Kunnskapsgrunnlag for vurdering av sensitive teknologier (KVAST)

Risikovurdering for utvalgte teknologiområder

Delleveranse 4

Rapport fra Nasjonal sikkerhetsmyndighet, Forsvarets forskningsinstitutt og Norges forskningsråd

Om KVAST-oppdraget

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. Se oppdragsbeskrivelse.

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

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

Kunnskapsgrunnlaget som etableres gjennom dette skal bidra til å:

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

Om delleveranse 4

Oppdragsbeskrivelsen for delleveranse 4:

> Basert på funn fra delleveranse 2 og delleveranse 3 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.
>
> Resultatet av disse analysene skal kunne samles i en oversikt som det er ønskelig å dele bredest mulig.

Delleveranse 4 er i hovedsak utført av Nasjonal sikkerhetsmyndighet (NSM), med bidrag fra Forsvarets forskningsinstitutt (FFI) og Norges forskningsråd.

Risikovurdering av sensitive teknologier

Definisjoner

Risiko

Risiko kan defineres som usikkerheten knyttet til om en uønsket hendelse vil inntreffe og hvilke konsekvenser den vil ha. Når det gjelder sensitive teknologier handler dette om faren for at teknologiske løsninger, enten ved uautorisert adgang, målrettet hacking, manipulering eller annen form for misbruk, kan skade nasjonale sikkerhetsinteresser eller grunnleggende nasjonale funksjoner[1].

Risiko oppstår når en teknologi med høy strategisk verdi for nasjonale sikkerhetsinteresser både har interne sårbarheter og utsettes for et aktivt eksternt trusselbilde.

Risikovurdering

En risikovurdering er en systematisk prosess der risiko identifiseres, analyseres og evalueres. I prosessen vurderes hvilke sårbarheter verdien har og hvilke trusler som kan føre til helt eller delvis bortfall av verdien.[2] Vurderingen gir et grunnlag for anbefalinger av tiltak som bør gjennomføres for å redusere risiko.

NSM bruker begrepene *verdi*, *trussel* og *sårbarhet* i sine risikovurderinger, der kombinasjonen av faktorene beskriver den samlede risikoprofilen. For sensitive teknologier er risiko som samspillet mellom tre kjernekomponenter: teknologiens verdi, teknologiens sårbarheter og det eksterne trusselbildet.

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

Den samlede risikoen estimeres som et produkt av hvor kritisk teknologien er for nasjonal sikkerhet, hvor utsatt den er for interne angrepsflater, og hvor aktivt det eksterne trusselbildet er. Høy teknologisk verdi, kombinert med betydelige sårbarheter og et aktivt trusselbilde, gir særlig høy risiko for misbruk.

---

[1] Grunnleggende nasjonale funksjoner er definert som «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser», jf. sikkerhetsloven § 1-5 nr. 2.

[2] NS 5814:2021+AC:2023

Metodikk for risikovurdering

Det finnes mange ulike metoder for å gjennomføre risikovurdering, og valg av tilnærming og detaljeringsgrad er avhengig av formålet og rammene.[3] I prosjektet er det gjennomført brede litteratursøk for å identifisere eksisterende teori og modeller for risikovurdering av teknologi. Gjennom søk ble det ikke funnet noen risikovurderingsmetode som er særlig egnet for vurdering av teknologier.[4]

I fravær av eksisterende rammeverk for risikovurdering, har prosjektgruppen utarbeidet en skreddersydd metode for risikovurdering av sensitive teknologier. Metoden er basert på en kvalitativ tilnærming til risikoanalyse der sannsynligheter og konsekvenser blir bestemt rent kvalitativt, og der det benyttes ord for å beskrive frekvens og alvorlighetsgrad.

Metodikken måler risiko med seks kriterier, valgt med utgangspunkt i oppdragsbeskrivelsen, omtale i liknende internasjonale vurderinger (fra bl.a. EU og USA), samt nasjonal sikkerhetsstrategi, og supplert med innspill fra prosjektgruppen. De opplistede kriteriene måles på en skala fra **lav til svært høy** (lav, middels, høy, svært høy)[5] ved hjelp av indikatorer som er utarbeidet for formålet (tabell 1). Deretter gjøres en totalvurdering av risiko, basert på utfallet av vurderingene for hvert kriterium. Resultatene fremstilles grafisk i slutten av risikovurderingen for hver teknologi. For å fremstille resultatene av risikovurderingene grafisk, er de ulike risikonivåene gitt en numerisk score fra 1 (lav) til 4 (svært høy). Totalvurderingen er ikke et gjennomsnitt av risikoutfallet på de ulike kriteriene, men er i stedet en skjønnsmessig vurdering av den totale risikoen.

Kriterier for risikovurdering

Følgende kriterier er benyttet i denne risikovurderingen:

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

[3] FFI Norsk rapport

[4] Nasjonal sikkerhetsmyndighets veileder «Risikovurdering av IKT-systemer» en praktisk metodikk for å kartlegge og redusere risiko i ugraderte IKT- og OT-systemer, og gir ikke det metodiske rammeverket som trengs for helhetlige risikovurderinger av teknologiområder.

[5] Risikovurderinger måler oftest risiko på en skala lav – høy. For denne rapporten er det imidlertid besluttet å benytte skala lav – svært høy. Årsaken er at typen teknologi som skal vurderes (sensitive teknologier) på bakgrunn av sin natur ofte vil oppnå høy risiko. Svært høy er derfor lagt til på skalaen for å gjøre det mulig å skille mellom teknologiene.

