for å finne ut hvor de er, hvor det er mulig å bevege og til å detektere og følge andre objekter. Sammen med annen informasjon bruker de dette til å bestemme hvordan de skal bevege seg, hvor de skal peke nyttelastsensor, hva som skal kommuniseres ol. innenfor gitt handlingsrom. Autonomi-funksjonalitet muliggjør blant annet effektiv og skalerbar utnyttelse av ubemannede systemer ved at det blir mindre ressurskrevende å kontrollere dem, operasjoner i bestridt miljø og oppgaver som krever samarbeid/koordinering mellom farkoster. Eksempler på autonome systemer inkluderer selvkjørende biler, autonome droner og industrielle roboter. Sammen representerer de en viktig del av hvordan vi automatiserer prosesser og skaper smarte maskiner som kan hjelpe til med et bredt spekter av aktiviteter.

Robotikk og autonome systemer tilbyr betydelige strategiske fordeler ved å gjøre Forsvarets operasjoner mer effektive, redusere risiko for menneskeliv og øke fleksibiliteten i en rekke militære operasjoner, men denne utviklingen innebærer også sikkerhetsmessige og etiske problemstillinger. Bruksområder for robotsystemer er blant annet å oppdage og uskadeliggjøre miner, improviserte eksplosive enheter (IED) og andre farlige materialer. Ubemannede farkoster kan blant annet brukes til informasjonsinnhenting (ISR), som våpen og til logistikk, herunder øke effektiviteten og redusere personellbehov, frakte forsyninger og utstyr til frontlinjer eller områder med begrenset tilgang, operere fremskutt tett på fienden og til transport av skadde og sårede.

Robotikk og autonome systemer inkluderer

- Droner og farkoster (luft, land, overflate og undervanns) (Drones and vehicles (air, land, surface and underwater))
- Roboter og robotstyrte presisjonssystemer (Robots and robot-controlled precision systems)
- Exoskjeletter (Exoskeletons)
- KI-aktiviserte systemer (AI-enabled systems)

3.10 Avanserte materialer, produksjons- og resirkuleringsteknologier

Advanced materials oversettes til avanserte materialer på norsk. Dette begrepet refererer til materialer som er utviklet eller modifisert for å ha spesifikke egenskaper eller ytelses-karakteristikker som er bedre enn tradisjonelle materialer. Avanserte materialer brukes i en rekke ulike bruksområder, inkludert elektronikk, romfart, medisin, energi og bygningsindustri. *Recycling technologies* på norsk kalles "gjenvinningsteknologier" eller "resirkulerings-teknologier". Dette begrepet refererer til de teknologiske prosessene og systemene som brukes for å resirkulere materialer og avfall, slik at de kan brukes på nytt i produksjon eller annen bruk. Målet med gjenvinningsteknologier er å redusere avfallsmengder, spare ressurser, og minimere miljøpåvirkningen ved å utnytte eksisterende materialer mer effektivt.

[17] Innenfor RAS er det ulik grad av menneskelig involvering i ulike systemer (f.eks. man in the loop, man on the loop, man out of the loop). Grad av menneskelig involvering er et viktig tema, men i denne sammenheng er det betydningen av hva maskinene klarer å gjøre rent teknologisk som er mest interessant.

Avanserte materialer, produksjon og resirkuleringsteknologier kan betydelig forbedre militære kapasiteter gjennom en rekke anvendelser. For det første, lette og høystyrkematerialer, som avanserte kompositter og legeringer, kan brukes til å produsere militært utstyr og kjøretøy som er lettere og mer holdbare. Dette forbedrer mobilitet og drivstoffeffektivitet samtidig som beskyttelsen, mekaniske egenskaper og yteevnen opprettholdes eller økes. Spesielt muliggjør additiv tilvirkning («additiv manufacturing»; AM) eller 3D-printing helt nye muligheter for geometri- og topologioptimalisering i design, bruk av mer avanserte materialer og kombinasjoner av disse. Det er også mulig å skrive ut (printe) sammensatte mekanismer, eller kombinere flere deler i en enkelt multifunksjonell del. I en bærekraftsammenheng reduserer AM materialforbruk. AM muliggjør produksjon når og hvor det trengs gjennom lokal produksjon eller mobile produksjonsenheter, som blant annet reduserer leveransetid og behov for delelager og transport av reservedeler. Videre kan stealth-teknologier utviklet fra materialer som absorberer eller avleder radar, infrarøde og andre sensorer, gjøre det vanskeligere å oppdage fly, skip og kjøretøy. Smarte materialer, som kan tilpasse seg miljø-endringer, gir også fordeler som adaptiv kamuflasje, selvhelbredende evner og sanntids-overvåkning av personellets helse og status gjennom integrerte sensorer i uniformer eller utstyr.

Avanserte materialer inkluderer

- Teknologier for nanomaterialer, smarte materialer, avanserte keramiske materialer, stealth-materialer, trygge og bærekraftige materialer designet med tanke på sikkerhet og bærekraft (Technologies for nanomaterials, smart materials, advanced ceramic materials, stealth materials, safe and sustainable by design materials)
- Additiv produksjon, inkludert mobile produksjonenheter (Additive manufacturing, including in the field)
- Digitalt kontrollert mikro-presisjon produksjon og småskala laserbearbeiding/-sveising (Digital controlled micro-precision manufacturing and small-scale laser machining/welding)
- Teknologier for utvinning, prosessering og gjenvinning av kritiske råmaterialer (inkludert hydrometallurgisk utvinning, bioutlekking, nanoteknologi-basert filtrasjon, elektrokjemisk prosessering og black mass) (Technologies for extraction, processing and recycling of critical raw materials (including hydrometallurgical extraction, bioleaching, nanotechnology-based filtration, electrochemical processing and black mass))

4 Andre lister over kritiske, sensitive og strategiske teknologier

En føring i dette oppdraget er at man i tillegg til EUs liste over kritiske teknologier skal:

> *«se hen til andre relevante lister, oversikter eller annen relevant kunnskap knyttet til kritiske teknologier av strategisk betydning for nasjonal sikkerhet, utarbeidet f.eks. av NATO og likesinnede land.»*[18].

Videre ble det påpekt at arbeidet med utarbeidelse av den systematiske sammenstillingen bør ses som en fortsettelse av arbeidet som resulterte i vedlegg B: vurdering av fag- og teknologiområder i forbindelse med «modelloppdraget».[19] Vårt utgangspunkt har derfor vært dokumentene som ble gjennomgått i vedlegg B. Dette er blitt supplert av et utvidet søk for å fange opp annen relevant dokumentasjon. For datainnsamlingen fra likesinnede land er det gjort et strategisk utvalg hvor kriteriene alliert tilknytning, antatte likhetstrekk, relevans og tilgjengelighet har vært retningsgivende. Basert på disse utvelgelseskriteriene ble det gjort søk i diverse ugraderte søkemotorer og som resultat gjennomgås lister og oversikter fra følgende land: USA, Canada, Storbritannia, Australia, Sverige, Danmark, Finland og Nederland. Videre inkluderes NATOs «priority technology areas» slik de omtales i NATO STO-rapporten *Science and Technology Trends 2023-2043.*

I hvert av underkapitlene redegjøres det for utsteders uttalte intensjon med dokumentet der hvor denne er tydeliggjort. Deretter oppsummeres hovedinnholdet fra dokumentet. Dette sammenlignes med om, og i så fall, hvordan tilsvarende tematikk er dekket i EU-kommisjonens liste for kritiske teknologier. Dernest påpekes eventuelle teknologiområder og teknologier som dekkes i den enkelte publikasjonen, som ikke dekkes i EUs liste. Avslutningsvis i kapitlet aggregeres en helhetlig oversikt som viser i hvilken grad de ulike dokumentene inkluderer og vektlegger teknologiområdene som omtales i EU-kommisjonens liste over kritiske teknologier.

4.1 NATO

Beskrivelsen av NATOs kritiske teknologier er utarbeidet av NATOs Science and Technology Organization (STO). STO er ansvarlig for å frembringe, dele og anvende avansert vitenskapelig kompetanse og teknologisk utvikling for å støtte NATOs kjerneoppgaver. En viktig del av STO er et nettverk av forskere, analytikere og ingeniører som samarbeider for å håndtere forsvars- og sikkerhetsutfordringer gjennom anvendt forskning og teknologiutvikling. Organisasjonen spiller en kritisk rolle i å sikre at NATO opprettholder sitt teknologiske forsprang ved å gi evidensbaserte råd og innsikt i nye teknologier. Disse rådene hjelper til med å veilede NATOs forsknings- og utviklingsinnsats, samt dens kapabilitetsplanlegging og innovasjonsinitiativer.

[18] Oppdragsbeskrivelse KVAST https://www.forskningsradet.no/contentassets/40eaf18a31fb400cb8134ec4aea5ef57/kvast-oppdragstekst-endelig-versjon-oktober-2024.pdf

[19] Se vedlegg B: Vurdering av fag- og teknologiområder i rapporten Et helhetlig forsyningssystem for åpen, skjermet og gradert forskning

Rapporten vi har valgt fra STO beskriver vitenskapelige og teknologiske trender mot 2043 og deres mulige innvirkning på NATOs militæroperasjoner, forsvarsevne, medlemslandenes forsvarsindustri og deres politiske beslutningstaking.

Overordnet tar rapporten fra STO mål av seg å være et strategisk verktøy for nasjonale beslutningstakere i å forutse det fremtidige sikkerhetsmiljøet og støtte effektiv utvikling av kapasiteter mot medlemslandenes statlige og ikke-statlige motstandere. Det primære målet er å øke forståelsen innad i alliansen om fremvoksende og banebrytende teknologier[20] (EDT) samt veilede NATOs FoU-porteføljestyring, innovasjonsaktiviteter og kapasitetsplanlegging. Rapportene omhandler også hvordan EDTene forventes å utvikle seg de neste 20 årene.

Figur 4.1 Presentasjonen av NATOs kritiske teknologier baseres på ett dokument, hvor begge er utgitt av NATOs Science and Technology Organization (STO).

De kritiske teknologiene er ikke presentert etter viktighet. I stedet blir de diskutert basert på deres relevans for NATOs strategiske interesser, mulige påvirkning og modenhetsnivå. Hver teknologi presenteres med en egen oversikt, som fremhever viktige utviklinger og fremtidige betraktninger innenfor NATOs rammeverk for operasjoner og kapabiliteter. Imidlertid ser vi at kunstig intelligens, robotikk og autonome systemer (RAS) og romteknologier får noe mer oppmerksomhet i dokumentene grunnet deres omfattende anvendelser på tvers av ulike militære funksjoner (flerbruksteknologi) og deres potensial for hurtig påvirkning i militære operasjoner.

NATO STO fremhever ti fremvoksende og banebrytende teknologiområder som kan påvirke NATOs fremtidige operasjoner betydelig.[21] Teknologiene understreker et samlet behov for at

[20] Emerging and Disruptive Technologies (EDT)
[21] Disse er *data, AI, RAS, Space, Hypersonics, Quantum, Biotechnology and human enhancement, Materials, Energy, Electronic & electromagnetic technologies.*

NATO opprettholder sitt teknologiske forsprang og tilpasser sine kapabiliteter til et raskt skiftende globalt miljø.

KI er avgjørende for automatisering av prosesser, dataanalyse og beslutningsstøtte, og kan potensielt revolusjonere militære operasjoner. RAS blir stadig mer integrert i militære operasjoner, og styrker kapasiteter fra overvåkning og rekognosering til kamp mens utviklingen av romteknologier vektlegger utnyttelsen av romressurser for forbedret kommunikasjon, navigasjon og etterretningsinnhenting. Hypersoniske teknologier derimot gir både strategiske muligheter og utfordringer med sine høyhastighetskapabiliteter. Energi- og fremdrifts-teknologier inkluderer effektive energiproduksjons- og lagringsløsninger som er avgjørende for autonome og langvarige systemer.

Elektronikk og elektromagnetisk teknologi er et annet kritisk felt som dekker innovasjon innen elektroniske og elektromagnetiske domene, noe som gir fremskritt innen avanserte sensorer, kommunikasjon og elektronisk krigføring. I tillegg vil kvanteteknologi sikre kommunikasjon og høy-kapasitets databehandling.

Biologiske og menneskelig forbedringsteknologier utnytter biologiske vitenskaper for å forbedre menneskelig ytelse, inkludert medisinske og genetiske fremskritt. Avanserte materialer og avansert produksjonsteknikk bidrar til innovative produksjonsteknikker som 3D- og 4D-printing, noe som kan endre hele logistikk- og produksjonsprosessen i Forsvaret.

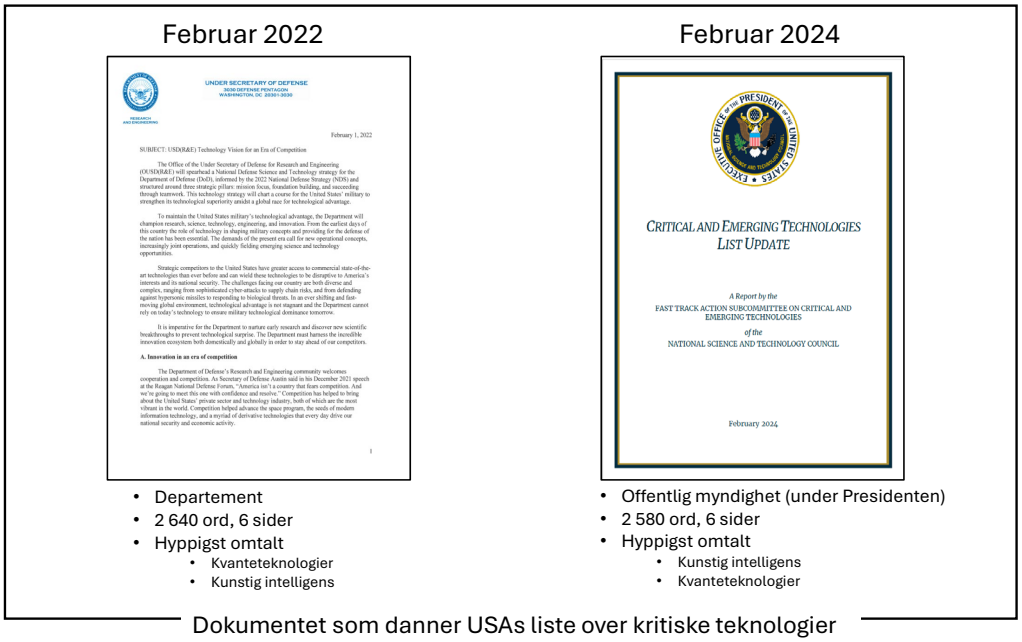
Både NATO STO og EU gir en omfattende og likeverdig oversikt over kritiske teknologi-områder, men NATOs dokument omfatter i større grad spesifikke teknologier som hypersoniske våpen, retningsstyrte energivåpen og romkapabiliteter som ikke er eksplisitt nevnt i EU-rapporten. NATOs fokus på militære anvendelser fremhever disse ulikhetene, noe som gjenspeiler NATOs mål om å opprettholde et teknologisk forsprang innen forsvar og nasjonal sikkerhet.

NATO råder sine medlemsland til å integrere fremvoksende og banebrytende teknologier (EDT-er) i militære kapasiteter for å opprettholde en strategisk fordel. Dette innebærer å forstå de mulige virkningene av disse teknologiene og samarbeide om forskning og utvikling på tvers i alliansen. Etiske og juridiske hensyn er avgjørende, og at det sikres at bruken av EDT-er er i samsvar med internasjonale lover og NATO-standarder. Medlemsland oppfordres til å vektlegge operasjonell integrasjon, investere i innovasjon og utvikle mottiltak mot trusler som følge av motstanderens bruk av EDT-er. Ved å arbeide sammen, har alliansen som mål å forbli teknologisk forberedt og operativt effektiv, adressere utfordringer og gripe muligheter innenfor en stadig skiftende sikkerhetssituasjon.

4.2 USA

Kritisk teknologier i USA baserer seg på to ulike dokumenter. Det første dokumentet *Critical and emerging technologies list* er utgitt fra Det nasjonale rådet for vitenskap og teknologi, det andre dokumentet *Technology Vision for an Era of Competition* er utgitt av det amerikanske forsvarsdepartementet

Det første dokumentet er en rapport utarbeidet av en hurtigarbeidende komité for kritiske og fremvoksende teknologier[22] i Det nasjonale rådet for vitenskap og teknologi (NSTC). Dokumentet gir en oppdatert liste over kritiske og fremvoksende teknologier som anses viktige for USAs nasjonale sikkerhet. Den reflekterer prioritetene og de strategiske målene for å beskytte amerikanske nasjonale interesser, fremme teknologisk lederskap, og ikke minst styrke internasjonalt samarbeid for teknologisk progresjon.