Eksponering for utenlandske aktører

Kriteriet måler hvorvidt teknologien eller forskning på teknologien kan være eksponert for påvirkning fra utenlandske aktører. Eksponering kan blant annet skje gjennom kompetanseoverføring, altså at aktørene kan få tilgang til, påvirke eller tilegne seg kunnskap og kompetanse gjennom felles prosjekter, åpne foredrag eller konferanser, internasjonale samarbeid, eller andre kontaktflater**.** Eksponering kan også skje gjennom målrettede etterretningshandlinger, altså at statsnære aktører kan innhente, påvirke eller degradere norsk teknologi, data og kunnskap gjennom åpen eller skjult etterretningsaktivitet. Dette inkluderer målrettet spionasje mot personer, miljøer, systemer og leverandørkjeder. Slike aktiviteter kan måles basert på data tilgjengeliggjort i åpne trussel- og risikovurderinger.

Med utenlandske aktører menes her land Norge ikke har sikkerhetssamarbeid eller på andre måter er allierte med. Kriteriet knytter ikke risiko til aktører som Norge har allianser til, eller som ellers er prioriterte partnerland. Høyest risiko knyttes til samarbeid med land som er direkte nevnt i åpne risiko og trusselvurderinger som land som kan (ønske å) skade nasjonale sikkerhetsinteresser, der det er identifisert innhentingsinteresse eller forsøk på innhenting.

Risiko ved eksponering påvirkes også av Norges internasjonale posisjon på teknologiområdet. Dersom Norge ikke er ledende og kunnskapsbasen er svakere, vil nytteverdien for ikke-allierte være begrenset. Da kan risikoen ved eksponering være lavere enn gevinsten Norge får gjennom bredt internasjonalt samarbeid. Når Norge derimot ligger i front, øker verdien av innsyn i metoder, data og praksis. I slike tilfeller blir risikoen for innhenting og ulovlig kunnskapsoverføring høyere dersom teknologiområdet eksponeres for utenlandske aktører utenfor våre allianser.

Regulatorisk kontroll og etterlevelse

Kriteriet måler hvor godt et teknologiområde er dekket av gjeldende regelverk. Dette inkluderer internasjonale traktater og ordninger Norge har sluttet seg til, nasjonale lover og forskrifter. Kriteriet ser både på hvorvidt det finnes relevant regelverk, hvorvidt regelverket er oppdatert i forhold til teknologiutvikling eller flerbrukspotensialer, i tillegg til hvorvidt kravene er så tydelige at aktører faktisk kan etterleve dem uten å trå feil.

I tillegg måler kriteriet håndheving i praksis, altså kapasitet og evne til å oppdage brudd, iverksette sanksjoner og drive veiledning; tilgjengelighet av kontrollmekanismer (tilsyn, revisjon, sporbarhet) og faktisk etterlevelse hos virksomheter og samarbeidspartnere. Vurderingene baserer seg på dokumenterte saker, etterlevelsesmålinger og modenhet i styringssystemer som indikator på om reglene virker etter hensikten og om aktører får tilstrekkelig veiledning til å gjøre rett.

Lav risiko knyttes til der teknologien er tydelig regulert av et modent, oppdatert og harmonisert regelverk, hvor kravene er forståelige, kontrollmekanismer fungerer, og brudd blir oppdaget og får konsekvenser. Høy risiko finnes der regelverket er mangelfullt, utdatert eller uklart, for eksempel ved nye/raskt utviklende/flerbruksteknologier, eller dersom håndhevingen er svak slik at brudd skjer uten oppfølging, eventuelt der aktører misforstår krav fordi veiledning og praktisk tolkning mangler.

Potensiell militær eller strategisk utnyttelse

Kriteriet skal fange opp om teknologien har egenskaper som kan styrke offensive eller defensive kapabiliteter, påvirke etterretning og overvåking, eller gi strategiske fordeler som undergraver Norges forsvars- og beredskapsmål. Systemmeldingen diskuterer teknologier som kan ha både militær relevans og nytteverdi[6]. EOS-tjenestene peker på at sentrale aktører vil kunne gjennomføre åpne og fordekte forsøk på å tilegne seg kunnskap og teknologi som kan brukes til å styrke landenes militære kapasitet og i så måte forringe Norges nasjonale forsvarsevne. Særlige utfordringer er knyttet til flerbruksteknologier, der løsninger utviklet for sivile formål også kan ha klar militær nytteverdi.

Kriteriet ser på muligheten for at teknologien har sivil eller militær hovedbruk, og i hvilken grad teknologien er sentral i offensive eller defensive militære operasjoner. Risikoen vurderes som høyest der teknologien kan gi tydelig effekt i offensive operasjoner, redusere norsk evne til å oppdage og motvirke trusler, eller bidra til kapasitetsbygging hos aktører som kan skade norske interesser.

Konsekvenser for kritisk infrastruktur

Kriteriet vurderer i hvilken grad teknologien er nødvendig for å opprettholde eller gjenopprette samfunnets kritiske funksjoner**,** og hvilke samfunnsmessige konsekvenser misbruk eller bortfall kan få.

Kriteriet ser blant annet på teknologiens systemrolle, altså i hvilken grad den understøtter en eller flere kritiske infrastrukturer, og hvorvidt teknologien er kjerne eller perifer i understøttelsen. Videre vurderes potensiell systemsvikt ved misbruk, varighet og utbredelse av konsekvenser, samt grad av reservekapasiteter og omstillingsevne**.** Lav risiko knyttes til der teknologien har liten eller begrenset betydning for infrastruktur og eventuelle avbrudd er kortvarige uten vesentlige samfunnsfølger. Høy risiko knyttes til tilfeller der teknologien er systemkritisk og bortfall kan gi langvarige, omfattende samfunnskonsekvenser for kritiske funksjoner, særlig der det mangler reservesystemer eller alternative løsninger.

Påvirkning på økonomisk sikkerhet målt i tilgang på strategisk kunnskap og kompetanse

Kriteriet måler konsekvensen for økonomisk sikkerhet dersom Norge mangler eller mister tilgang til strategisk viktig kunnskap og kompetanse innen et teknologiområde. I tråd med den nasjonale sikkerhetsstrategien[7] forstås økonomisk sikkerhet her som evnen til å bevare konkurransekraft og omstillingsevne, og til å forstå og anvende ny teknologi. Vi vurderer derfor nasjonal posisjon (ledende/gap/avhengighet), kvalitet og omfang av forskningsaktivitet, robusthet i kompetansemiljøer, rekrutterings- og utdanningskapasitet, samt muligheten for å dekke behov gjennom trygge partnerland (EU/EØS, NATO, prioriterte partnere).

Lav risiko gis der det finnes bred og stabil kompetansebase, høy forskningstetthet og -kvalitet, og gode rekrutteringsmuligheter fra norske miljøer og/eller partnerland. Høy risiko gis der forskning og

[6] Meld st. 14 (2024-2025) Sikker kunnskap i en usikker verden
[7] Nasjonal sikkerhetsstrategi - regjeringen.no

kompetanse er svært begrenset eller svak, der det foreligger kritisk kunnskapsmangel, eller der tilgangen i praksis er avhengig av usikre partnere som kan utebli. Datagrunnlaget inkluderer blant annet kilder om forskningskvalitet.

Respekt for menneskeverd

Kriteriet måler i hvilken grad teknologien fremmer eller undergraver menneskeverd og menneskerettigheter, herunder individets autonomi, privatliv, rettferdig behandling og mulighet til å delta i demokratisk meningsdannelse. I vurderingen ser vi særlig på om teknologien samler eller behandler av personopplysninger (bl.a. biometriske data), hvor omfattende og sensitive disse er, om formål og hjemmelsgrunnlag er tydelige, og om innsamlingen skjer med nødvendig transparens, kontroll og etterprøvbarhet.

Lav risiko knyttes til teknologier som ikke samler inn persondata, eller kun samler inn data i begrenset omfang med tydelig hjemmel, informert samtykke, åpenhet om formål og solide kontrollmekanismer. Høy risiko knyttes til teknologier som muliggjør vedvarende overvåking eller omfattende innhenting av person- og biometriske data uten tilstrekkelig rettslig grunnlag, uten transparens og uten effektive mekanismer mot misbruk, særlig der dette kan lede til systematiske inngrep i privatliv, urettferdig forskjellsbehandling eller nedkjølende effekter på ytrings- og deltakelsesfrihet.

Fullstendig indikatorkart

Tabell 1 Oversikt over kriterier og indikatorer

Kriterium / Indikator	Lav	Middels	Høy	Svært høy
Eksponering for utenlandske aktører	Samarbeid med allierte, lav sårbarhet i kompetanseoverføring og ingen kjente etterretningstrusler.	Hovedsakelig samarbeid med allierte, noe med ikke-allierte. Middels sårbarhet og noe interesse fra aktører som kan true nasjonal sikkerhet.	Markant samarbeid med ikke-allierte, stor kompetansesårbarhet og dokumenterte etterretningstrusler.	Avhengighet av ikke-allierte, betydelig manipulasjons- og innhentingsrisiko. Flere dokumenterte forsøk på innhenting.
Regulatorisk kontroll og etterlevelse	Teknologien er godt dekket av regelverk, nasjonalt eller internasjonalt med få gråsoner. Håndheving av regelverket er aktiv og god, med effektivt tilsyn. God etterlevelse.	Noen gråsoner og uklarheter i regelverket grunnet teknologiutvikling eller flerbruk. Middels god håndheving. Kontroll og oppfølging varierer, enkelte svakheter i etterlevelse.	Regelverket er umodent eller ikke tilpasset dagens behov, med klare hull.. Håndheving er mangelfull; alvorlige brudd kan overses. Etterlevelse er lav med lav forståelse av regelverket.	Uklare eller fraværende rammer eller ikke oppdatert regelverk. Manglende modenhet i oppdaterte regelverk. Håndheving og kontroll er fraværende. Forståelse og etterlevelse er fraværende.
Potensiell militær eller strategisk utnyttelse	Marginal eller ingen militær verdi; teknologien har få eller ingen militære anvendelsesområder (eks. flerbruk). Misbruk påvirker ikke forsvarsevnen.	Noe militær verdi, men hovedsakelig sivilt bruk. Misbruk gir begrenset innvirkning på nasjonal forsvarsevne og alliert samhandling.	Vesentlig militær-strategisk verdi i flere kapasiteter.. Hovedsakelig militær hovedbruk. Misbruk kan svekke nasjonal forsvarsevne og alliert samhandling.	Kritisk for strategiske og offensive/defensive kapabiliteter. Tap eller misbruk gir svært alvorlig skade på den nasjonale forsvars- og beredskapsevnen.
Betydning for kritisk infrastruktur	Teknologien har begrenset betydning for kritisk infrastruktur. Svikt eller misbruk gir liten eller ingen samfunnseffekt. Høy redundans og solid sikring.	Viktig for én kritisk kjede med noe redundans. Svikt gir noen kortvarige konsekvenser, men er ikke kritisk. Sikkerheten er god, men noen svakheter og varierende beredskap.	Viktig for flere kritiske infrastrukturer, med lav redundans. Svikt eller misbruk gir store og merkbare konsekvenser. Sikkerhet og beredskap er utilstrekkelige.	Systemkritisk rolle, lav eller ingen redundans. Svikt eller misbruk gir langvarige samfunnskonsekvenser med nasjonale kaskadeeffekter. Infrastrukturen er sårbar og dårlig sikret.
Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse	Høy forskningsaktivitet og kvalitet. Bred, robust tilgang på strategisk kunnskap/kompetanse, god rekruttering fra EU/EØS/NATO-land. Lite avhengighet av partnere uten sikkerhetssamarbeid.	Middels forskningsaktivitet og kvalitet, noe fragmentert tilgang på kritisk kunnskap. Moderat avhengighet og rekruttering, samarbeid primært med sikre partnere, men noe utenforliggende forekommer.	Lav forskningsaktivitet/ kvalitet, mangelfull tilgang og høy personavhengighet. Stor avhengighet av partnere uten sikkerhetsavtaler og svak rekruttering fra sikre land, hyppig tap av kompetanse. Fare for norsk konkurranseevne.	Svært lav forskningsaktivitet/kvalitet og kritisk mangel på kunnskap/kompetanse. Kritisk avhengighet av usikre partnere, minimal rekruttering fra EU/EØS/NATO-land, stor risiko for tap av samfunnsviktige funksjoner og norsk konkurranseevne.
Respekt for menneskeverd (personvern, rettferdighet, demokrati)	Minimal innsamling/overvåking. Klare hjemler og personverntiltak.. Høy transparens og tydelig etterlevet formål.	Moderat bruk av persondata. Klare hjemler og personverntiltak. Etterlevet formål og middels høy transparens.	Omfattende databruk og overvåking, svekket personvern. Risiko for urimelig inngripen. Tvetydig formål og lav transparens.	Systematisk innhenting og misbruk av persondata, fravær av personvern og rettigheter. Formål er ikke etterlevet, og transparens er fraværende.