Figur 4.1 Presentasjonen av USAs kritiske teknologier baseres på to dokument, utgitt av NSTC og det amerikanske forsvarsdepartementet.

NSTC-dokumentet ble utviklet gjennom en omfattende tverrsektoriell prosess som involverer eksperter fra flere føderale departementer og skisserer teknologier som er grunnleggende for å opprettholde et fritt, sikkert og velstående samfunn. Innledningsvis gis en kort kontekst om betydningen av kritiske og fremvoksende teknologier for USAs nasjonale sikkerhet og hvordan listen tjener til å informere innsatsen på tvers av regjeringen og spesifikke byråer relatert til teknologisk konkurranseevne og beskyttelse av kritisk teknologi.

Videre listes opp de kritiske og fremvoksende teknologier hvor NSTC fremhever ulike teknologiområder som er spesielt kritisk for nasjonal sikkerhet, inkludert avansert databehandling, kunstig intelligens, bioteknologier, ren energiproduksjon og -lagring, samt kvanteinformasjon og «muliggjørende» teknologier (enabling technologies). For hvert teknologiområde opplistes spesifikke teknologiske aspekter som ekspertene har vurdert.

Det andre dokumentet beskriver hvordan USAs forsvarsdepartement (DoD) planlegger å opprettholde teknologisk overlegenhet i en tid med global konkurranse og et tiltakende

[22] Fast Track Action Subcommittee on Critical and Emerging Technologies of the National Science and Technology Council (NTSC)

teknologikappløp. Strategien bygger på tre hovedpilarer: Oppdragsbasert (mission focus), som skal sikre at teknologiske fremskritt kan brukes til å innfri militære behov; Fundamentbygging (foundation building), som innebærer investering i talent, infrastruktur og modernisering; og suksess gjennom samarbeid (success through teamwork), hvor man utnytter partnerskap med industri, akademia og allierte nasjoner. Dokumentet vektlegger viktigheten av rask innovasjon, operasjonell smidighet og evnen til å møte nye trusler som cyberangrep, hypersoniske våpen og sårbarheter i forsyningskjeder.

Videre identifiserer dokumentet 14 kritiske teknologiområder og kategoriser disse i de tre hovedkategorier: 1) Fremvoksende muligheter (seed areas of emerging opportunity), 2) militær anvendelse av kommersiell teknologi, (effective adoption areas – where there is existing vibrant commercial sector activity) og 3) forsvarsspesifikke områder (defense-specific areas).

Innenfor fremvoksende muligheter listes bioteknologi (Biotechnology), kvantevitenskap (Quantum Science), nestegenerasjons trådløse nettverk (FutureG), avanserte materialer (Advanced Materials). Innenfor militær anvendelse av kommersiell teknologi listes pålitelig KI og autonomi (Trusted AI and Autonomy), integrerte nettverkssystemer (Integrated Network Systems-of-Systems), mikroelektronikk (Microelectronics), romteknologi (Space Technology), fornybar energiproduksjon og lagring (Renewable Energy Genration and Storage), avansert databehandling og programvare (Advanced Computing and Software), menneske-maskin-grensesnitt (Human-Machine Interfaces). Under forsvarsspesifikke områder listes strålevåpen (Directed Energy), hypersonisk teknologi (Hypersonics) og integrert sensor-teknologi og cyberkapasiteter (Integrated Sensing and Cyber). Disse fjorten teknologiområdene er de samme som gjengis i DoDs påfølgende forskning- og teknologistrategi fra 2023.[23]

Hvis en sammenligner den amerikanske listen over kritisk teknologi med EUs liste så gir den amerikanske en mer omfattende og detaljert liste over teknologiske underfelt, som gjenspeiler et bredt spekter av områder avgjørende for USAs nasjonale sikkerhet. Både de amerikanske dokumentene og EU-dokumentene beskriver betydningen av avansert databehandling og halvledere, med fokus på forbedringer innen mikroelektronikk og høyytelsesdatabehandling. Videre er kunstig intelligens fremhevet som kritisk teknologi, og fremhever flerbrukspotensialet (dual-use) på tvers av sivile og militære sfærer grunnet anvendelser innen databehandling, maskinlæring og beslutningsstøttesystemer.

Videre anses kvanteteknologier som avgjørende for deres evne til å revolusjonere samfunnssektorer med innovasjon innen databehandling, kryptografi og kommunikasjon. Dessuten fremhever både USA og EU viktigheten av bioteknologi, og bemerker deres innvirkning på helsevesen, jordbruk og produksjonsprosesser, spesielt med tanke på gen-teknologi og syntetisk biologi. Samsvaret i vurderingen av kritisk teknologi tjener som avgjørende elementer for å opprettholde lederskap i teknologiske progresjon, samfunnssikkerhet og konkurransekraft.

[23] Department of Defense. National Defense Science & Technology Strategy 2023. National Defense Science and Technology Strategy 2023 – DoD Research & Engineering, OUSD(R&E)

De amerikanske dokumentene fremhever også noen kritiske teknologiområder som ikke er eksplisitt nevnt i EU-dokumentene som for eksempel avanserte gassturbinmotor-teknologier relatert til luftfart, maritime og industrielle applikasjoner, med vekt på produksjons- og kontrollteknologier. Videre fremheves avanserte ingeniørmaterialer, spesielt nye materialer og teknikker for egenskapskarakterisering og livssyklusanalyser. Avansert produksjon er også beskrevet i noe mer detalj enn i EU dokumentene, som for eksempel additiv produksjon og bærekraftige, smarte produksjonsteknikker. Dessuten er styrt energi mer detaljert beskrevet, hvor USA vektlegger teknologier som lasere og partikkelstråler. Integrerte kommunikasjons- og nettverksteknologier er også vektlagt i større grad, med vekt på moderne datautveksling, radiofrekvenskomponenter og sikre kommunikasjonssystemer. I tillegg inkluderes posisjonerings-, navigasjons- og tidsbestemte (PNT) teknologier som er kritiske for sikre og forbedre navigasjon og timing (enhanced navigation and timing capabilities). Til slutt diskuteres romteknologier og systemer, med fokus på vedlikehold i rommet, produksjon, motstandsdyktige kommunikasjonssystemer, og teknologier som muliggjør tilgang til nye kretsløp/baner for satellitter (novel orbits and cislunar space).

EU-dokumentene vektlegger mer spesifikt noen få nøkkelteknologiområder, med vekt på deres økonomiske sikkerhet og risikovurdering. Selv om det er det en betydelig overlapp i vektlegging av KI, kvanteteknologier, bioteknologier og avansert databehandling, så er det noe mer variasjon i beskrivelsen av detaljene på kritisk teknologi fra USA. Selv om det er stor overlapp, vektlegger og fremhever de amerikanske dokumentene forsvarssektorens behov. Både EU og USA vektlegger kunstig intelligens, kvantevitenskap, bioteknologi, halvlederteknologi, romteknologi, avanserte materialer, cybersikkerhet og sensorteknologi, men de har ulike tilnærminger. USA vektlegger disse teknologienes betydning for å sikre militær dominans på, med sterk vekt på autonomi, kommando- og kontrollsystemer, samt integrerte nettverk for militære operasjoner. EU fokuserer i større grad på teknologisk uavhengighet og forsynings-sikkerhet, spesielt innen mikroelektronikk, energilagring og resirkulering av kritiske råmaterialer.

Samtidig omtaler de amerikanske dokumentene flere forsvarsspesifikke teknologier som ikke er like fremtredende i EU-dokumentet, slik som hypersoniske våpen, rettet energivåpen (lasere og mikrobølger) og avanserte menneske-maskin-grensesnitt. EU har derimot et bredere perspektiv på propulsjonssystemer, robotikk og bærekraftige materialer, noe som viser en sterkere kobling til både sivil og militær bruk. Begge dokumentene tar for seg cyber- og sensorteknologi, men USA legger større vekt på hvordan disse integreres i forsvarssystemer, mens EU er mer opptatt av digital sikkerhet generelt, inkludert overvåking av cybersystemer og beskyttelse av kritisk infrastruktur.

4.3 Storbritannia

Kritisk teknologi i Storbritannia baseres på tre dokumenter, fra tre ulike institusjoner.

Departement for Science, Innovation and Technology (DSIT) i Storbritannia ble etablert for å utnytte kraften i forskning og utvikling til å drive frem økonomisk vekst, skape høykvalitets-jobber, og legge til rette for banebrytende oppdagelser. For å befeste Storbritannia som en

vitenskaps- og teknologisupermakt innen 2030, koordinerer DSIT innsats på tvers av regjeringen for å dyrke et arbeidsmiljø som er gunstig for innovasjon og teknologisk utvikling. DSIT leder an på flere fronter, inkludert den strategiske utviklingen og implementeringen av kritiske teknologier som kunstig intelligens, ingeniørbiologi, fremtidig telekommunikasjon, halvledere og kvanteteknologier. Disse innsatsene støttes av betydelige investeringer i infrastruktur og talent samt reguleringsutforming med hensikt å fremme et robust F&U-økosystem. Ved å samarbeide med akademia, næringslivet og internasjonale partnere, har DSIT som mål å drive vitenskapelige fremskritt som forbedrer produktivitet, forbedrer offentlige tjenester, stimulerer innovasjon, og sikrer Storbritannias globale lederskap innen vitenskap og teknologi. Gjennom initiativer som *Science and Technology Framework* jobber DSIT for å oppnå en integrering av banebrytende teknologier inn i nasjonen, økonomisk og sosialt.

Innovate UK er Storbritannias innovasjonsbyrå, dedikert til å drive produktivitet og økonomisk vekst ved å støtte bedrifter i utviklingen og realiseringen av nye ideer. Organisasjonen kobler bedrifter med partnere, kunder og investorer for å hjelpe til med å transformere innovative ideer til kommersielt vellykkede produkter og tjenester, og dermed fremme bedriftsvekst. *Innovate UK* tilbyr finansiering for forretnings- og forskningssamarbeid, med mål om å akselerere innovasjon og oppmuntre til investering i forskning og utvikling. Støtten spenner over alle økonomiske sektorer, verdikjeder og regioner i Storbritannia. Som en del av *UK Research and Innovation*, spiller *Innovate UK* en avgjørende rolle i å fremme banebrytende teknologier og hjelpe nasjonen med å opprettholde konkurransekraft i globale markeder.

The Royal Academy of Engineering tar mål av seg å utnytte ingeniørkunstens kraft til å fremme et mer bærekraftig samfunn og en inkluderende økonomi. I samarbeid med sine medlemmer og partnere vektlegger institusjonen det å pleie talent og utvikle fremtidige ferdigheter ved å identifisere utfordringer i en stadig forandrende verden. Det fremmer innovasjon ved å investere i banebrytende ingeniørideer og bygge globale partnerskap som forener ledende ingeniører fra industri, entreprenørskap og akademia. Gjennom *UKs National Engineering Policy Centre* gir akademiet uavhengig ekspertstøtte til britiske beslutningstakere i viktige spørsmål, samtidig som det engasjerer publikum ved å vise frem ingeniørbaserte produkter.

Figur 4.2 Presentasjonen av Storbritannias kritiske teknologier baseres på tre dokumenter, fra tre ulike institusjoner som jobber på vegne av offentlige interesser.

Rammeverket fra DSIT gir en oppdatering på Storbritannias innsats for å bli en vitenskapelig og teknologisk supermakt. Det beskriver fremgang innen forskjellige områder, inkludert investeringer i kritiske teknologier som KI, kvanteteknologi og telekommunikasjon. Dokumentet vektlegger internasjonalt samarbeid, viktigheten av innovative offentlige sektorer, og en integrert tilnærming til infrastruktur, talent og regulering for å oppnå Storbritannias strategiske mål.

Dokumentet fra *Innovate UK* utforsker 50 fremvoksende teknologier som forventes å forme Storbritannias økonomi innen 2040 og utover. *Innovate UK* skisserer ulike teknologitrender, identifiserer fremvoksende teknologi med økonomisk potensial, og gir innsikt fra et bredt spekter av interessenter. Den stimulerer nysgjerrighet omkring spirende sektorer som KI, kvantedatabehandling og bioteknologi, med vekt på bærekraftig, innovativ utvikling.

The Royal Academy of Engineering undersøker tidligere og fremtidig prioritering av teknologi av den britiske regjeringen, med fokus på økonomisk vekst, nasjonal sikkerhet og bærekraft. Det vurderer initiativer som de åtte store teknologiene og fremhever prinsipper for fremtidig prioritering, som vektlegger samarbeid, strategiske kapabiliteter, robuste økosystemer, og balansering av sikkerhets- og økonomiske mål.

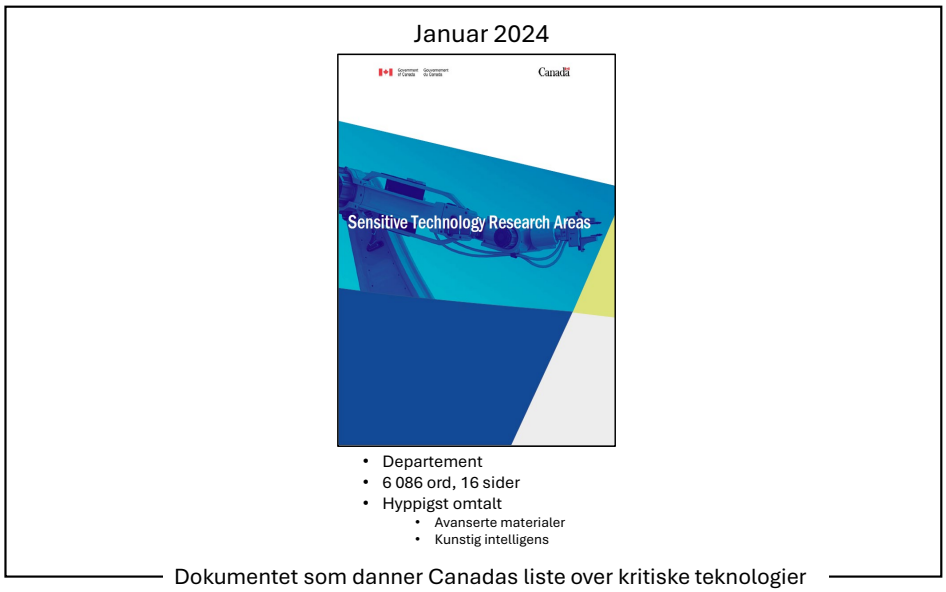
Samlet sett understreker både EU og Storbritannia den strategiske betydningen av avanserte teknologier for å opprettholde økonomisk vekst og sikkerhet, selv om de britiske dokumentene i større grad går inn på spesifikke anvendelser og bredere kategorier av teknologisk innovasjon. Både Storbritannia og EU-dokumentene fremhever flere kritiske teknologier med vidtspennende innvirkning på ulike sektorer. Avanserte halvledere blir fremhevet for deres avgjørende rolle innen databehandling, energi og forsvarsapplikasjoner. Kunstig intelligens (KI) er identifisert

som en nøkkelteknologi med flerbrukspotensial (dual-use) i både sivile og militære domener. Kvanteteknologier er anerkjent for deres store potensial til å revolusjonere ulike samfunnssektorer inkludert kommunikasjon og sensorer. Videre erkjenner både EU og Storbritannia den transformative naturen til bioteknologier innen helsevesenet, landbruk og miljømessig bærekraft, og understreker betydningen i å drive innovasjon i møte med fremtidige utfordringer. De britiske dokumentene nevner også flere unike teknologier sammenlignet med listen fra EU, og understreker deres betydning i ulike samfunnssektorer i Storbritannia. Elektronikk og fotonikk blir fremhevet for deres rolle i telekommunikasjon og nasjonal sikkerhet. Teknisk biologi gis spesiell oppmerksomhet utover standard bioteknologier, med søkelys på biologisk ingeniørkunst og innovasjon innen syntetisk biologi.

Mens EU setter søkelys på avansert konnektivitet som en del av digitale teknologier, utvider Storbritannia denne vektleggingen spesielt til fremtidige telekommunikasjonsteknologier, inkludert 6G. Energi- og miljøteknologier er avgjørende for Storbritannias netto nullvisjon, med kjernefysisk fusjon, hydrogenproduksjon og fornybare energisystemer som spiller en viktig rolle. Robotikk og autonome systemer er bemerket for sine applikasjoner på tvers av forskjellige miljøer, inkludert romfart, mens EU-dokumentene kun indirekte refererer til robotikk under automatisering. Til slutt er det en betydelig vektlegging på avanserte materialer og produksjonsteknologier, essensielt for luftfarts- og bilindustri.

4.4 Canada

Dokumentet med tittelen "Sensitive Technology Research Areas" ble publisert av Canadas regjering, representert ved Departementet for Innovasjon, Vitenskap og Økonomisk Utvikling.



Figur 4.4 Presentasjonen av Canadas kritiske teknologier baseres på ett dokument, utgitt av Canadas regjering.