Caseutvalg

Prosjektgruppen har utarbeidet en anbefalt oversikt over sensitive teknologier for norske forhold med utgangspunkt i EUs oversikt over kritiske teknologier. Oversikten er sammenliknet med informasjon fra andre lands oversikter over kritiske eller sensitive teknologier. Den endelige oversikten omfatter 48 teknologier, fordelt på 11 overordnede kategorier. Gitt tilgjengelig tid og ressurser er det ikke mulig å gjennomføre risikovurderinger for alle teknologiene. Vi har derfor gjort et utvalg basert på tydelige kriterier, og med støtte i funn fra KVAST delleveranse 3.

Som et minimumsprinsipp valgte vi minst en teknologi fra hver av de 11 kategoriene i oversikten, for å sikre tilstrekkelig bredde i vurderingene. Videre prioriterte vi teknologier som i data fra delleveranse 3 enten har rapportert høy forskningsaktivitet, vurderes av fagmiljøene selv som særlig sensitive, eller er rapportert som å ha høyt potensiale for militær eller strategisk bruk. Med bakgrunn i dette ble 14 teknologier valgt til risikovurdering (tabell 2).

Metodiske begrensninger

Teknologiene som vurderes er i utgangspunktet regnet som sensitive, ettersom de er hentet fra en oversikt over sensitive teknologier for norske forhold. Selv om metodikken kun er anvendt på 14 underkategorier, betyr ikke det nødvendigvis at disse områdene har høyere iboende risiko enn de øvrige. Vurderingene som presenteres er heller ikke noe «fasitsvar» for all risiko i hele teknologiområdet. Vurderingene som er gjennomført, er gjort på brede underkategorier. Når én kategori rommer teknologier med svært ulike formål, modenhet og risikoflater, vil noen delteknologier nesten alltid skåre høyt på ett eller flere kriterier. Det øker risikoen for å bli upresis, og skåren kan fange ytterpunkter snarere enn et representativt gjennomsnitt.

Det at mange av teknologiene har samlet vurdering «høy» eller «svært høy», betyr heller ikke nødvendigvis at samarbeid med utenlandske aktører bør begrenses, eller at tiltak må innføres på all forskning innenfor disse teknologifeltene for å skjerme eller beskytte forskningen. Risikoen kan også knyttes til at det er viktig for norske sikkerhetsinteresser å tilegne seg kunnskap og kompetanse gjennom samarbeid. Vurderingene synliggjør denne kompleksiteten. De er ment som eksempler på hvordan risikovurderinger *kan* gjennomføres, og som utgangspunkt for videre, mer detaljerte analyser.

Prosjektgruppen vurderte også flere andre kriterier utover dem som ble tatt med i modellen, blant annet teknologiens modenhetsnivå målt på TRL-skalaen, teknologiens muliggjørende potensiale, og sårbarhet for cyberangrep. Sårbarhet for cyberangrep ble ikke vurdert som relevant fordi det ikke er et kriterium som det er hensiktsmessig å måle på alle typer teknologier (for eksempel ikke-cybersikkerhetsteknologier). Teknologiens muliggjørende potensiale, altså hvorvidt den er viktig for ingen, noen få, eller flere grunnleggende nasjonale funksjoner, samt teknologiens modenhetsnivå (TRL) og anvendelse ble ikke tatt med i modellen fordi underkategoriene som analysen skulle gjennomføres på var for brede til at kriteriene ga noen verdi i risikovurderingen. Teknologiens muliggjørende potensiale ble beholdt som en generell beskrivelse for hver teknologi. Når det gjelder teknologiens modenhet ble denne tatt ut av modellen fordi kategoriene som er valgt ut for analysen nesten alltid vil romme bredden av TRL-skalaen, og resultatet vil nesten alltid være svært høyt (høy modenhet/bruk). Imidlertid kan teknologier med høy modenhet når det gjelder anvendelse, øke sannsynligheten for misbruk og konsekvensen ved bortfall. Dette kan det være relevant å se nærmere på i videre arbeid.

Kildegrunnlag

Analysen bygger på et sammensatt grunnlag: åpne trussel- og risikovurderinger fra norske myndigheter (PST, NSM og Etterretningstjenesten) for å beskrive trusselaktørers kapasitet, modus og intensjon; KVAST-prosjektets egne delleveranser for metode, datagrunnlag og sektorspesifikke funn; samt relevante lov- og regelverk, herunder eksportkontroll (DEKSA-listene) og annet nasjonalt og internasjonalt regelverk som rammer teknologibruk, samarbeid og kunnskapsoverføring. I tillegg er NIFUs rapport (2025:17) brukt for å belyse forskningstrender, samarbeid, mobilitet og kompetansesituasjon på tvers av teknologiområder.

Tabell 2 Teknologiområder som vurderes med hensyn til risiko

De 11 hovedkategoriene		**De 14 underkategoriene som er valgt ut for nærmere risikovurdering**	
1	**Avanserte halvlederteknologier**	1	Fotonikkteknologier, inkludert høyenergilaser
2	**Teknologier med kunstig intelligens**	2	Dataanalytiske teknologier
		3	Maskinlæring og dyplæring
3	**Kvanteteknologier**	4	Kvantesensorer og -radar
4	**Bioteknologier**	5	Syntetisk biologi
5	**Avansert samband, navigasjon og digitale teknologier**	6	Cybersikkerhetsteknologier, inkludert cyberovervåkning og sikkerhets- og inntrengningssystemer, og digital etterforskning
		7	Styrings-, navigasjons- og kontrollteknologier, inkludert avionikk og maritim posisjonering
6	**Avanserte sensorteknologier**	8	Elektrooptiske, kjemiske, biologiske og distribuerte sensorer, radar- og strålingssensorer
7	**Romfarts- og fremdriftsteknologier**	9	Romovervåknings- og jordobservasjonsteknologier
8	**Energiteknologier**	10	Kraftteknologier, inkludert smarte strømnett, energilagring og batterier
9	**Robotikk og autonome systemer**	11	Ubemannede farkoster (i luft, på land, på overflaten og under vann)
		12	KI-drevne systemer
10	**Avanserte materialer, produksjons- og resirkuleringsteknologier**	13	Teknologier for nanomaterialer, smarte materialer, avanserte keramiske materialer, lavsignaturmaterialer og trygge materialer utformet med tanke på sikkerhet og bærekraft
11	**Undervannsteknologier**	14	Undervannsposisjonering og navigasjon, inkludert sonarbasert navigasjon, terrengkorrelering og treghetsnavigasjon

Risikovurdering av sensitive teknologier

1. Fotonikkteknologier, inkludert høyenergilaser

Fotonikk er generering, styring og oppdagelse av lys for å overføre og behandle informasjon og kontrollere ulike fysiske prosesser. Kategorien inneholder blant annet våpen for rettet energi. Feltet har bruksområder som spenner fra kommunikasjon og sensorer, til additiv produksjon, industriell måling, medisinsk instrumentering og militær bruk som målavstandsmåling og ildledelse. Teknologien er bredt muliggjørende og understøtter en rekke grunnleggende nasjonale funksjoner, særlig digital infrastruktur, etterretning og situasjonsforståelse.

Eksponering for utenlandske aktører – MIDDELS RISIKO

Det foreligger vedvarende innhentingsinteresse for norsk teknologi og kunnskapsoverføring fra stater som Norge ikke har sikkerhetssamarbeider med. Fotonikk og laser har tydelige flerbrukspotensiale og våpen for rettet energi har klar militær bruk. Flere åpne trusselvurderinger beskriver fordekte innhentingsoperasjoner, og bruk av studenter og forskere, for å få tilgang til sivil teknologi med formål om militær sluttbruk.[8] Trusselvurderinger peker i tillegg på økende militær anvendelse av laser, blant annet innen romdomenet. Industrispionasje er kjent problem, og ikke-allierte (spesielt Russland, Kina, Iran) har vist særskilt stor interesse for tilgang og kunnskapsoverføring.

På fotonikk er Kina tredje største samarbeidsland og Iran er tiende største samarbeidsland når det gjelder publiseringer. Med henholdsvis 43 og 15 sampubliseringer i perioden 2015-2024 tilsvarer det likevel under en håndfull artikler årlig. Tallene måler antall artikler og ikke forfatterandeler. Mål for iranske forfatterandeler viser at antall forfatterandeler iranske forskere har i artikler der Norge også er med som samarbeidspartner er svært lave, hvilket indikerer at artikkelsamarbeid der både norske og iranske forskere er med ofte involverer mange forskere fra mange forskjellige land. Selv om slike samarbeid rett nok representerer et kontaktpunkt mellom norske og iranske forskere og miljøer, utgjør de sannsynligvis en marginal risiko for uønsket teknologioverføring. Dette reflekteres også i siteringsanalysen hvor Iran ikke figurerer på noen av listene over land Norge sampubliserer mest med når det gjelder høyt siterte artikler. Russland og Nord-Korea har svært begrenset eller ingen betydning som samarbeidspartnere innen avanserte halvledere. Samarbeidet med Kina har imidlertid vært stabilt og betydelig over tid, både i volum og kvalitet[9].