Det første vi legger merket til er at det kanadiske dokumentet bruker ordet *sensitive teknologier*, mens EU bruker ordet *kritiske teknologier*. Vi viser derfor til diskusjonen i kapittel 2 for betydningen av eventuelle forskjeller og nyanser i begrepsbruken mellom Canada og EU har for den foreslåtte norske definisjonen av *kritiske, sensitive og strategiske teknologier*.

Det kanadiske dokumentet diskuterer avanserte og fremvoksende teknologier som er avgjørende for forskning og utvikling, men som kan tiltrekke interesse fra utenlandske eller ikke-statlige aktører som har som mål å misbruke Canadas teknologiske progresjon. Dokumentet beskriver ulike sensitive teknologiområder, med vekt på behovet for å sikre at Canadas åpne og samarbeidsvillige forskning ikke kompromitterer nasjonal sikkerhet eller forsvar. Samtidig som det er viktig å fremme vekst i disse områdene, er det viktig å sikre at statlig finansiert, åpen og samarbeidsorientert forskning ikke setter landets nasjonale sikkerhet eller forsvar i fare. Det er ment å veilede forskere ved å identifisere områder av teknologisk fremskritt som krever sikkerhetshensyn. I tillegg er det planlagt regelmessige oppdateringer av listen for å reflektere utviklende teknologiområder.

Basert på de fremlagte dokumentene har både Canada og EU identifisert kritiske teknologiområder som er essensielle for nasjonal sikkerhet og økonomisk utvikling. Imidlertid er det forskjeller i vektlegging og beskrivelse av spesifikke teknologier. En utfordring når vi sammenligner dokumentene er at EUs liste er veldig konkret og kortfattet i tabells form, mens Canada-dokumentets listing av kritiske teknologier er noe mer utfyllende representert og diskutert. Avhengig av ordlyden kan det gi inntrykk av at Canada vektlegger enkelte teknologiske områder mer enn EU. Basert på de tilgjengelige dokumentene har både Canada og EU identifisert kritiske teknologiske områder som er essensielle for nasjonal sikkerhet og økonomisk utvikling, selv om det finnes forskjeller i vektlegging og spesifikke teknologier.

Både Canada og EU understreker viktigheten av områder som avanserte halvledere og mikroelektronikk, og fremhever deres betydning for å drive innovasjon og ytelse på tvers av ulike samfunnssektorer. I tillegg anerkjenner både Canada og EU kunstig intelligens og stordatateknologier for deres flerbrukerpotensial (dual-use) i behandling av informasjon og muligheten til å fremme fremskritt innen andre (forsknings)felt. Kvanteteknologier får også oppmerksomhet for sitt fremtidige potensial til å revolusjonere nye systemer og materialer.

Imidlertid nevner det kanadiske dokumentet spesifikke teknologiområder som ikke er detaljert i EU-vedlegget. For eksempel inkluderer Canada avanserte sensor- og overvåkningsteknologier med søkelys på avanserte overvåkningsteknikker, et punkt som er mindre markert i EUs oversikt. Videre går Canadas debatt om avanserte materialer og produksjon nærmere inn på

høy-entropi materialer[24], auxetiske materialer[25] og metamaterialer[26], som har unike egenskaper og anvendelser.

Det er også en merkbar vektlegging på luftfart, rom- og satellitteknologi i den kanadiske listen, med detaljer om tjenesteytelser i bane og avanserte vindtunneler som ikke er beskrevet i EU-dokumentet. I tillegg diskuterer Canada menneske-maskin integrasjonsteknologier, som hjerne-datamaskin-grensesnitt og exoskjeletter, mer inngående enn EU-listingen, som bare nevner eksoskjeletter kort.

Fremhevingen av kategorien *avanserte våpenteknologier*, med referanser til rettet energivåpen og hypersoniske våpen, er et annet område dekket av Canada, men som mangler i EU-dokumentet. De teknologiske fremskrittene innen materialteknologi, produksjon, fremdrift og energi har i betydelig grad brakt nyere våpen som retningsstyrt energi og hypersoniske våpen nærmere operativ virkelighet. I tillegg har innovasjoner innen nanoteknologi, syntetisk biologi, kunstig intelligens og sensorteknologier forbedret eksisterende våpen, inkludert biologiske og kjemiske våpen, samt autonome våpensystemer.

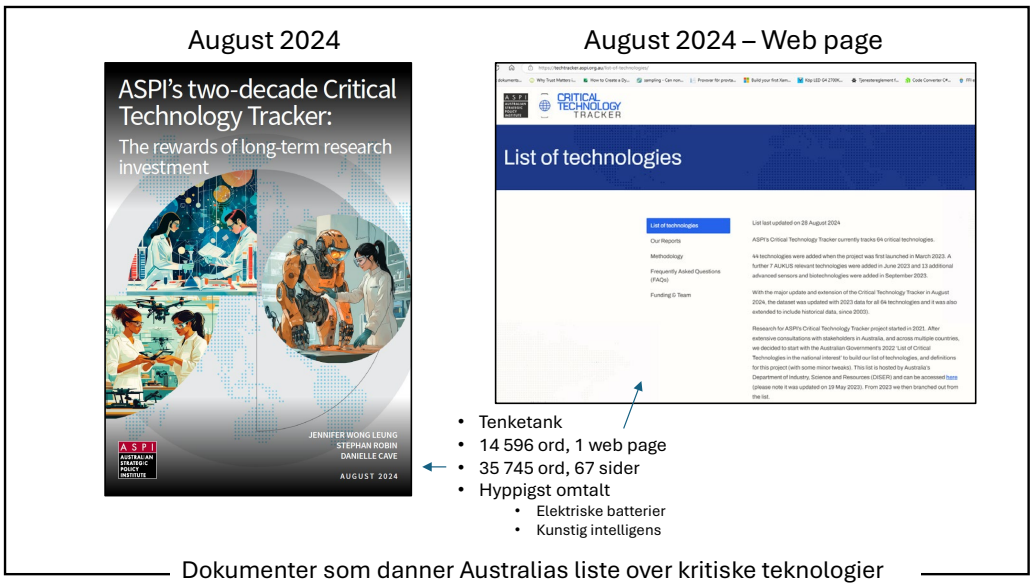
Vektleggingen på dette området understreker Canadas bekymring for de strategiske implikasjonene av slike teknologier og fremhever utfordringer med flerbruksteknologi (dual-use) der sivil teknologi også kan anvendes for militære formål. Canada-dokumentets omtale av utviklingen av avanserte våpen signaliserer Canadas proaktive holdning for å beskytte nasjonal sikkerhet samtidig som de fremmer teknologiske kapasiteter innen eget forsvar. Denne tilnærmingen bidrar vedvarende årvåkenhet mot trusler som kan oppstå fra (teknologi)lekkasje eller misbruk av kanadisk teknologisk fremskritt innen våpenteknologi av utenlandske aktører en ikke har sikkerhetssamarbeid med.

Videre vektlegger Canada medisinske fremskritt innen nanomedisin og genterapi, noe som utvider den generelle bioteknologi-kategorien fra EU. Generelt, selv om det er overlapp, detaljerer Canadas omfattende liste ytterligere aspekter og spesifikke underkategorier som indikerer et bredere interesse- og bekymringsområde sammenlignet med EU.

[24] Høyentropiske materialer, inkludert legeringer og oksider, består av flere hovedelementer, ofte fem eller flere, i lignende konsentrasjoner, i motsetning til tradisjonelle legeringer som domineres av ett eller to elementer. Denne unike sammensetningen forbedrer egenskaper som styrke, seighet og korrosjonsmotstand. På grunn av deres unike atomstrukturer er disse materialene egnet for krevende anvendelser i sektorer som luftfart og energi, og de er en del av en bredere forskningskategori av avanserte materialer for høyverdianvendelser (high-value applications).
[25] Materialer med auxetiske egenskaper er unike ved at de har en negativ Poissons forholdstall, noe som betyr at de utvider seg sideveis når de strekkes og blir tynnere når de komprimeres, motsatt av de fleste materialer. Dette skyldes deres spesielle indre struktur. Som et resultat utviser de økt energiabsorpsjon, høy bruddmotstand og forbedret fleksibilitet, noe som gjør dem verdifulle for anvendelser i beskyttende utstyr, medisinske implantater og komponenter i romfartsindustrien. De er en del av kategorien avanserte materialer som utforskes for innovative bruksområder på tvers av sektorer.
[26] Metamaterialer er konstruert på mikro- eller nanoskala for å ha egenskaper som mangler i naturlige materialer, og påvirker elektromagnetiske bølger som lys, lyd og varme på en unik måte. De kan manipulere disse bølgene for å oppnå negativ refraksjon, superlinser eller tilsløring, slik at objekter blir mindre synlige for sensorer. Denne unike interaksjonen gjør dem verdifulle for anvendelser innen optikk, akustikk, telekommunikasjon og medisinsk bildebehandling, og tiltrekker seg betydelig forskningsinteresse.

4.5 Australia

Listen over kritiske teknologier fra Australia er laget av *Australian Strategic Policy Institute* (ASPI) som ble grunnlagt i 2001. ASPI er en uavhengig, tverrpolitisk tenketank spesielt opprettet for å informere den australske regjeringen om forsvar, sikkerhetspolitikk og strategiske spørsmål. ASPI fokuserer på å generere innovative ideer og fremme offentlig debatt om et bredt spekter av emner, herunder kritisk teknologi.



Figur 4.5 Presentasjonen av Australias kritiske teknologier baseres på to dokumenter, fra ASPI som jobber på vegne av den australske regjeringen.

ASPIs Two-Decade Critical Technology Tracker: The Rewards of Long-Term Research Investment, gir en oppdatering av ASPIs nettbaserte oppslagsverk i perioden 2003 til 2023 og belyser spesielt endringer i global forskningsledelse. Dokumentet fremhever Kinas ledelse i 57 av de 64 teknologiene og analyserer trender og måleparametere knyttet til risiko for teknologisk monopol. Dokumentet gir også innsikt i landskapet av teknologiske kapasiteter og strategisk planlegging, og oppmuntrer til informerte beslutninger. Nettsiden som ASPI henviser til gir en oversikt over teknologiene som følges opp av tjenesten *ASPI Critical Technology Tracker*, som for tiden inneholder 64 kritiske teknologier. Opprinnelig lansert i mars 2023 med 44 teknologier, ble det gjennom ytterligere oppdateringer økt til 64 i september 2023. Nettsiden beskriver prosjektets metodikk, viktigheten av å spore disse teknologiene, og en definisjon av kritiske teknologier. Nettsiden fungerer som et åpent tilgjengelig oppslagsverk som «overvåker» trender innenfor kritiske teknologier og deres innvirkning på (australske) nasjonale interesser.

Ett første inntrykk er at ASPI har identifisert veldig mange flere teknologier (64 stk) enn listen fra EU (10 stk). Imidlertid har ASPI kategorisert de 64 teknologiene i ni hovedkategorier og EU har EU 4–5 teknologier for hver kritisk teknologi (42 stk totalt). ASPI omtaler også noen av teknologiområdene som mer kritiske enn andre på grunn av deres mulige innvirkning på nasjonal sikkerhet, økonomisk velstand og sosial samhørighet. ASPI identifiserer noen

teknologier som ekstra kritiske fordi de har kapasitet til å betydelig forbedre eller utgjøre risiko for et lands nasjonale interesser. Noen av disse teknologiene fremheves også på grunn av deres flerbrukskarakter (dual-use) og dette gjør dem til fokus for geopolitisk og strategisk konkurranse. Teknologier med høy "teknologimonopolrisiko", det vil si at de domineres av et enkelt land innen forskning med stor innvirkning, kan også betraktes som spesielt kritiske da deres kontroll kan føre til betydelige strategiske fordeler eller sårbarheter. Følgende teknologier anses som svært kritiske fordi de har betydelige militære eller strategiske anvendelser, og det er en bekymring for monopol i forskning med høy innvirkning, spesielt av land som Kina.

- Avanserte flymotorer (inkludert hypersoniske)
- Droner, sverm og autonome roboter som samarbeider
- Avansert optisk kommunikasjon
- Avansert trådløs kommunikasjon under vann
- Elektriske batterier[27]
- Superkondensatorer
- Kvantumkommunikasjon og sensorer
- Radar
- Hypersonisk deteksjon og sporing

V legger merke til at ASPI lister opp noen teknologier som "mer kritiske" enn andre som følge av geopolitisk betydning, potensielle implikasjoner for nasjonal sikkerhet, og risiko for monopolisering fra ett land man ikke har sikkerhetssamarbeid med. Selv om for eksempel kunstig intelligens (KI) er vurdert som ekstra kritisk av EU og andre land, basert på argumentet om flerbrukteknologi, har ASPI identifisert teknologier som "mer kritiske" basert på dens direkte og umiddelbare implikasjon for forsvaret og strategiske kapabiliteter. Dette under-vurderer ikke betydningen av KI, men fremhever vektleggingen og ASPIs analyse av risiko-faktorer knyttet til monopolisering og strategisk konkurranseevne for teknologier som har direkte påvirkning på nasjonal sikkerhet.

Når vi sammenligninger ASPIs og EUs liste over kritiske teknologier ser vi at begge listene anerkjenner kritiske teknologiområder som kunstig intelligens, kvanteteknologi og bioteknologi. Både ASPI og EU fremhever teknologiske spesifikasjoner som har betydning for regionale strategiske prioriteringer, men ASPI vektlegger i større grad avanserte materialer, forsvars-materiell og energi, mens EU vektlegger avansert konnektivitet og romteknologi.

Både ASPI og EU understreker betydningen av kunstig intelligens og fremhever teknologier som maskinlæring, naturlig språkbehandling og dataanalyse som avgjørende for økonomisk sikkerhet og med transformative effekter. Kvanteteknologier, inkludert kvantedatabehandling, kommunikasjon og avansert sensorteknologi, blir også fremhevet for deres transformative potensial. Bioteknologier, spesielt genetisk og syntetisk biologi blir omtalt og deres betydning for innovasjon innen helse og landbruk fremheves, samtidig som mulige sikkerhetsrisikoer

[27] Uttrykket "elektriske batterier" refererer spesifikt til enheter som lagrer og frigjør elektrisk energi gjennom kjemiske reaksjoner. Selv om alle batterier lagrer energi kjemisk, brukes uttrykket "elektriske batterier" ofte for å understreke deres anvendelse i lagring og frigjøring av elektrisitet til ulike formål som å drive elektriske kjøretøy, forbrukerelektronikk og fornybare energilagringssystemer.

påpekes. I tillegg diskuterer både ASPI og EU avanserte halvlederteknologier, og anerkjenner deres kritiske rolle innen fremtidens elektronikk og databehandling.

Sammenlignet med EU nevner ASPI flere kritiske teknologier som understreker deres spesielle relevans for forsvars- og industriprogrammer. Avanserte materialer og produksjon, inkludert 3D-printing, avanserte kompositttmaterialer og nanoskala materialer, for å nevne noen. I tillegg tar ASPI for seg energi- og miljøteknologier fra elektriske batterier, hydrogen og ammoniakk til energi, og solceller, og fremhever spesielt deres avgjørende rolle i energi-overgangen og nasjonal energisikkerhet. Innenfor området avansert sensorteknologi, timing og navigasjon, nevnes teknologier som treghetsnavigasjon og multispektral bilde-behandling for deres militære anvendelser. Videre understreker ASPI viktigheten av autonomi- og robot-teknologier, spesielt avanserte flymotorer, droner og robotikk.

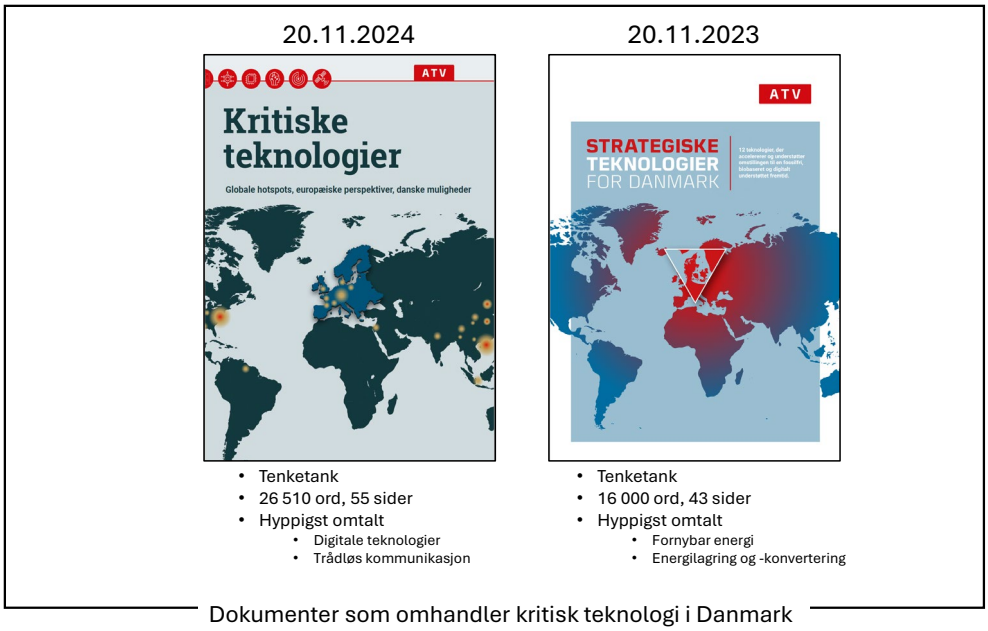
Sammenlignet med ASPI fremhever EU kritisk teknologi innen romfart og fremdrift, som omfatter rombaserte teknologier, sikre kommunikasjonsmidler og fremdriftssystemer, inkludert hypersoniske systemer. I tillegg legger EU i større grad vekt på avansert konnektivitet, som dekker sikre digitale kommunikasjonsmidler og cybersikkerhetsteknologier, samt neste generasjons tilkoblingssystemer som 6G. Innenfor robotikk og autonome systemer vektlegges droner og KI-aktiverte systemer, autonomi og presisjon.