Når det gjelder hvor attraktiv Norge er å samarbeide med, viser NIFUs analyse at det generelle bildet er at norske institusjoner har siteringstall under verdensgjennomsnittet innen *avanserte halvlederteknologier.* Volumet på publiseringen er heller ikke stor. Avanserte halvlederteknologier er blant hovedkategoriene som har lavest vekst i publisering i perioden 2015-2024 (fra 66 til 125 artikler, dvs. en vekst på 90 prosent). Samtidig viser Forskningsrådets evalueringen av matematikk, informatikk og teknologi (2023-2024) at Norge har miljøer som regnes som internasjonalt ledende.

Samlet vurderes risiko som middels i norsk kontekst, gitt det begrensete samarbeidet. Flere institusjoner har oppgitt i samtalene med prosjektgruppen at de ikke lenger ansetter personer fra

[8] PST, nasjonal trusselvurdering 2024
[9] NIFU Rapport 2025:17

Iran og Kina. Det er noe nedgang i samarbeidet fra 2023-2024. FoU-samarbeid er et mulig risikoelement som det er viktig å følge med på fremover.

Regulatorisk kontroll og etterlevelse – MIDDELS RISIKO

Fotonikk er dekket av modne, harmoniserte rammeverk for både sivile, flerbruks- og rent militære anvendelser. Direktoratet for eksportkontroll og sanksjoners Vareliste II over flerbruksvarer[10] speiler EUs dual-use-forordning og er direkte relevant for fotonikk i sivil og militær bruk. Vareliste I speiler EU Common Military List og dekker militære systemer som våpen for rettet energi.

Risiko vurderes som middels. Selv om regelverket er modent og godt dekkende kan etterlevelse i praksis oppstå gråsoner der prosjekter er FoU-tunge, internasjonale og flerbruksnære. Teknologien er fragmentert mellom sivile og militære domener, og det kan være vanskelig å sikre full etterlevelse, særlig i FoU-prosjekter.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Fotonikk er kjerne i både offensive og defensive systemer og har høy sannsynlighet for bruk. Teknologien vokser raskt i både sivil og militær sektor. Lasere benyttes til målavstandsmåling, ildledelse, blinding/forstyrring av sensorer, og har kapabilitet til å bekjempe droner, missiler og kjøretøy. Rettet energi-våpen vurderes som et paradigmeskift for fremtidens forsvarssystemer. Systemene er direkte sentrale for defensive/offensive systemer og integreres i våpenplattformer (land, luft og sjø).

Ringvirkningene for nasjonale forsvars- og beredskapsmål ved misbruk er betydelige. Underliggende fotonikk muliggjør kritiske funksjoner i sensorkjeder, kommunikasjon og presisjonsstyring. Kapasitetsforskyvning eller degradering kan føre til følgeeffekter for beredskap, transport, energi og situasjonsforståelse. Samlet gir dette en totalvurdering på svært høy.

Betydning for kritisk infrastruktur – HØY RISIKO

Fotonikk er kjerne i flere kritiske funksjoner i kommunikasjon (fiberoptikk, lasersamband), overvåking (LIDAR), og prosessindustri. Manipulasjon eller degradering av teknologien kan ramme samfunnet bredt. Våpen for rettet energi kan brukes til å forstyrre/ødelegge elektronikk og sensorer, noe som kan lamme kritiske infrastrukturer innen samferdsel, strømforsyning og offentlig sikkerhet dersom systemene misbrukes eller kompromitteres. Svikt eller misbruk kan gi store forstyrrelser og i enkelte tilfeller kaskadeeffekter nasjonalt. Samlet vurderes konsekvensene som høye, og potensielt svært høye der avhengigheten av optisk kommunikasjon og sensorkjeder er stor og det er lite eller ingen alternative løsninger.

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – MIDDELS RISIKO

Feltet har betydning for verdiskaping i industri, forsvar, energi og helse. Svak kompetanse kan svekke evnen til å skape, videreutvikle og beskytte avanserte produkter og løsninger, og øke avhengighet til land som kan true norske interesser.

[10] Vedlegg II til Forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester Liste II – flerbruksvarer (2024)

KVAST-undersøkelsen peker på moderat tilgang på kandidater fra EU/EØS og NATO. Fire miljøer oppgir at det er noe vanskelig å rekruttere ph.d.-kandidater eller postdoktorer fra NATO-land for fotonikk-feltet, to rapporterer at rekruttering er lett, og respondenten fra fagmiljøet for våpen for rettet energi beskriver rekruttering som noe vanskelig. Kombinasjonen av middels forskningsaktivitet og moderat tilgang på kandidater fra trygge partnerland kan tilsi middels risiko hos de kartlagte miljøene, men med tydelig sårbarhet dersom kompetanse forvitrer. Tap eller mangel på kritisk kompetanse i fotonikk, laser og rettet energi vil gi merkbare negative effekter for økonomisk sikkerhet og omstillingsevne.