4.6 Danmark

I Danmark foreslås det å utvikle en nasjonal strategi som inkluderer EUs prioriteringer, basert på å fremheve de danske teknologifeltene som styrker økonomien, sikkerheten og samfunnets motstandskraft (resiliens). Den danske tenketanken ATV[28] har siden 1 desember 2022 påtatt seg et femårig prosjekt for å styrke Danmarks teknologiske infrastruktur mot en mer bærekraftig fremtid. Prosjektet er finansiert av alle de åtte universitetene i Danmark og fem fond[29]. Målet er å styrke Danmarks økonomi, konkurranseevne, selvstendighet og velferd ved å optimalisere landets vitenskaps- og ingeniørøkosystem.

I prosjektbeskrivelsen[30] fremheves tre teknologiske transformasjonstrender som anses som avgjørende for en bærekraftig utvikling; Fornybare teknologier, Biobaserte teknologier og digitale teknologier. Prosjektet har gitt ut en mengde rapporter og artikler, men til dette notatets formål har vi valgt å se nærmere på to dokumenter fra ATV, som illustrert i figur 4.6. Begge dokumentene i er utarbeidet som en del av ATV's prosjekt "Guide til et resilient Danmark" og har til hensikt å fremme Danmarks posisjon innen kritisk teknologier, med utgangspunkt i EUs liste.

[28] Akademiet for de Tekniske Videnskaber
[29] Novo Nordisk Foundation, Villum Fonden, Poul Due Jensen Foundation (Grundfos), Rambøll Fonden og NIRAS Alectia Fonden. Prosjektet har ett budsjett på ca. 50 mill. DKK (ca. 80 mill NOK).
[30] https://atv.dk/udgivelser-viden/resume-guide-til-resilient-danmark



Figur 4.3 Presentasjonen av kritiske teknologier i Danmark baseres på to dokument, hvor begge er utgitt av tenketanken ATV.

Dokumentet «Strategiske teknologier» fra 2023 fremhever på de 12 strategiske teknologifeltene som anses avgjørende for Danmarks fremtid, med en sterk vekt på anvendelsene for Danmarks økonomi og motstandskraft (resiliens) gjennom teknologisk utvikling og eksportpotensial. Det andre dokumentet fra 2024, «Kritiske teknologier», handler mer om det europeiske perspektivet og Danmarks muligheter innen de konkrete teknologifeltene EU har definert som kritiske for nasjonal sikkerhet og økonomi, inkludert teknologiens rolle i den geopolitiske konteksten. Begge dokumentene er basert på analyser og vurderinger fra fagpersoner og samarbeids-partnere i ATV, men de har ulike inngangsverdier basert på konteksten som adresseres.

Til forskjell fra EU-kommisjonens mer detaljerte dokumentasjon av de ti spesifikke teknologiområdene presenterer ATV de kritiske teknologiområdene i forhold til Danmarks økonomi og motstandsdyktighet (resiliens). For eksempel presenterer EU-kommisjonen bioteknologi som genetisk modifikasjon og manipulering av biologisk materiale mens ATV omtaler bioteknologi i konteksten av bærekraftig produksjon og biobaserte produkter.

I dokumentet «strategiske teknologier» fremhever ATV 12 teknologifelter som er avgjørende for Danmarks fremtid og landets overgang til et fossilfritt, biobasert og digitalt understøttet samfunn. Denne omtalen tar sikte på å styrke Danmarks konkurranseevne og motstands-dyktighet (resiliens). Dokumentet deler de strategiske teknologiene inn i tre kategorier: fossilfrie, biobaserte og digitalt understøttede teknologier. For den fossilfrie fremtiden nevnes fornybar energi, energilagring og -konvertering, landbruksteknologi og grønn transport som viktige teknologiområder. Innen biobaserte teknologier fremheves biomedisinske teknologier, nye ingredienser og proteinkilder, bioteknologisk produksjon og bioenergi og bærekraftige brensler. I den digitalt understøttede fremtiden fokuseres det på robotteknologi, kvanteteknologi og smart infrastruktur. Rapporten argumenterer videre for at Danmark har gode forutsetninger

for å utvikle og eksportere teknologiløsninger globalt og understreker viktigheten av politisk støtte for å dra nytte av de strategiske teknologiområdene.

Begge dokumentene fra Danmark omtaler også militære eller forsvarsrelaterte aspekter. I dokumentet "Kritiske teknologier" diskuteres hvordan kritiske teknologier kan ha både sivile og forsvarsmessige anvendelser, og det foreslås at Danmark, i likhet med EU, NATO og Storbritannia, bør forholde seg til flerbruksteknologier som har betydning for både sivile og forsvarsmessige formål. Dokumentet nevner også NATOs initiativer for innovasjon og transatlantisk samarbeid om teknologier. I det andre dokumentet "Strategiske teknologier" er militære aspekter nevnt i forbindelse med kvanteteknologi, spesielt i forhold til sikkerhet og forsvar. Det beskriver hvordan kvanteteknologi kan spille en rolle i sikkerhets- og forsvars-aspekter og nevner Danmarks posisjon i kvanteteknologisk forskning med støtte fra NATO gjennom etableringen av et kvante-samarbeid i København.

EU-kommisjonen fremhever spesifikke teknologier som avanserte halvledere (inkludert mikroelektronikk og fotonikk), og teknikker for genetisk modifikasjon og cybersikkerhets-teknologi, noe som er mindre fremtredende i de danske dokumentene fra ATV. EU-dokumentet inkluderer også teknologier for romovervåkning og hypersoniske framdriftsteknologier. På den andre siden fremhever de danske dokumentene teknologier som bioteknologisk produksjon og robotteknologi med vekt på posisjonering i det globale markedet, noe som reflekterer Danmarks prioritering av den kritiske teknologien.

4.7 Sverige

Vinnova har på oppdrag fra den svenske regjeringen i 2024 ledet et arbeid med å identifisere og foreslå strategiske teknologier for Sverige.[31] EUs liste over kritiske teknologier for økonomisk sikkerhet har vært utgangspunkt for kunnskapsgrunnlaget, men målsettingen med arbeidet har vært å vurdere hvilke av disse teknologiområdene som er særskilt viktige for Sverige.

[31] Vinnova (2024). Strategiska tekniker för Sverige Ett underlag för nationella prioriteringar. Strategiska tekniker för Sverige

Figur 4.4 Presentasjonen av kritiske teknologier i Sverige baseres på ett dokument fra Vinnova – en statlig myndighet underlagt det svenske Næringsdepartementet

Anbefalingene er basert på hvilke teknologiområder som anses kritiske for store transformasjonsprosesser med sentral betydning for Sverige og er ment å sikre satsinger på teknologiforskning og innovasjon som kan være til fordel for både Sverige og Europa, med fokus på økonomisk sikkerhet, konkurranseevne og produktivitet. Satsningene skal også underbygge nasjonal sikkerhet, motstandskraft og bærekraftig omstilling.

Ifølge rapporten fra Vinnova er flere teknologiområder identifisert som strategisk viktige for Sverige. Disse er viktige på grunn av deres potensiale til å bidra til økonomisk vekst, samfunnsomstilling og for å adressere globale utfordringer. Spesielt (1) kunstig intelligens og autonome systemer fremheves som avgjørende for innovasjon og effektivitetsforbedring i samfunn og industri. De har et bredt spekter av anvendelser, fra transport til helsevesen, og er kritiske for fremtidens digitale økosystemer. Videre fremheves, i prioritert rekkefølge, følgende teknologiområder: (2) avansert digital teknologi for produktivitet og sikkerhet, (3) kvanteteknologi for sikkerhet og industrielle anvendelser, (4) energiteknologi for fossilfri elektrifisering, (5) material- og produksjonsteknologi for omstilling og bioteknologi for helse og klimaomstilling (6). Disse områdene er også valgt på bakgrunn av deres evne til å gi høy økonomisk avkastning, styrke nasjonal sikkerhet og gi løsninger for miljømessige og sosiale utfordringer. Teknologiområdene gir muligheter for å lede an internasjonalt og styrker Sveriges innovasjonsevne.

For vårt arbeid er det interessant å bemerke seg rapportens kommentar om det de anser som mangler på EUs liste, gitt svenske behov og kontekst. For eksempel så legger Sverige vekt på sin evne til å utvikle komplekse systemløsninger der ulike systemer slås sammen (system-av-

system). Dette kan ses som en svensk styrke spesielt innenfor industrier som tele-kommunikasjon, transport og forsvar. Sverige satser også på domenespesifikke KI-løsninger, spesielt innen sektorer hvor landet har sterke industrielle økosystemer som produksjon, kjøretøyer, gruvedrift, og skogindustri. Videre så legges det betydelig vekt på energiteknologi for fossilfri elektrifisering, noe som inkluderer smarte kraftnett, batteriteknologi, og hydrogen. Selv om EU også dekker mange av disse teknologiene, kan energitransisjon være spesielt avgjørende for Sveriges strategi. Sverige anerkjenner også en sterk forskningsbase innen materialteknologi, hvor de fremhever innovasjon for sirkulær økonomi og bærekraftig produksjon. Avslutningsvis kan det nevnes at Sverige også fremhever viktigheten av synergier mellom teknologiområder som helt fundamentalt for å utvikle nye løsninger (radikalt forbedrede).

Rapporten fra Vinnova understreker også viktigheten av teknologisk utvikling for nasjonal sikkerhet og forsvarsformål. Flere teknologiområder er spesielt fremhevet med tanke på deres betydning for forsvarsindustrien og nasjonal sikkerhet. For eksempel så fremheves kvante-teknologiens potensial for sikker kommunikasjon og kvantresistent kryptering som viktige områder for nasjonal sikkerhet. Videre så omtales autonome systemer (robotikk og droner) og viktigheten av satellittbaserte teknologier, som posisjonering, navigasjon og tidssynkronisering (PNT), som er kritiske for militære anvendelser. Sensorer for overvåking og sikkerhet, inkludert militære applikasjoner, er også nevnt. Rapporten anbefaler videre å prioritere betydningen av fremtidige samarbeidsprogrammer for utvikling og bruk av banebrytende teknologi i både sivil og militær kontekst – for å styrke Sveriges forsvarsevne og nasjonale sikkerhet, spesielt i NATO-samarbeidet.

Ifølge Vinnova må Sverige øke de statlige FoU-midlene til over 1 prosent av BNP innen 2030 for at Sverige skal styrke sin posisjon innen viktige teknologiområdene. Dette innebærer en økning av de statlige FoU-bevilgningene med minst 20 milliarder svenske kroner sammenlignet med 2024. Denne investeringen skal bidra til å sikre Sveriges konkurransekraft og økonomiske sikkerhet i en økende internasjonal konkurranse.

4.8 Finland

I en request for information (RFI) besvart av det finske forsvarsdepartementet kom det frem at det pågår arbeid for å oppdatere finsk politikk på kritiske teknologier, og at man i hovedsak legger til grunn listene fra EU og NATO. Den gjeldende strategiske policyen[32] finner man i Finlands forsvarspolitiske «hvitbok» fra desember 2024. I svaret fra det finske forsvars-departementet ble det også henvist til et eldre dokument fra 2016 som omhandlet finsk forsvarsindustriell kapasitet og teknologiske base.[33] I tillegg har vi funnet frem et dokument som i større grad omhandler bredden av kritisk teknologi i Finland, eller rettere sagt «Utenlandske investeringer og kritisk immateriell eiendom[34]», som er utgitt fra statsministerens

[32] Kan sammenlignes med forsvarsdepartementets langtidsplan, før den behandles av Stortinget.
[33] Det finske forsvarsdepartementet (2016)
Suomen_puolustuksen_teknologisen_ja_teollisen_perustan_turvaaminen.pdf
[34] Ulkomaiset investoinnit ja kriittinen aineeton omaisuus

kontor (Statsrådets kansli). Dette er det eneste Finske dokumentet henviser spesifikt til EUs liste over kritiske teknologier.

Figur 4.5 Presentasjonen av Finlands kritiske teknologier baseres på tre dokumenter, hvorav to fra Forsvarsdepartementet og ett fra Statsministerens kontor.

I dokumentet fra 2016 omtales Finlands forsvarsteknologiske og industrielle grunnlag. Det er et beslutningsgrunnlag, fra det finske forsvarsdepartementet, som beskriver hvordan Finland bør gå frem for å opprettholde og utvikle sin teknologiske og industrielle kapasitet som støtter nasjonal forsvars- og sikkerhetspolitikk. Dokumentet dekker ulike tema som er viktige i forsvarssektoren uten at vi går nærmere inn på disse.

Imidlertid kan vi fremheve omtalen av kritiske teknologier, det vil si teknologier som er avgjørende for Forsvarets effektivitet og evne til å operere selvstendig. Her fremheves C4ISTAR[35] kapabiliteter, avanserte materialer og konstruksjonsteknologier, avanserte sensorer, autonome systemer og teknologier for systemdefinisjon, design, integrasjon og livssyklus-administrasjon samt teknologier for beskyttelse mot kjemiske og biologiske trusler. Dokumentet legger vekt på å opprettholde Finlands evne til å selvstendig administrere og utvikle de teknologiske og industrielle ressursene som er nødvendig for et effektivt forsvar.

I det gjeldende strategiske policy dokumentet, publisert av det finske forsvarsdepartementet i desember 2024, fremheves spesielt cybersikkerhetsteknologi i sammenheng med å beskytte

[35] C4 er en forkortelse for command, control, communications and computer (kommando, kontroll, kommunikasjon og datamaskiner). ISTAR er en forkortelse for Intelligence, Surveillance, Target Acquisition and Reconnaissance (etterretning, overvåking, målanvisning og oppklaring). C4 og ISTAR kan brukes i tekst hver for seg, eller slått sammen.

nasjonal sikkerhet, motvirke trusler og sikre beredskap i henhold til NATOs krav. Videre fremheves behovet for et integrert luft- og missilforsvar i sammenheng med Finlands forpliktelse som en del av NATO og (sikre interoperabilitet med) NATOs systemer. Imidlertid understreker det strategiske policy dokumentet at alle teknologiområdene er avgjørende for å opprettholde et forsprang innen forsvar, og derfor ikke rangerer det eksplisitt. Teknologi-områdene er integrerte for å sikre nasjonal sikkerhet, forbedre militære kapasiteter og sørge for teknologisk beredskap.

Imidlertid omtaler det gjeldende strategiske policy dokumentet flere kritiske teknologier med mulig transformative effekter på forsvarsevner. Kunstig intelligens blir trukket frem for sin evne til å revolusjonere krigføring og beslutningsprosessen. Utviklingen av autonome og ubemannede systemer, spesielt fjernstyrte enheter, blir identifisert som et sentralt fokusområde. Romteknologi anses som avgjørende for å forbedre situasjonsforståelse, etterretningsinnhenting og håndtering av trusler som oppstår fra eller i verdensrommet. I tillegg blir kvanteteknologi anerkjent som et av de fremvoksende og banebrytende feltene som krever oppmerksomhet på grunn av mulige nyvinninger innen kryptografiske metoder og sikker kommunikasjon. Til slutt erkjennes også bredere kategorien av fremvoksende og banebrytende teknologier, som augmentert kognisjon og syntetisk biologi.

I dokumentet fra statsministerens kontor (SMK), det eneste som spesifikt referer og henviser til EUs liste over kritisk teknologi, spesifikt de såkalte *Key Enabling Technologies*. Vi ser at det er et betydelig samsvar mellom hvilke teknologier som anses som kritiske i Finland og i EU. Det legges vekt på avanserte teknologier som mikro- og nanoelektronikk, kunstig intelligens og bioteknologi. SMK peker også på områder som fotonikk, kvanteteknologi og cybersikkerhet som viktige for Finland, noe som overlapper med EUs fokusområder. Både Finland og EU er opptatt av teknologier som muliggjør avanserte produksjonsmetoder og opprettholder teknologisk suverenitet i møte med internasjonal konkurranse.

Dette er i tråd med EUs overordnede mål om strategisk autonomi og teknologisk suverenitet. Finland ser ut til å tilpasse sine nasjonale strategier etter disse prioriteringene for å identifisere hvilke teknologier som er kritiske for landets fremtidige konkurranseevne og sikkerhet. Kvanteteknologi og helseteknologi får også mye oppmerksomhet i den finske konteksten, noe som kan skille seg litt fra prioriteringer i EUs liste over kritiske teknologier. På den annen side, EU fokuserer også på avanserte halvlederteknologier, kvanteteknologier og bioteknologier, men med en mer bred tilnærming til hvordan hver teknologi påvirker økonomien og samfunns-sikkerheten. SMK nevner spesifikt at Finlands tilnærming kan tilpasse seg til lokale prioriteringer og nasjonale behov, mens EU sikrer en koordinert innsats mellom medlems-landene.

4.9 Nederland

Nederland har i sin nasjonale teknologistrategi, skrevet av *Ministry of Economic Affairs and Climate Policy,* identifisert ti nøkkelteknologier der nederlandsk kunnskap kan gi et komparativt fortrinn, styrke økonomiske og teknologiske konkurransekraft, samt bidra til å løse samfunns-utfordringer og styrke nasjonal sikkerhet. Departementet er ansvarlig for å fremme en

bærekraftig og konkurransedyktig økonomi i en global kontekst, samtidig som de omtaler klimaendringer og energipolitikk i Nederland.

Figur 4.9 Presentasjonen av Nederlands kritiske teknologier baseres på ett dokument, utgitt av Ministry of Economic Affaris and Climate Policy.

Ministry of Economic Affaris and Climate Policy vektlegger spesielt strategiske investeringer i kritiske teknologier for å forbedre nederlandsk inntektspotensial og nasjonal sikkerhet. Disse anstrengelsene er i tråd med å opprettholde landets ledende posisjon innen teknologisk innovasjon gjennom offentlig-private partnerskap og internasjonalt samarbeid. Målsetningen er å sikre at teknologiske fremskritt gir positive bidrag til samfunnet, samtidig som de reduserer risikoen med hensyn til geopolitiske utviklinger og miljømessig bærekraft.

Det nederlandske dokumentet skisserer videre en strategisk tilnærming for å prioritere og utvikle kritiske teknologier. Det understreker viktigheten av innovasjon for å håndtere samfunnsutfordringer, styrke nasjonal sikkerhet, og øke landets økonomiske inntjenings-potensial. Strategien identifiserer ti kritiske og prioriterte teknologier, som for eksempel kunstig intelligens, energiteknologier, og halvlederteknologier, som er avgjørende for å opprettholde teknologisk lederskap og fremme økonomisk vekst. Den fremhever også behovet for målrettede investeringer, internasjonalt samarbeid og en tverrfaglig tilnærming til innovasjon for å sikre Nederlands posisjon på den globale teknologiarenaen mot 2035.

Både Nederland og EU anerkjenner betydningen av teknologiske fremskritt for økonomisk sikkerhet og strategisk lederskap, og identifiserer flere overlappende kritiske teknologier. Halvlederteknologier fremheves i både Nederland og EU, inkludert kravene til avanserte node-størrelser og produksjonsutstyr, som er essensielle for økonomisk vekst og teknologisk selvforsyning. Kunstig intelligens (KI) er også anerkjent som en transformativ teknologi med anvendelser på tvers av ulike sektorer, som muliggjør innovasjoner innen dataanalyse, høytytende databehandling og skylagring. Kvanteteknologier er fremhevet for sitt

revolusjonerende potensial, som omfatter kvantedatabehandling, kryptografi og kommunikasjon, som kan redefinere beregnings- og sikkerhetsparadigmer. Begge dokumentene fremhever også bioteknologier, med delt vekt på genetiske modifikasjonsteknikker, nye genomiske teknikker og syntetisk biologi, som anerkjenner deres brede anvendelser innen helse, landbruk og miljø. I tillegg refererer begge dokumentene til avanserte materialer og produksjonsteknologier som nanomaterialer, smarte materialer og additiv produksjon.

Imidlertid understreker dokumentet fra Nederland, sammenlignet med EU-kommisjonen, spesifikke teknologier som fremhever landets unike industrielle styrker og økonomiske målsetninger. Spesielt fremheves optiske systemer og integrert fotonikk, som viser nasjonens ekspertise som er avgjørende for halvledere og kommunikasjonsteknologier. Det nederlandske dokumentet fremhever også prosessteknologi, inkludert prosessintensivering, som er essensielt for overgangen til bærekraftige kjemiske råstoffer og prioritering av miljømessig bærekraft. Biomolekylære og celleteknologier vektlegges for deres anvendelser innen helse og landbruks-teknologi. I tillegg blir avbildningsteknologier trukket frem for både medisinske og industrielle anvendelser, noe som demonstrerer nederlandsk kompetanse innen vitenskapelig forskning og industri. Mekatronikk[36] blir anerkjent for sine systemintegrasjonskapasiteter, spesielt innen robotikk og det vies også oppmerksomhet til energimaterialer for energilagring og -konvertering, noe som fremhever deres rolle i nasjonens energiovergang. Til slutt er cybersikkerhetsteknologier detaljert som et prioritert område med spesifikke initiativer, noe som avslører en noe mer variert tilnærming som står i kontrast til EUs rammeverk som sentreres rundt økonomisk sikkerhet og teknologisk autonomi.

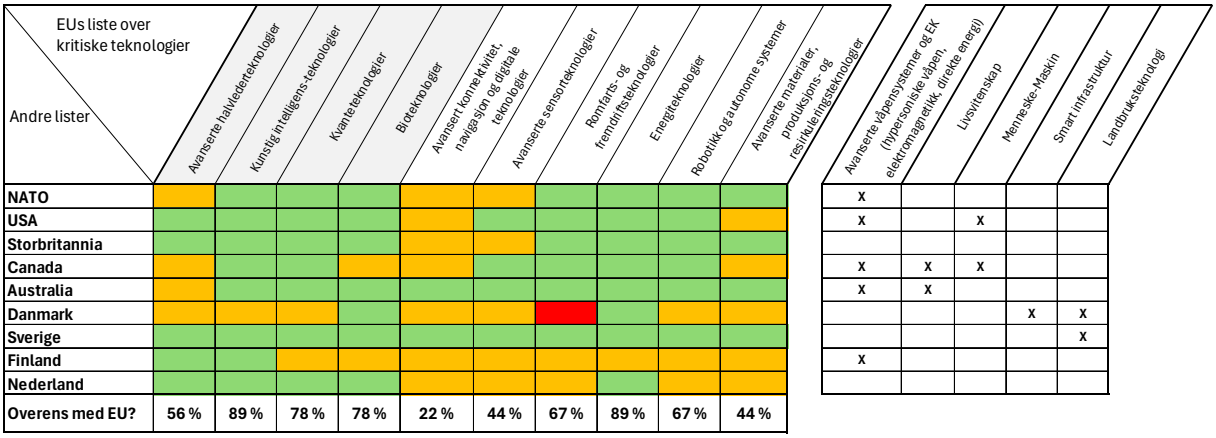
Det nederlandske dokumentet understreker også betydningen av kritiske teknologier, spesielt halvlederteknologier og kvanteteknologier, for militære applikasjoner og nasjonal sikkerhet. Dokumentet fremhever at disse teknologiene er avgjørende for å opprettholde strategisk lederskap og redusere avhengigheter som kan påvirke Nederlands geopolitiske posisjon og nasjonale sikkerhet. Det tar også for seg rollen disse teknologiene spiller i å sikre nødvendige forsyningskjeder vitale for forsvarsformål.

4.10 En samlet oversikt: EUs kritiske teknologier sammenlignet andre lister

Gitt vurderingene i kapittel 4.1–4.9 har vi sammenlignet de andre listene mot EUs liste over kritiske teknologier i figur 4.10. Grønn farge innebærer at EUs kategori også er eksplisitt oppgitt som egen kategori i den andre listen. Gul farge indikerer at EUs kritiske teknologi er diskutert, men den er ikke oppgitt som en «hovedkategori» i den andre listen. Rød farge betyr at teknologiområdet fra EU ikke er nevneverdig diskutert eller vurderte som kritisk eller viktig i den andre listen. Prosentandelen nederst i tabell 4.10 indikerer hvor mange grønne celler det er i kolonnen. I de fem kolonnene ytterst til høyre indikeres at den andre listen også omfatter annen kritisk teknologi. I all hovedsak dreier dette seg om teknologi relatert til nasjonal sikkerhet og militære kapabiliteter (EUs liste over kritisk teknologi argumenteres ut fra økonomisk

[36] Mekatronikk er et tverrfaglig felt som integrerer mekaniske systemer, elektronikk, informatikk og kontrollteknikk for å designe og skape komplekse elektromekaniske systemer.

sikkerhet/konkurranseevne). Legg merket til at det er bare ett land, Sverige, som er mer eller mindre identisk med EUs liste over kritiske teknologier.



Figur 4.10 *En sammenstilling og oppsummering av vurderingene fra andre lands lister opp mot EUs liste over kritisk teknologi. Grønn farge indikerer tilsvarende kategorisering som i EU, gul en delvis lik inndeling og omtale av kritisk teknologi mens rød indikerer et avvik. I tabellen til høyre indikeres andre teknologiområder som ikke nevnes i EUs liste.*

I teksten nedenfor følger en kort oppsummering av forskjellene mellom de andre listene (ulike land) og EUs liste over kritisk teknologier. Oppsummeringen innebærer at vi presenterer bakgrunnen/vurderingen for hvorfor en celle er markert gul og hvorfor det er satt en «X» i tabellen til høyre i figur 4.10.

4.10.1 NATO

NATO fokuserer i større grad på teknologier med militær bruk og sikter mot å opprettholde et teknologisk forsprang innen forsvar og nasjonal sikkerhet. Dette gjenspeiler organisasjonens primære rolle som en militær allianse. Noen teknologier som er fremhevet av NATO, men som ikke nødvendigvis er like fremtredende på EUs lister, inkluderer hypersoniske våpen og strålevåpen. Disse teknologiene har direkte relevans for militære operasjoner og kapabiliteter. På den andre siden er EUs tilnærming mer fokusert på økonomisk sikkerhet, teknologisk suverenitet og flerbrukspotensial (dual-use), altså teknologier som kan brukes både sivilt og militært. EU-kommisjonen prioriterer teknologiområder som avanserte halvledere og kunstig intelligens, og vektlegger hvordan disse teknologiene kan bidra til å styrke EUs økonomiske posisjon, redusere avhengigheter fra utenforstående parter, og unngå teknologilekkasje. Mens begge enhetene deler noen felles interesser – som kunstig intelligens og kvanteteknologier – er EUs liste mer fokusert på å fremme økonomisk utvikling gjennom teknologiske fremskritt, og tar i større grad hensyn til regulatoriske aspekter og den bredere innvirkningen på folks hverdag. NATO legger derimot større vekt på teknologier som gir direkte gevinster i militære operasjoner og forsvarsevner, og deres liste reflekterer en prioritering av direkte militær relevans.

4.10.2 USA

USAs liste over kritiske teknologier er mer detaljert og omfattende enn EUs liste, og vektlegger en bredere rekke av teknologiområder som ansees avgjørende for nasjonal sikkerhet, inkludert avansert databehandling, bioteknologier og kvanteteknologier. USA legger mye større vekt på forsvarsspørsmål, med spesifikke områder som hypersoniske våpen, direkte rettet energi (høyenergivåpen) og integrerte sensor- og cyberkapasiteter som ikke er fremtredende i EUs dokumenter. Både USA og EU anser teknologier som kunstig intelligens og kvanteteknologier som kritiske, men legger EU mer vekt på teknologisk suverenitet, økonomisk sikkerhet og flerbrukspotensial. EUs tilnærming er mer økonomisk og strategisk orientert mot å redusere avhengighet og risiko ved geopolitiske spenninger, mens USA understreker behovet for å opprettholde militær teknologisk overlegenhet med sterke prioriteringer innen autonomi, kommando- og kontrollsystemer. Videre understreker de amerikanske dokumentene mer detaljert avanserte produksjonsteknikker, herunder additiv produksjon, samt nye materialer i relasjon til avanserte gassturbinmotorer og bioteknologi, mens EU i større grad fremhever energiteknologier og resirkulering av kritiske råmaterialer. Totalt sett er det større variasjoner i vektlegging av forsvarsapplikasjoner i USA, mens EU eksemplifiserer et bredere perspektiv på teknologienes betydning for teknologisk uavhengighet og økonomisk robusthet.

4.10.3 Storbritannia

Storbritannia og EUs lister over kritiske teknologier reflekterer ulike prioriteringer og tilnærminger når det gjelder teknologisk utvikling og strategisk planlegging. Storbritannia legger vekt på et bredere spekter av teknologier, inkludert fremtidige telekommunikasjons-teknologier som 6G, teknisk biologi, og energiteknologier som kjernefysisk fusjon og hydrogenproduksjon. Dette indikerer en nasjonal tilpasning til egne industri- og sikkerhetsbehov samt en forståelse av teknologiene som bidrar både til økonomisk vekst og sikkerhet. EU, derimot, fremhever økonomisk sikkerhet, teknologisk suverenitet, og flerbrukspotensial, med klare risikovurderinger for hver teknologi. EUs prioriteter inkluderer avanserte halvledere, kunstig intelligens, kvanteteknologier og bioteknologier, med tanke på å redusere avhengighet fra eksterne parter og styrke intern markedsposisjon. Selv om Storbritannia også anerkjenner disse områdene, legger de større vekt på nasjonale styrker og spesifikke fremtidige teknologiske muligheter i sin strategi. Begge setter imidlertid kunstig intelligens, kvanteteknologi, bioteknologier og avansert databehandling høyt på agendaen, men Storbritannia fokuserer spesielt på anvendelser som fremtidige telekommunikasjoner og nullutslippsteknologier, som er mindre fremtredende i EUs dokumenter. Disse forskjellene reflekterer ulikheter i hvordan Storbritannia og EU velger å navigere i det globale teknologilandskapet, med Storbritannia som understreker det å utnytte nasjonale kapabiliteter og unike muligheter, og EU som tilstreber å bygge en sammenhengende teknologisk autonomi gjennom medlemslandene.

4.10.4 Canada

Både Canada og EU har identifisert kritiske teknologiområder som essensielle for nasjonal sikkerhet og økonomisk utvikling, men det finnes distinkte forskjeller i deres lister. EUs liste er meget konkret og kortfattet, med spesifikke teknologiområder som avanserte halvledere, kunstig intelligens, kvanteteknologier og bioteknologier, fremhevet for deres flerbrukspotensial (dual-

use) og sikkerhetsmessige implikasjoner. Canada, derimot, omtaler sitt dokument som en liste over sensitive teknologier og gir en mer utfyllende presentasjon, inkludert avanserte sensor- og overvåkningsteknologier, menneske-maskin integrasjons-teknologier, og avanserte materialer med unike egenskaper som høy-entropimaterialer, auxetiske- og metamaterialer. Videre nevner Canada avanserte våpenteknologier, som hypersoniske og retningsstyrte energivåpen, som ikke er fremtredende i EU-dokumentet. Canada inkluderer også medisinske fremskritt som nano-medisin og genterapi, og understreker potensialet i luft- og romteknologi, noe som viser et bredere spektrum av strategiske interesser og sikkerhetsbekymringer sammenlignet med EU-dokumentet. Dermed reflekterer de to landenes lister ulike tilganger og prioriteringer, med Canada som betoner spesifikke nasjonale teknologier innenfor en kontekst av mulig misbruk og de strategiske truslene dette kan inneha.

4.10.5 Australia

Det er tydelige forskjeller mellom Australias og EUs lister over kritiske teknologier, særlig når det gjelder prioritering og bredde av teknologiområder. Australias liste omfatter 64 kritiske teknologier fordelt på ni hovedkategorier, med en sterk vekt på teknologiske spesifikasjoner som har militære eller strategiske anvendelser. Dette inkluderer avanserte flymotorer, droner, autonome systemer, og hypersoniske teknologier, som betraktes som svært kritiske på grunn av risiko for monopol innen teknologiene fra land som Kina. I motsetning til EUs mer konsentrerte liste på ti teknologiområder, der avanserte halvledere, kunstig intelligens og kvanteteknologier står sentralt, har Australia et bredere spektrum av inkluderte teknologier. EU vektlegger det å sikre teknologisk suverenitet gjennom redusert avhengighet av eksterne leverandører, og legger stor vekt på økonomisk sikkerhet og flerbrukspotensial (dual-use) av teknologier. Selv om både EU og Australia anerkjenner viktigheten av kunstig intelligens, kvanteteknologier og bio-teknologier, fokuserer Australia mer på energiteknologier som elektriske batterier og hydrogen-teknologier, samt avanserte materialer og produksjonsteknikker. Totalt sett reflekterer Australias liste en sterkere militær og strategisk vektlegging, samt en bekymring for teknologisk monopol, mens EUs liste er rettet mot å fremme økonomisk sikkerhet og strategisk teknologi-utvikling innen EU.