Avanserte halvlederteknologier (med fotonikkteknologier som største underkategori) er et område hvor Norge generelt sett publiserer lite, forskningen siteres lite og det hentes inn relativt lite midler fra EU. Det finnes noen sterke fagmiljøer. SINTEF, NTNU og UiO er de mest aktive norske institusjonene. Kina er verdens største produsent av vitenskapelige artikler innen avanserte halvledere og har også høy gjennomslagskraft (siteringstall). USA regnes som en av de to globale lederne sammen med Kina. For Norge er samarbeidet med USA, Kina og europeiske land er betydelig og utgjør en stor del av norsk internasjonal publisering innen avanserte halvledere. For å styrke norsk kompetanse og konkurransekraft vil det trolig også være viktig å fortsette samarbeidet med Kina. Norge har lavere aktivitet enn Sverige, Danmark og Finland på avanserte halvlederteknologier/fotonikk i EU-prosjekter (2020-2024) og mottok betydelig mindre EU-midler enn de andre nordiske landene. Norsk næringsliv har relativt høy andel av midlene på dette området (37,5 %), høyere enn i Sverige og Danmark, men det totale volumet er lavt.

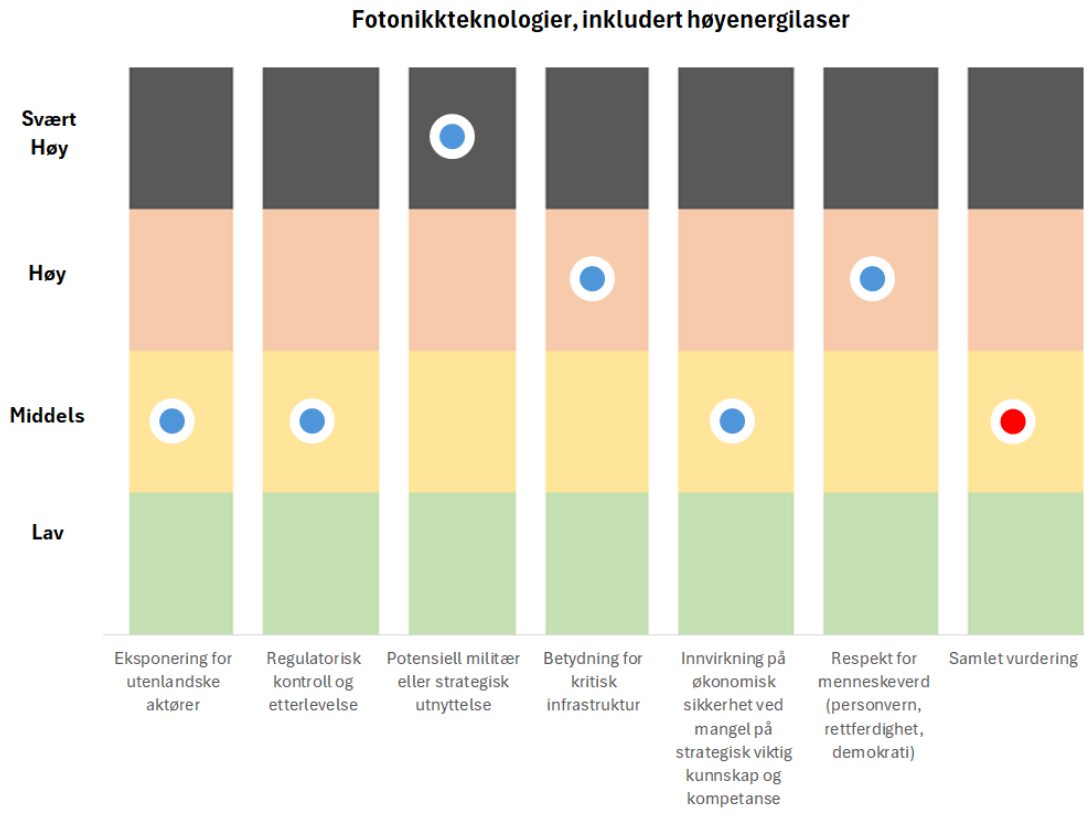
Respekt for menneskeverd – HØY RISIKO

Fotonikk spenner fra industrielle prosess- og målesystemer som normalt ikke behandler personopplysninger til sensorer i offentlige rom og våpen for rettet energi. I den «rene» industribruken er risikoen lav etter indikatorene. Risikoen øker der fotonikk brukes til overvåking, identifikasjon eller atferdskontroll, for eksempel persontelling med LIDAR eller personsøk med elektro-optikk. Her kan datainnsamlingen bli omfattende, formål og hjemmel være uklare, og transparens, klageadgang og menneskelig kontroll være svake. Dette kan gi inngrep i privatliv, skjevheter i beslutninger og nedkjølende effekter på ytring og deltakelse.

Våpen for rettet energi medfører en mer fremtredende menneskerettighetsrisiko. Systemer som kan blinde, skade eller brukes ved folkemengdekontroll, utfordrer grunnleggende rettigheter og humanitetsprinsipper. Uten klar hjemmel, strenge bruksrammer, dokumentert proporsjonalitet og robuste ansvar. Med bakgrunn i dette er risiko vurdert som høy.

Samlet vurdering – MIDDELS RISIKO

Samlet knyttes det middels risiko til feltet fotonikkteknologier, inkludert høyenergilaser. Risiko er middels både når det gjelder regulatorisk kontroll og innvirkning på økonomisk sikkerhet, som taler for en lavere total risikovurdering. Teknologiens flerbrukspotensiale og delteknologier innenfor feltet med direkte militære anvendelsesområder gjør at risikoen som knyttes til feltet øker betraktelig. Gitt Norges posisjon innen halvledere vurderes imidlertid den samlete risikoen som middels.