4.10.6 Danmark

Danmarks tilnærming er å innlemme EUs prioriteringer og samtidig fremheve teknologier som styrker økonomien, sikkerheten og samfunnets motstandsdyktighet (resiliens). Mens EUs liste over kritiske teknologier er detaljert med klare prioriteringer innen områder som avanserte halvledere, kunstig intelligens og kvanteteknologi, har Danmark en bredere tilnærming som organiserer teknologier i tre transformasjonskategorier: fossilfrie, biobaserte, og digitalt understøttede teknologier. Danmark legger større vekt på bærekraftig utvikling og teknologier som kan fremme miljøinnsats, som fornybar energi, bioteknologisk produksjon, og grønn transport, noe som viser en sterk orientering mot bærekraft og økonomisk uavhengighet. Samtidig betoner deres strategier betydningen av digitale teknologier og robotteknologi for å sikre fremtidig innovasjon og konkurranseevne. Mens EU diskuterer det å oppnå teknologisk suverenitet og redusere utenlandsk avhengighet, vektlegger Danmark synergier mellom sektorer for å forbedre internasjonal markedsførbarhet og selvstendighet. Den danske tilnærmingen

inkluderer hvordan kritiske teknologier kan ha både sivile og forsvarsmessige anvendelser, med konkrete prioriteringer innen digital teknologi og energilagring. Selv om det er betydelige overlappinger, viser forskjellene mellom Danmark og EU en lokal tilpasning til nasjonale prioriteringer og spesialiserte styrker, noe som reflekterer Danmarks behov for grønne løsninger og innovativ teknologiutvikling.

4.10.7 Sverige

Sveriges liste gir innsyn i landets unike prioriteringer sammenlignet med EUs oversikt over kritiske teknologier. Begge lister anerkjenner viktigheten av teknologier som kunstig intelligens, kvanteteknologi og bioteknologi, men Sverige legger særlig vekt på teknologiområder som energiteknologi for fossilfri elektrifisering og materialteknologi, noe som er drevet av landets prioritering på bærekraft og overgang til et grønnere samfunn. Sverige fremhever spesifikke styrker innen utvikling av komplekse systemløsninger, spesielt innen telekommunikasjon, transport og forsvar, samt domenespesifikke KI-løsninger i sterke industrielle sektorer som produksjon og skogindustri. Denne fokuserte tilnærmingen gjenspeiler et mål om å sikre økonomisk vekst og nasjonal motstandskraft mot globale utfordringer. I motsetning til dette, har EU en bredere tilnærming hvor de spesifikt fremhever avanserte materialer, halvlederteknologi og cybersikkerhet for å opprettholde et teknologisk forsprang og redusere avhengigheter fra eksterne leverandører. Selv om det er overlapp mellom de to listene, reflekterer Sveriges liste en lokal tilpasning basert på nasjonale behov og muligheter, som energiteknologi og system-av-system synergier, mens EU fremhever teknologisk autonomi gjennom en mer generell økonomisk sikkerhet. Sverige understreker også betydningen av internasjonalt samarbeid og alliansesamarbeid, spesielt innen NATO, for å sikre at Sveriges teknologiske fremskritt gir strategiske fordeler både hjemme og i internasjonale samarbeid.

4.10.8 Finland

Finlands tilnærming til kritiske teknologier viser en sterk overensstemmelse med EUs liste, men med prioriteringer som reflekterer nasjonale sikkerhetsbehov. Mens både Finland og EU legger vekt på avanserte halvlederteknologier, kunstig intelligens, kvanteteknologi og bioteknologi, legger Finland spesielt vekt på cybersikkerhet og mikro- og nanoelektronikk, som er avgjørende for beskyttelse av nasjonal sikkerhet og integrasjon med NATOs systemer. Finland betrakter cybersikkerhetsteknologier som kritiske for å motvirke trusler og opprettholde beredskap i henhold til NATO-krav, spesielt gjennom integrert luft- og missilforsvar. Samtidig vektlegger den finske strategiske tilnærmingen romteknologi og autonome systemer, som oppfattes å ha transformative innvirkninger på forsvarsevner. Selv om EU også dekker disse teknologiene, prioriterer Finland utviklingen av C4ISTAR kapabiliteter og energiteknologier for fossilfri elektrifisering. Små nyanser i Finlands tilnærming inkluderer en økt vektlegging på synergier mellom teknologiområder og en sterkere vektlegging av domenespesifikke KI-løsninger for lokalt sterke industrier som skogbruk og gruvedrift. Dette reflekterer Finlands kontekstuelle prioriteringer innen teknologisk suverenitet og nasjonal sikkerhet, som står i harmoni med EUs brede mål om strategisk autonomi.

4.10.9 Nederland

Nederland og EU har begge lister over kritiske teknologier som fremhever det å opprettholde økonomisk sikkerhet og teknologisk lederskap, men deres tilnærminger og prioriteringer varierer noe. Begge parter legger vekt på avanserte halvlederteknologier, kunstig intelligens, kvanteteknologier og bioteknologier på grunn av det økonomiske potensialet og betydningen for teknologisk suverenitet. Nederland fremhever imidlertid spesifikke teknologiområder som optiske systemer og integrert fotonikk, som reflekterer landets styrker innen halvleder-produksjon og kommunikasjonsteknologier. Videre legger Nederland vekt på prosess-intensivering og biomolekylære teknologier for å fremme bærekraft i kjemisk produksjon og landbruk, samt mekatronikk for systemintegrasjon innen robotikk. Denne spesialiseringen viser Nederlands mål om å kapitalisere på konkrete industrielle styrker. I kontrast til dette har EU en bredere vektlegging på teknologiområder som romfart og konnektivitet, inkludert romteknologier for fremdriftssystemer og skybaserte kommunikasjoner. EU fokuserer i tillegg mer på cybersikkerhet og neste generasjons konnektivitetsløsninger som 6G. Nederlands strategi legger også vekt på å forbedre nasjonal energisikkerhet gjennom teknologiområder som energimaterialer for lagring og konvertering, noe som ikke er like spesifikt fremhevet i EUs bredere tilnærming til energi- og resirkuleringsteknologier. Dette viser hvordan Nederland tilpasser sine prioriteringer til nasjonale styrker og økonomiske mål, mens EU søker å styre et koordinert teknologisk lederskap blant sine medlemsland.

4.10.10 Den prinsipielle forskjellen mot EUs liste over kritiske teknologier

Den prinsipielle forskjellen mellom EUs liste over kritiske teknologier og listene fra andre land ligger i EUs hovedfokus på å sikre økonomisk sikkerhet, teknologisk suverenitet og flerbruks-potensial (dual-use) av teknologier for å redusere avhengighet fra eksterne parter og styrke intern markedsposisjon. EU har en strategisk tilnærming som er mer orientert mot å fremme økonomisk utvikling ved å bruke teknologiske fremskritt som avanserte halvledere, kunstig intelligens og kvanteteknologier. I motsetning til dette, vektlegger andre land ofte mer spesifikke nasjonale sikkerhetsbehov, forsvarsteknologier og strategiske militære anvendelser. NATO, for eksempel, fremhever militær relevans og teknologisk forsprang innen forsvar, mens USA understreker forsvarsfokus med omfattende dekning av avansert databehandling og våpenteknologier. Storbritannia og Australia legger vekt på en bredere portefølje av teknologier for å støtte nasjonale industri- og sikkerhetsbehov, og Canada fremhever sensitive teknologier basert på ulike sikkerhetsbekymringer. Land som Danmark og Sverige viser en sterk lokal tilpasning til bærekraftig utvikling og grønne løsninger, mens Finland og Nederland fremhever på spesifikke industri- og sikkerhetsstyrker. Disse forskjellene reflekterer hvordan hvert land eller region tilpasser sine teknologiske prioriteringer til sine unike målsetninger innen sikkerhet, økonomisk vekst og politisk strategisk posisjonering.

5 Forslag til Norges liste over sensitive teknologier

Med utgangspunkt i anbefalt definisjon (kapittel 2), EUs liste over kritiske teknologiområder (kapittel 3) og andre lister (kapittel 4) vil dette kapittelet utlede et forslag til en norsk liste over sensitive teknologiområder, tilpasset norske forhold og behov. Dette er ikke ment som en endelig liste, men favner bredt over de teknologiområder og konkrete teknologier som anses relevant for ytterligere forankring og gransking (delleveranse 3) og risikovurderingen som skal gjøres i delleveranse 4. I denne fasen av prosjektet har man dermed en inkluderende tilnærming, for så senere i prosjektet avgjøre om nyoppførte teknologier bør beholdes eller forkastes.

Metodisk tas det utgangspunkt i alle teknologiområdene fra EUs liste over kritiske teknologier (kapittel 3). Deretter gjøres en vurdering av å inkludere teknologiområder og teknologier som fremheves i andre lands lister (kapittel 4), men som ikke er nevneverdig nevnt i EUs liste. Hovedkriteriet er hvor sterkt de vektlegges og om det er flere lister som dekker teknologier som ikke er med i EUs liste. I sum danner dette vurderingsgrunnlaget for utarbeidelsen av en norsk liste over sensitive teknologier.

	EU kategori av sensitive teknologier	EUs eksempler på sensitive teknologier innen kategorien	EUs kategori oversatt til Norsk	EUs eksempler på teknologi inne hver kategori, oversatt til norsk	Forslag til ytterligere teknologiområder basert på andre lands lister
Av de ti kritiske teknologiområdene lister EUs anbefalinger disse fire teknologiske områder som mer sensitive. De representerer en umiddelbar og høyere risiko for tekkasje og uønsket kunnskapsoverføring til land og aktører en ikke har formelt sikkerhetssamarbeid med.	Advanced Semiconductors Technologies	Microelectronics, including processors	Avanserte halvlederteknologier	Mikroelektronikk, inkludert prosessorer	Antenner og antennedesign, dvs. 4D-arrays og mekanisk manipulerte antennedesign for å forbedre ytelsen og muliggjøre trådløs kommunikasjon over lange avstander, inkludert underjordisk og undervannskommunikasjon.
		Photonics (including high energy laser) technologies		Fotonikk (inkludert høyenergilaser) teknologier	Adaptiv kamuflasje ved bruk av nye materialer og prosesser . Spektrumsadministrasjon innebærer avanserte sensorer som benytter KI/ML-algoritmer for mer effektiv og smidig bruk av det elektromagnetiske miljøet.
		High frequency chips		Høyfrekvente databrikker	Rettede energivåpen: Laser, høyenergi mikrobølge-våpen og partikkelstråler, inkludert evnen til å skade/ødelegge elektronisk utstyr
		Semiconductor manufacturing equipment at very advanced node sizes		Utstyr for produksjon av halvledere på svært avanserte node-størrelser	
	Artificial Intelligence Technologies	High Performance Computing	Kunstig intelligens-teknologier	Høytelsesdatabehandling	Bruke AI for å analysere data, optimere systemytelse, og forbedre beslutningstaking i byer, transport og energinettverk. Generativ KI som arbeidstidsbesparende tiltak.
		Cloud and edge computing		Sky- og kantdatabehandling	
		Data analytics technologies		Dataanalysesteknologier	
		Computer vision, language processing, object recognition		Datamaskinsyn, språkbehandling, objektgjenkjenning	
	Quantum Technologies	Quantum computing	Kvanteteknologier	Kvanteberegning	
		Quantum cryptography		Kvantekryptografi	
		Quantum communications		Kvantkommunikasjon	
		Quantum sensing and radar		Kvantesensorer og radar	
	Biotechnologies	Techniques of genetic modification	Bioteknologier	Teknikker for genetisk modifikasjon	Nanoteknologi kan brukes til å lage nye biomedisinske produkter, som systemer for legemiddellevering og diagnostiske verktøy, spesielt i skjæringspunktet mellom biologi og materialvitenskap.
		New genomic techniques		Nye genomiske teknikker	Bioteknologi og kjemiteknologi i forsvaret mot kjemiske og biologiske trusler.
		Gene-drive		Gen-driv	Forsterkning eller fornying av mennesklige egenskaper/sanser/prestasjon
		Synthetic biology		Syntetisk biologi	Biosensorer for overvåkning av mennesklige egenskaper/sanser/prestasjon
	Advanced connectivity, Navigation and digital Technologies	Secure digital communications and connectivity, such as RAN & Open RAN (Radio Access Network) and 6G	Avansert konnektivitet, navigasjon og digitale teknologier	Sikker digital kommunikasjon og tilkobling, som RAN og Open RAN (Radio Access Network) og 6G	Elektronisk krigføring: Avanserte kommunikasjonsteknologier og cybersikkerhetssystemer i sammenheng med militær bruk.
		Cyber security technologies incl. cyber-surveillance, security and intrusion systems, digital forensics		Cybersikkerhetsteknologier inkludert cybersurveillanse, sikkerhet og inntrengingssystemer, digital etterforskning	Sikre digitale kommunikasjonssystemer og navigasjonsteknologier for å administrere ressurser effektivt i sanntid. Dette inkluderer smart grid-teknologier og IoT-løsninger for å forbedre effektiviteten i strømfordeling og ressursstyring.
		Internet of Things and Virtual Reality		Tingenes internett og virtuell virkelighet	
		Distributed ledger and digital identity technologies		Distribuerte ledgers og digital identitetsteknologi	
		Guidance, navigation and control technologies, including avionics and marine positioning		Veiledning, navigasjon og kontrollteknologier, inkludert avionikk og maritim posisjonering	

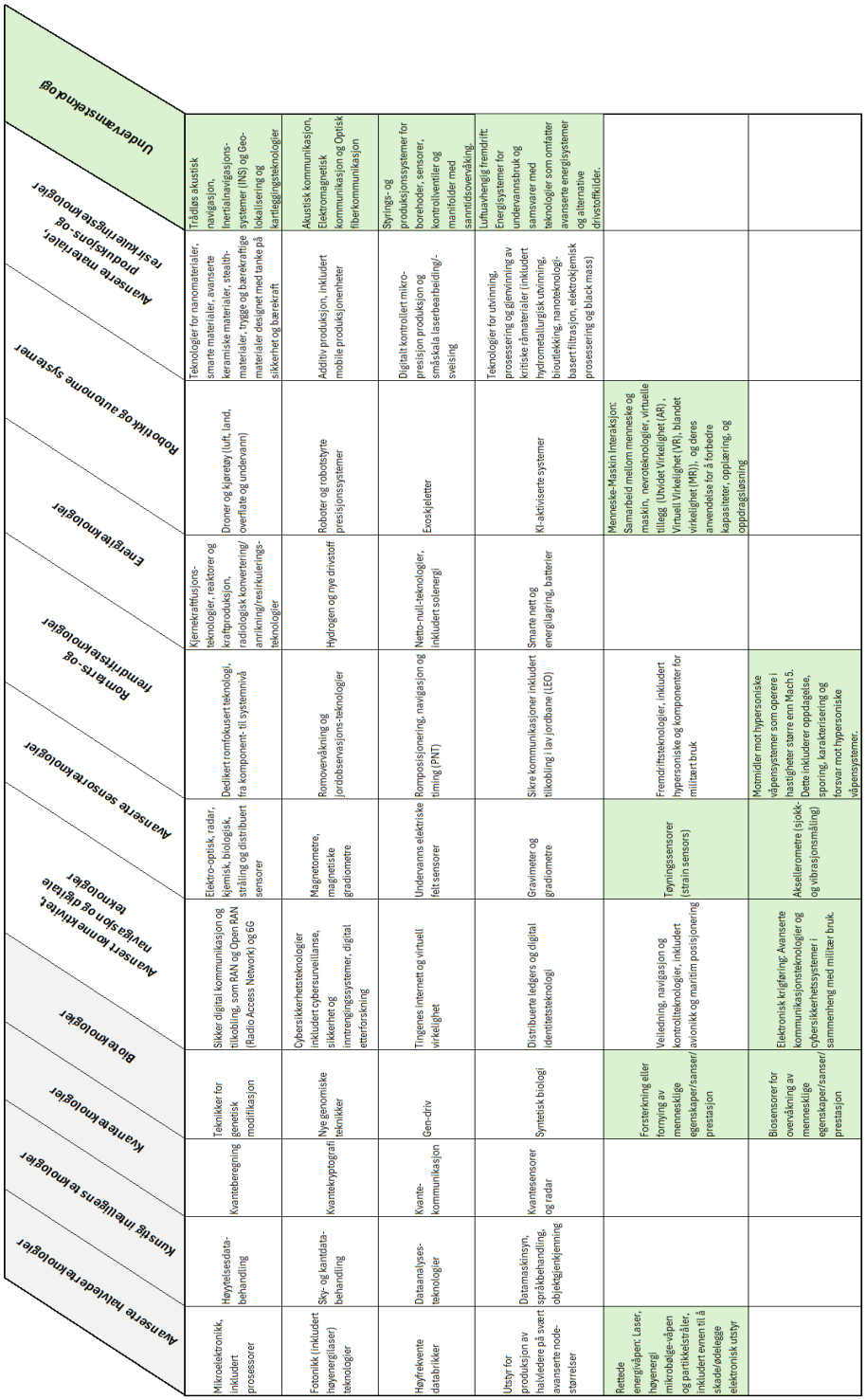
Figur 5.1 *Forslag til norsk liste over sensitive teknologier baseres på EUs liste over kritiske teknologier. EUs teknologiområder er gjengitt i de to kolonnene til venstre – og de to neste kolonnene er en norsk oversettelse av EUs liste. Teknologiene listet i ytterste høyre kolonne foreslås som et tillegg innenfor teknologiområdet fra EU – basert på andre lands lister i kapittel fire.*

EU kategori av sensitive teknologier	EUs eksempler på sensitive teknologier innen kategorien	EUs kategori oversatt til Norsk	EUs eksempler på teknologi inne hver kategori, oversatt til norsk	Forslag til ytterligere teknologiområder basert på andre lands lister
Advanced sensing Technologies	Electro-optical, radar, chemical, biological, radiation and distributed sensing	Avanserte sensorteknologier	Elektro-optisk, radar, kjemisk, biologisk, stråling og distribuert sensorer	Avanserte sensorteknologier som forbedrer målretting, styring eller overvåkningsaspekter ved våpensystemer.
	Magnetometers, magnetic gradiometers		Magnetometre, magnetiske gradiometre	Tøyningssensorer (strain sensors)
	Underwater electric field sensors		Undervanns elektriske feltsensorer	Akselerometre (sjokk- og vibrasjonsmåling)
	Gravity meters and gradiometers		Gravimeter og gradiometre	
Space & propulsion technologies	Dedicated space-focused technologies, ranging from component to system level	Romfarts- og fremdriftsteknologier	Dedikert romfokusert teknologi, fra komponent- til systemnivå	Motmidler mot hypersoniske våpensystemer som operere i hastigheter større enn Mach 5. Dette inkluderer oppdagelse, sporing, karakterisering og forsvar mot hypersoniske våpensystemer.
	Space surveillance and Earth observation technologies		Romovervåkning og jordobservasjonsteknologier	Avanserte eksplosiver og energimaterialer: Materialer med en stor mengde lagret eller potensiell energi som kan forårsake en eksplosjon. Anvendelser spenner vanligvis over industrier som gruvedrift, anleggsteknikk, produksjon og Forsvaret.
	Space positioning, navigation and timing (PNT)		Romposisjonering, navigasjon og timing (PNT)	
	Secure communications including Low Earth Orbit (LEO) connectivity		Sikre kommunikasjoner inkludert tilkobling i lav jordbane (LEO)	
	Propulsion technologies, including hypersonics and components for military use		Fremdriftsteknologier, inkludert hypersoniske kapasiteter og komponenter for militært bruk	
Energy technologies	Nuclear fusion technologies, reactors and power generation, radiological conversion/enrichment/recycling technologies	Energiteknologier	Kjernekraftfusjonsteknologier, reaktorer og kraftproduksjon, radiologisk konvertering/ anrikning/resirkulerings-teknologier	Luftuavhengig fremdrift: Energisystemer for undervannsbruk og samsvarer med teknologier som omfatter avanserte energisystemer og alternative drivstoffkilder.
	Hydrogen and new fuels		Hydrogen og nye drivstoff	Smart infrastruktur inkluderer smarte strømnett (smart grids) og energilagringssystemer som er sentrale for integrering av fornybare energikilder og økt energiforsyningssikkerhet.
	Net-zero technologies, including photovoltaics		Netto-null-teknologier, inkludert solenergi	Teknologier for strømproduksjon (generatorer, brenselceller m.m.)
	Smart grids and energy storage, batteries		Smarte nett og energilagring, batterier	Energiomforming (reformering, elektrolyse, m.m.)
Robotics and autonomous systems	Drones and vehicles (air, land, surface and underwater)	Robotikk og autonome systemer	Ubemannede farkoster i alle domener (luft, land, overflate og under vann)	Menneske-Maskin Interaksjon: Samarbeid mellom menneske og maskin, nevroteknologier, virtuelle tillegg (Utvidet Virkelighet (AR) , Virtuell Virkelighet (VR), blandet virkelighet (MR)), og deres anvendelse for å forbedre kapasiteter, opplæring, og oppdragsløsning
	Robots and robot-controlled precision systems		Roboter og robotstyrte presisjonssystemer	Anvendelsen av nanoteknologi kan strekke seg til molekylære eller nano-roboter, som er miniatyriserte robotsystemer som kan fungere på en veldig liten skala og utføre oppgaver som målrettet legemiddellevering eller miljøovervåking.
	Exoskeletons		Exoskjeletter	Navigasjon og samhandlings teknologi: Droner, kjøretøy og roboters evne til å navigere og samhandle med andre autonome systemer/plattformer (sverm) og omgivelsene sine.
	AI-enabled systems		KI-aktiviserte systemer	
Advanced materials, manufaturing and recycling technologies	Technologies for nanomaterials, smart materials, advanced ceramic materials, stealth materials, safe and sustainable by design materials	Avanserte materialer, produksjons- og resirkulerings-teknologier	Teknologier for nanomaterialer, smarte materialer, avanserte keramiske materialer, stealth-materialer, trygge og bærekraftige materialer designet med tanke på sikkerhet og bærekraft	Teknologier tilpasset ekstreme klimaforhold som kan påvirke materialhåndtering, konstruksjon og vedlikehold. Dette omfatter teknologier som håndterer svært kalde temperaturer eller maritim operasjoner i nord områdene
	Additive manufacturing, including in the field		Additiv produksjon, inkludert mobile produksjonenheter	
	Digital controlled micro-precision manufacturing and small-scale laser machining/welding		Digitalt kontrollert mikro-presisjon produksjon og småskala laserbearbeiding/-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, bioutlekking, nanoteknologi-basert filtrasjon, elektrokjemisk prosessering og black mass)	

Figur 5.2 En fortsettelse av figur 5.1.

De to tabellene som er gjengitt i figur 5.1 og 5.2 er en utvidet liste av EUs liste over kritiske teknologier, men hvor andre lister (fra kapittel 4) er satt inn under EUs kategorisering av teknologiområder. Dette er grunnlaget for utarbeidelsen av et første forslag til den norske listen over sensitive teknologier. Hvis en ser litt nøye etter så er det to teknologiområder fra andre lister som ikke er tatt med i figur 5.1 og 5.1; livsvitenskap og landbruksteknologi. Livsvitenskap tas ikke med i den videre vurderingen da formålet ved denne studien dekkes godt av teknologi-området bioteknologi og følger dermed også den samme avgrensingen som EU er en del av – og hvor EU har avgrenset teknologiområdet gjennom benevnelsen «bioteknologi». Vi velger å følge den samme avgrensningen som EU. Landbruksteknologi er en kritisk teknologi for Norge, men ikke nødvendigvis sensitiv på en slik måte at utenlandske aktører kan bruke den mot oss. Derfor velger vi å utelate dette også i den videre vurderingen.

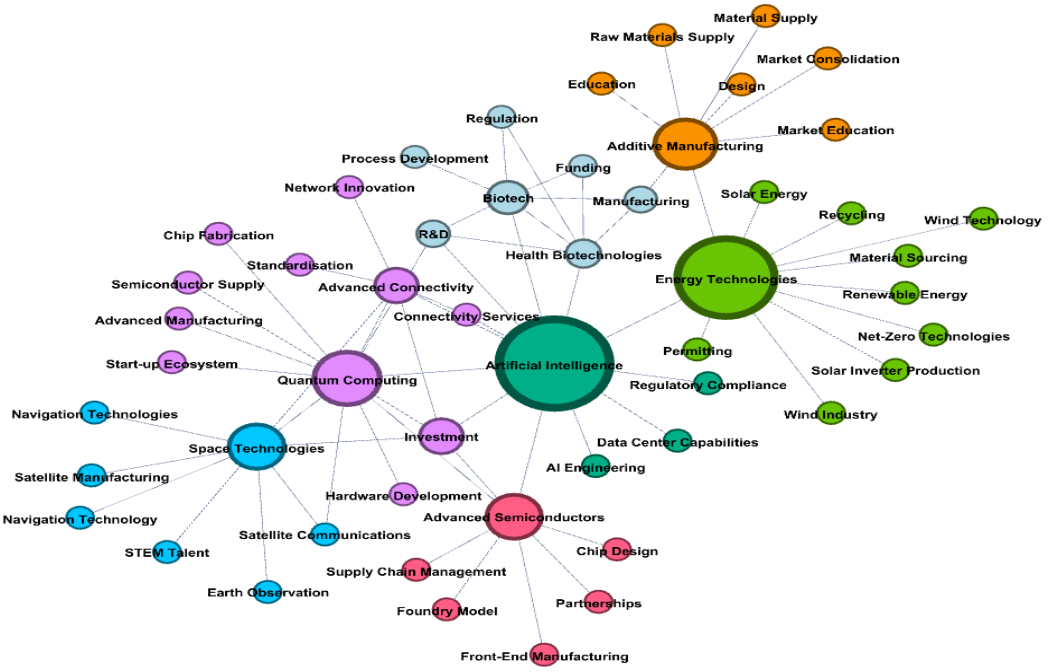
Basert på dette grunnlaget, og definisjonen på kritiske, sensitive og strategiske teknologier for nasjonal sikkerhet (se kapittel 2), fremmes en første versjon av en norsk liste over sensitiv teknologi, se figur 5.3.



Figur 5.3 Forslag til liste over norsk sensitiv teknologi baseres på EUs liste

De «nye» forslagene som faller inn under sensitive teknologiområder i norsk sammenheng (inspirert fra andre lister i kapittel 4) er menneske-maskin teknologi, direkte rettet energi (høyenergivåpen) og mottiltak mot avanserte våpensystemer. Disse er merket grønn i figur 5.3. I tillegg foreslås det en ny hovedkategori – Undervannsteknologi – som vi anser sensitiv i en norsk sammenheng. Som vi ser fra figur 5.1 og 5.2 så er forslaget over norske sensitive teknologier i figur 5.3 primært basert på EUs liste over kritisk teknologi.

De fire første teknologiområdene, gjengitt i figur 5.1, ansees å være mer sensitive enn de andre teknologiområdene. Dette baseres på EUs argument om at de fire første teknologiområdene har stort flerbrukspotensial (dual-use) sammenlignet med de andre teknologiområdene. I tillegg vil vi påstå at det er teknologiområder også bidrar til en gjensidig avhengighet mellom alle andre teknologiområder listet i figur 5.1 og 5.2. Som en illustrasjon på gjensidige avhengighet har vi gjennomført en semantisk analyse av teksten i det mest ordrike dokumentet fra EU og DIGITALEUROPE (se figur 3.1). Det innebærer at vi har brukt generativ KI for å «hente ut» alle teknologiområdene i teksten, og dermed laget en liste over teknologier som opptrer parvis gjennom teksten. Desto oftere de opptrer parvis, desto større sirkel i figur 5.3.



Figur 5.3 *Resultatet av en semantisk analyse av EU dokumentet fra DIGITALEUROPE som viser hvilke teknologier som omtales parvis gjennom teksten. Desto større sirkel, desto mer parvis omtale sammen med andre teknologiområder. I dette tilfelle ser vi at mange teknologiområder på EUs liste er gjensidig avhengig av kunstig intelligens og energiteknologi. Illustrasjonen er laget i Gephi[37].*

[37] Gephi er en åpen programvare for nettverksanalyse og datavisualisering. Gephi benyttes av forskere, dataanalytikere og utviklere som arbeider med sosiale nettverk, biologiske nettverk og andre typer relasjonsdata.

6 Sammendrag

Dette notatet er delleveranse to i oppdraget fra Kunnskapsdepartementet, som har som mål å utvikle et kunnskapsgrunnlag for vurdering av sensitive teknologier (KVAST). Arbeidet er et samarbeid mellom Norges forskningsråd, Forsvarets forskningsinstitutt og Nasjonal sikkerhetsmyndighet. Delleveranse to 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. Kapittelet fremhever viktigheten av definisjon og oversettelse av kritiske teknologiområder for norsk kontekst, og understreker åpenhet og samarbeid mellom ulike aktører for ytterligere utvikling og beskyttelse av nasjonale sikkerhetsinteresser.

Notatet diskuterer blant annet viktigheten av teknologi i dagens hurtig utviklende landskap, særlig i forhold til nasjonal sikkerhet. Det 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, som ofte overlapper. Det understreker behovet for samarbeid mellom offentlige myndigheter, akademia og næringslivet for å møte kravene til forskningssikkerhet.

Videre foreslås det i notatet, i kapittel to, en definisjon på kritiske, sensitive og strategiske teknologier. Kritiske teknologier er avgjørende for en nasjons sikkerhet og samfunnsfunksjoner. Sensitive teknologier er de som må skjermes på grunn av risiko for misbruk, mens strategiske teknologier er de som gir et land komparative fortrinn. Det understrekes at noen sensitive teknologier er kritiske for nasjonal sikkerhet og må overvåkes for å sikre beskyttelse, kompetanse og internasjonalt samarbeid.

I kapittel tre, "EUs liste over kritiske teknologier," tar notatet for seg 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 konnektivitet og navigasjon, avanserte sensorteknologier, romfartsteknologier, energiteknologier, robotikk og autonome systemer, samt avanserte materialer og produksjonsteknologier. Kapittelet diskuterer 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. Dokumentet fra 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.

I kapittelet som følger, kapittel fire, sammenligner vi 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 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.

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 foreslår å inkludere enkelte teknologier som er fremhevet i andre lands lister for å styrke nasjonal sikkerhet og økonomisk konkurranseevne. Forslaget inkluderer å utvide eksisterende kategorier med teknologiområder i EUs liste samt å introdusere en ny kategori kalt "Undervannsteknologi" Den «nye» kategorien omfatter spesielt teknologi for navigasjon, kommunikasjon og (miljø)sensorer under vann. 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 liste (sammenlignet med EUs liste), basert på nasjonale behov og globale teknologitrender. Denne listen er ikke endelig, men danner grunnlaget for videre arbeid i KVAST. Listen kan bli endret som følge av videre arbeid i KVAST, eller innspill prosjektet får i det videre arbeidet.

Referanser

I første del av referanselisten sorterer vi de listene og dokumentene som oppgir andre lands lister over kritiske, sensitiv eller strategisk teknologi som er sammenlignet med EUs liste over kritisk teknologi. Deretter listes andre referanser som vi henviser til i notatet.

Australia

Australia Strategic Policy Institute (2024). *ASPI's two-decade Critical Technology Tracker: The rewards of long-term research investment.* https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2024-08/ASPIs%20two-decade%20Critical%20Technology%20Tracker_1.pdf?VersionId=1p.Rx9MIuZyK5A5w1SDKIpE2EGNB_H8r

Australia Strategic Policy Institute (2024). *Technology tracker – List of Technologies.* https://techtracker.aspi.org.au/list-of-technologies/

Canada

Government of Canada (2024). *Sensitive Technology Research Areas.* https://science.gc.ca/site/science/sites/default/files/documents/2024-01/1081-sensitive-technology-research-areas-09Jan2024.pdf

Danmark

Akademiet for de Tekniske Videnskaber (2023). *Strategiske Teknologier for Danmark - 12 teknologier, der accelererer og understøtter omstillingen til en fossilfri, biobaseret og digitalt understøttet fremtid.* https://atv.dk/files/media/document/Web_dobbeltsidet_Kritiske%20teknologier%20for%20Danmarks%20fremtid%20rapport.pdf

Akademiet for de Tekniske Videnskaber (2024). *Kritiske teknologier - Globale hotspots, europæiske perspektiver, danske muligheder*. https://atv.dk/files/media/document/Kritiske%20teknologier_web.pdf

Europeiske Union

European Commission (2023). *Commission Recommendation of 03 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States.* https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

DIGITALEUROPE (2024). *The EU's Critical Tech Gap: Rethinking economic security to put Europe back on the map.* https://www.digitaleurope.org/resources/the-eus-critical-tech-gap-rethinking-economic-security-to-put-europe-back-on-the-map/

Finland

Puolustusministeriö (2016). *Suomen puolustuksen teknologisen ja teollisen perustan turvaaminen.* https://julkaisut.valtioneuvosto.fi/handle/10024/162637

Valtioneuvoston kanslia (2023). *Ulkomaiset investoinnit ja kriittinen aineeton omaisuus.* https://julkaisut.valtioneuvosto.fi/handle/10024/165130

Puolustusministeriö (2024). *Government Defence Report* https://julkaisut.valtioneuvosto.fi/handle/10024/166004

NATO

NATO STO (2023). *Science & Technology Trends 2023-2043 - Across the Physical, Biological, and Information Domain.* https://cesmar.it/wp-content/uploads/2023/04/stt23-vol1.pdf

Nederland

Ministerie van Economische Zaken en Klimaat (2024). *National Technology Strategy - Building blocks for strategic technology policy. https://www.kia-st.nl/_asset/_public/__site_4/257-034_Nationale_Technologie_Strategie-EN_met_agenda.pdf*

Storbritannia

Innovate UK (2023). *Welcome to the future - Innovate UK's 50 Emerging Technologies*. https://www.ukri.org/wp-content/uploads/2023/12/IUK-05122023-INO0617_Emerging-Tech-Report_AW2-final.pdf

Department for Science, Innovation and Technology (2024). *Science & Technology Framework - Update on progress* https://assets.publishing.service.gov.uk/media/65c9f67714b83c000ea7169c/uk-science-technology-framework-update-on-progress.pdf

Royal Academy of Engineering (2024). *Critical technologies: Past and Future*. https://raeng.org.uk/media/is3l3g03/critical_technologies_final.pdf

Sverige

Vinnova (2024). *Strategiska tekniker för Sverige - Ett underlag för nationella prioriteringar* https://www.vinnova.se/globalassets/publikationer/2024/rapport-ru-strategiska-teknikomraden_ver-01.0-final-1.pdf?cb=20241030174857

USA

Department of Defense (2022). *Technology Vision for an Era of Competition.* https://dod-critical-technology-area-roadmaps.zoiclabs.io/

NSTC (2024). *Critical and Emerging Technologies List Update.* https://www.govinfo.gov/content/pkg/CMR-PREX23-00185928/pdf/CMR-PREX23-00185928.pdf

Øvrige kilder

Forskningsrådet, Forsvarets forskningsinstitutt og Nasjonal sikkerhetsmyndighet. (2024). Et helhetlig forskningssystem for åpen, skjermet og gradert forskning. Fire anbefalinger for et helhetlig forskningssystem for åpen, skjermet og gradert forskning

Forsvarsdepartementet. (2021). Meld. St. 17 (2020–2021): Samarbeid for sikkerhet. https://www.regjeringen.no/contentassets/5f29db6ef1b34054a025ffddb7073b31/en-gb/pdfs/stm202020210017000engpdfs.pdf

Forsvarsdepartementet. (2024). Prop. 87 S (2023–2024): Forsvarsløftet – for Norges trygghet. Langtidsplan for forsvarssektoren 2025–2036. https://www.regjeringen.no/no/dokumenter/prop.-87-s-20232024/id3032217/

Justis- og beredskapsdepartementet. (2018). Lov om nasjonal sikkerhet (sikkerhetsloven). https://lovdata.no/dokument/NL/lov/2018-06-01-24

Nasjonal sikkerhetsmyndighet. (2023). Sikkerhetsfaglig råd - Et motstandsdyktig Norge. https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglig-rad-et-motstandsdyktig-norge

Utenriksdepartementet. (2024). Arbeidet med å ferdigstille endringer i eksportkontroll-forskriften er i sluttfasen. https://www.regjeringen.no/no/dokumentarkiv/regjeringen-stoere/andre-dokumenter/ud/2025/aktuelt/arbeidet-med-a-ferdigstille-endringer-i-eksportkontrollforskriften-er-i-sluttfasen/id3054211/

Saksfremlegg
Porteføljestyremøte 2/25

Sak PS-Forskningssystemet 25/25 Orienteringer

Til	Ansvarlig direktør	Saksbehandler	Vedlegg
Porteføljestyret for forskningssystemet	Johannes W. Løvhaug	Ingeborg Owesen / Seka Iraguha / Lillian Baltzrud	1. Langtidsmøteplan

Fra

Områdedirektør

Benedicte Løseth

ORIENTERINGSSAK

Forslag til vedtak	Porteføljestyret tar orienteringene til etterretning.
Kort bakgrunn	Orienteringer er en fast sak i møtene til porteføljestyret for forskningssystemet. Saken kan inneholde både skriftlige og muntlige orienteringer. Sistnevnte vil det orienteres om i møtet. Oppdatert langtidsmøteplan legges alltid ved.
Hvorfor saken fremmes til dette møtet	Porteføljestyret skal være kjent med pågående saker som angår deres ansvarsområder.

Hovedpunkter

1. Stortingsmelding om forskningssystemet (systemmeldingen)

Fredag 21. mars 2025 legges stortingsmeldingen om forskningssystemet fram. I porteføljestyremøtet vil det komme en kort, muntlig orientering om innholdet i stortingsmeldingen. I porteføljestyremøte 3/25 vil det legges fram en sak som redegjør nærmere for meldingens konsekvenser for forskningssystemet og evt. konsekvenser for porteføljestyrets ansvarsområder.

Det er to skriftlige orienteringer til møtet:

2. Prosess for oppdatering av Forskningsrådets Plan for kjønnsbalanse, kjønnsperspektiver og mangfold i forskning og innovasjon

Forskningsrådet skal i løpet av 2025 oppdatere vår Plan for kjønnsbalanse, kjønnsperspektiver og mangfold. Planen vil være utformet som en plan for Forskningsrådets arbeid på feltet. I den forbindelse ønsket vi innspill, og sendte ut en åpen høring med svarfrist 7. februar (Se Forskningsrådets nettsider for mer informasjon). Høringen var rettet til institusjonene, og ikke til enkeltforskere eller privatpersoner. I møte 3/25 får porteføljestyret forelagt et utkast til den nye planen, og får en mulighet til å komme med innspill til utkastet.

Følgende institusjoner svarte på høringen:

- Universitet/Høgskole (5): NHH, UiO, UiA, NTNU, UiB
- Fakultet/Institutt (2): Fakultet for helse- og sosial vitenskap, HVL og Senter for tverrfaglig kjønnsforskning, UiO
- Andre (1): Kif-komiteen

Kort oppsummering av innkomne innspill:

Når det gjelder kjønnsbalanse er det en utfordring at det stor forskjell mellom fag. Noen fag er fortsatt svært mannsdominerte, men andre fag er i ferd med å bli kvinnedominerte.

Hovedutfordringen med mangfold, er at det ikke er konsensus om hva begrepet viser til. Begrepet «mangfold» er stort og komplekst, noe som gjør det vanskelig å iverksette konkrete tiltak. «Mangfold i forskningssystemet» kan vise til en rekke dimensjoner, slik som mangfold i forskerkorpset, mangfold i tematiske forskningsområder, mangfold som fokus for undersøkelser i forskning, mangfold som anvendt perspektiv i forskningsprosjekter, mangfold i forskningsdesign og metodologi og mangfold i form av at ulike epistemiske kulturer er representert i et forskningsfelt. Mangfold forstås i dag altfor lett som majoritet/minoritet/etnisitet.

Foreslåtte tiltak er blant annet å revidere mal til prosjektbeskrivelse. Det foreslås at Forskningsrådet kan kreve at både kjønnsperspektiv og mangfold gjøres rede for, likeledes redegjørelse for sammensetning av forskerteamet (kjønnsbalanse).

Forskningsrådet oppfordres til å ha gode og informative nettsider om tematikken som er lette å finne fram i, samt å se på representasjon i våre egne kanaler, for eksempel ved inkluderende bildebruk og synliggjøring av forskere med ulike bakgrunner.

3. Panoramaseminar 2025

Forskningsrådet er medarrangør for Panoramaseminaret 2025. Seminaret arrangeres sammen med Direktoratet for kompetanse og høyere utdanning (HK-dir) og Norges Tekniske og Naturvitenskapelige Universitet (NTNU) den 11.-12. juni i Trondheim. Den overordnete tematikken for Panoramaseminaret 2025 er på hvilken måte internasjonalt kunnskapssamarbeid kan bidra til å løse de store kompetansebehovene vi står overfor. Forskningsrådet vil holde flere sesjoner om ansvarlig internasjonalt samarbeid, forskningssikkerhet og kunstig intelligens' påvirkning på samfunnet.

Forberedelse / prosess	Administrasjonen har utviklet saken.

Møteprotokoll

Porteføljestyre for Forskningssystemet, møte 2/2025

Dato	**Sted**
26. mars 2025, kl. 10.00-15.00	Digitalt på Teams

Til stede	Tanja Storsul, leder Ågot Aakra Sandrine Benard Astri Dankertsen Magnus Gulbrandsen Ingeborg Palm Helland Marit Lofnes Mellingen Dagfinn Myhre Tove Klæboe Nilsen David Budtz Pedersen Rebekka Borsch Sven Stafström Gørill Kristiansen, observatør KD Kristin Celius, observatør KLD
Forfall	Rune Dahl Fitjar
Til stede fra Forskningsrådet	Benedicte Løseth, områdedirektør Johannes Waage Løvhaug, avdelingsdirektør Solveig Flock, avdelingsdirektør Rune Vistad, avdelingsdirektør Lillian Baltzrud, porteføljestyrekoordinator Heidi Dybesland, referent Espen Sandøe Karlsen, sak 19/25 John Baarli, sak 19/25 Seka Iraguha, sak 20/25 Marianne Jensen, sak 20/25 Kristin Danielsen, sak 21/25 Kirsti Solberg Landsvik, sak 23/25
Sak PS-Forskningssystemet 16/25	**Godkjenning av sakslisten**
Vedtak:	Porteføljestyret for forskningssystemet godkjenner sakslisten.
Sak PS-Forskningssystemet 17/25	**Godkjenning av møteprotokoll**
Vedtak:	Porteføljestyret godkjente møteprotokollen
Sak PS-Forskningssystemet 18/25	**Spørsmål om habilitet**

Vedtak:

I dette møtet skal porteføljestyret beslutte tildeling og avslag til søknader til nasjonale forskerskoler, PS-FS sak 19/25.

Forskningsrådets administrasjon har foretatt en habilitetsvurdering, og følgende porteføljestyremedlemmer er inhabile og fratrer derfor når sak 19/25 diskuteres i porteføljestyretstyremøtet:

- Tanja Storsul, som er inhabil for behandling av søknadene 356538, 356534, 356488, 356464, 356560, 356599, 356490, 356427, 356390, 356423 og 356569.
- Tove Nilsen Klæboe, som er inhabil for behandling av søknadene 356499, 356550, 356464, 356520 og 356488.
- Ågot Aakre, som er inhabil for behandling av søknadene 356560 og 356390.
- Dagfinn Myhre, som er inhabil for behandling av søknadene 356462, 356560 og 356569.
- Astri Dankertsen, som er inhabil for behandling av søknaden 356499.
- Rune Dahl Fitjar, som er inhabil for behandling av søknadene 356477 og 356560.

For å sikre at porteføljestyret er beslutningsdyktig i saken er professor Barabara van Loon, ved Institutt for klinisk og molekylær medisin ved NTNU, oppnevnt som settemedlem. Van Loon er medlem i Porteføljestyret for banebrytende forskning og er valgt ut fordi hun har kompetanse om saken. Habilitet er kartlagt i forkant av oppnevningen.

Siden porteføljestyreleder Tanja Storsul er inhabil i saken, er porteføljestyremedlem Sven Stafström oppnevnt som setteleder under behandling av saken.

Sak PS-Forskningssystemet 19/25

Søknadsbehandling nasjonale forskerskoler [U.off. § 14]

Vedtak:

Porteføljestyret tildeler 80 millioner kroner til søknader som kom inn til utlysningen nasjonale forskerskoler for arbeidslivsrelevans, med søknadsfrist 13.11.2024.

Søknadsbehandlingen har fulgt prosedyren som ble vedtatt i porteføljestyremøte 1/25 5. februar 2025, sak 11/25.

Avslag en bloc:

Alle søknader med gjennomsnittskarakter under 5 fra ekspertpanelet, avslås en bloc i tråd med vedtatt prosedyre.

Søknader som får vedtak om tildeling:

Pro-sjektnr	Prosjekttittel	Prosjekt-ansvarlig	Prosjekt-leder	Tildelt inntil (mill.kr)

Øvrige søknader avslås da de ikke nådde opp i konkurransen.

Innstilt beløp er en øvre ramme. Beløp og støtteandel vil kunne bli justert. Administrasjonen gis fullmakt til å fatte endelig beslutning om tildeling av midler basert på innhenting og vurdering av revidert søknad med obligatoriske vedlegg.

Sak PS-Forskningssystemet 20/25 **INTPART: Deltagelse fra HK-dir**

Vedtak: Representanter fra administrasjon i Direktoratet for høyere utdanning og kompetanse (HK-dir) inviteres til å være til stede i porteføljestyremøter under behandlingen av saker som gjelder INTPART-ordningen

Sak PS-Forskningssystemet 21/25 **Internasjonal stimuleringspott: ytterligere kriterier for bruk og bevilgning U.off. § 14**

Vedtak: Porteføljestyret for forskningssystemet vedtar to nye kriterier for bruk av internasjonal stimuleringspott, som kommer i tillegg til kriteriene vedtatt i møte 1/25 5. februar. I tillegg vedtas det en investering til internasjonal stimulering.

Porteføljestyret for forskningssystemet vedtar følgende nye kriterier:

A. Geografi – prioriterte områder eller land; Nordiske land inkludert Baltiske land, Panoramaland (USA, Canada, Brasil, Sør-Afrika, Japan, India, Kina, Sør-Korea, Russland (Russland er p.t ekskludert)), Ukraina, Tyskland, UK og Frankrike, samt Afrikanske land.

B. Multilateralt utlysningssamarbeid og instrumenter som stimulerer til økt internasjonalt samarbeid prioriteres

C. Bidrag fra internasjonal stimuleringspott til internasjonale fellesutlysninger der Norges bidrag er ubalansert i forhold til andre land eller i spesielle tilfeller der Norge (etter søknadsbehandling) har havnet i en situasjon der vi blokkerer innvilgelseslisten. I begge tilfeller har ikke ansvarlig porteføljestyre mulighet til å øke bevilgningen. Bevilgning fra internasjonal stimuleringspott kan ikke overstige bidrag fra ansvarlig porteføljestyre.

Investering:

Porteføljestyret for forskningssystemet vedtar bruk av den internasjonale stimuleringspotten for 2026 til:

10 millioner kroner til en utlysning mellom flere land med tittel: «Klimatjenester for å redusere risiko i Vest Afrika». Utlysningen er allerede finansiert med 20 millioner kroner fra porteføljestyre for Klima og polar, men oppfyller flere av kriteriene for medfinansiering fra Internasjonal stimuleringspott, som beskrevet i saken.

Samlet bevilgning for 2025 utgjør nå 91 - 97 millioner kr og 55 millioner kroner for 2026.

Sak PS-Forskningssystemet 22/25 **Refleksjonsnotat 2025 U.off. § 14**

Vedtak:	Porteføljestyret for forskningssystemet slutter seg til disposisjon og tematikk foreslått av arbeidsutvalget for refleksjonsnotat 2025. Arbeidsutvalget gis mandat til å arbeide videre med refleksjonsnotatet i tråd med dette og evt. kommentarer som kom fram i diskusjonen i porteføljestyremøtet.
Sak PS-Forskningssystemet 23/25	**Arbeidet med oppdatering av norsk veikart for forskningsinfrastruktur og ny utlysning** ***U.off. § 14***
Vedtak:	Administrasjonen arbeider videre med oppdateringen av veikartet og utforming av ny utlysning på grunnlag av kommentarer og innspill fra Porteføljestyret for forskningssystemet.
Sak PS-Forskningssystemet 24/25	**Forskningssikkerhet**
Vedtak:	Porteføljestyret tar orienteringen om arbeidet med forskningssikkerhet, ny portefølje for forsvar og sikkerhet og utarbeidelsen av et kunnskapsgrunnlag for vurdering av sensitive teknologiområder (KVAST) til etterretning. Administrasjonen tar med seg innspill fra porteføljestyret i det videre arbeidet.
Sak PS-Forskningssystemet 25/25	**Orientereringer**
Vedtak:	Porteføljestyret for forskningssystemet tar orienteringene til etterretning.
Sak PS-Forskningssystemet 26/25	**Evaluering av møtet**
Sak PS-Forskningssystemet 27/25	**Møteprotokoll godkjennes**
Vedtak:	Porteføljestyret for forskningssystemet godkjenner møteprotokollen.