Figur 1 Grafisk fremstilling av den samlede risikoen for fotonikkteknologier

2. Dataanalytiske teknologier

Dataanalytiske teknologier innenfor kunstig intelligens er KI-drevne metoder og verktøy som henter inn, bearbeider og analyserer store datasett for å finne mønstre, forutsi utvikling, oppdage avvik og gi beslutningsstøtte. Teknologien er bredt muliggjørende og inngår i alt fra etterretning/overvåking/rekognosering (ISR), cybersikkerhet og beslutningsstøtte til logistikk, helse, energi og finans. I forsvarssektoren brukes dataanalyse og maskinlæring allerede operativt for automatisk tolkning av bilde- og signalstrømmer, språkbehandling og endringsdeteksjon, samtidig som potensialet vokser raskt i retning av autonome funksjoner og bedre utnyttelse av åpne kilder[11]. KI-analyse er gjennomgående i digital transformasjon og bærer for innovasjon både sivilt og militært. Teknologien har høy modenhet og inngår allerede i mange kritiske systemer.

Eksponering for utenlandske aktører – LAV RISIKO

KI-datakraft, algoritmer og datasett er av stor interesse for aktører som kan true nasjonal sikkerhet. Teknologien er globalt tilgjengelig, men de mest avanserte verktøyene utvikles av sentrale aktører i USA og Kina, mens norske og felles-europeiske systemer er avhengige av utenlandske skytjenester, programvare og ekspertise. Norske trusselvurderinger beskriver at norsk kunstig intelligens-teknologier kan være interessante mål for aktører underlagt sanksjoner og eksportkontrollregimer [12].

[11] FFI (2025) Forsvarsanalysen 2025
[12] Etterretningstjenesten (2025) FOKUS

Der dataanalyseteknologier har militær sluttbruk kan teknologiene være mål for forsøk fra Russland, Kina og Iran på fordekte anskaffelser og ulovlig kunnskapsoverføring, også via studenter og forskere[13]. Plattformer, opplæringsdata og algoritmer kan overføres via FoU-samarbeid eller leverandørkjeder og er attraktive mål for spionasje og påvirkning. Innenfor kunstig intelligens er dataanalytiske teknologier den underkategorien med lavest publiseringsvolum, med kun 18 av publikasjonene i Web of Science i perioden 2015-2024. Til sammen får de seks nye, nasjonale forskningssentrene for kunstig intelligens inntil 200 millioner hver over fem år. Flere av sentrene for kunstig intelligens som ble opprettet i juni 2025 skal utvikle dataanalytiske teknologier. Disse kan bidra til at Norge blir mer attraktiv å samarbeide med, og det er derfor viktig å følge nøye med på risikoen fremover.

Regulatorisk kontroll og etterlevelse – HØY RISIKO

Det finnes per i dag ikke et helhetlig eller fullmodent regelverk, verken nasjonalt eller internasjonalt, som regulerer KI dataanalyseteknologier fullt ut. Enkelte deler av KI-feltet reguleres delvis gjennom personopplysningsloven/GDPR (lovlig grunnlag, formålsbegrensning, dataminimering, rettigheter) og sikkerhetsloven (beskyttelse av skjermingsverdige verdier). EUs KI-forordning (EU AI Act) er fortsatt ikke fullt ut innfaset i norsk lovgiving og det finnes fremdeles gråsoner spesielt knyttet til dokumentasjon, ansvar og etterprøvbarhet i algoritmer. Bildet forsterkes av at evnen til praktisk håndhevelse og tilsyn fortsatt er begrenset. Etter indikatorene tilsier dette høy risiko: det finnes et rammeverk, men rammeverket som finnes er umodent og inneholder vesentlige gråsoner.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

KI dataanalyseteknologier har svært høyt potensiale for militært og strategisk bruk. KI-drevet dataanalyse er allerede i operativ bruk i Forsvaret for å tolke store datamengder, blant annet satellitt- og dronebilder, signal- og endringsdeteksjon, og språkbehandling og beslutningsstøtte[14]. KI-drevet dataanalyse kan også øke tempo, presisjon og utholdenhet i cyberforsvar, inkludert raskere oppdagelse og respons, og mer autonome beslutninger ved begrenset kommunikasjon. Dette viser høy operativ nærhet, høy overførbarhet til militære systemer og en kritisk rolle i kapabilitetskjedene; flertallet av fagmiljøene spurt i KVAST-undersøkelsen vurderer videre militær bruk for teknologien som veldig sannsynlig. Nasjonale trussel- og risikovurderinger fastslår at statlige aktører bruker KI til å forsterke cyberoperasjoner. NSM fremhever videre at tilgjengeligheten av KI-modeller kan senke terskelen for cyberangrep. Samlet treffer dette indikatorene for svært høy. Teknologien er kjerne i digitaliserte operasjoner, og tap eller misbruk vil gi alvorlig svekkelse av forsvarsevne og beredskap.

Konsekvenser for kritisk infrastruktur – HØY RISIKO

Dataanalyse-teknologier drevet av kunstig intelligens har allerede betydning for flere kritiske samfunnsfunksjoner, blant annet energistyring, transport, kommunikasjon, og helse og beredskap. Teknologien understøtter flere kritiske infrastrukturer samtidig. Feil, bortfall eller manipulering av teknologien kan skape store forstyrrelser, feil i prioriteringer eller beslutninger, eller tap av styring og kontroll. Feil eller misbruk kan få kaskadeeffekter mellom sektorer dersom samme modeller gjenbrukes på tvers og når alternative manuelle prosesser er svake. Der det er få eller dårlige alternative løsninger og manuelle reserveprosedyrer, kan konsekvensene bli langvarige og

[13] Politiets sikkerhetstjeneste (2024) Nasjonal Trusselvurdering
[14] FFI (2025) Forsvarsanalysen 2025

omfattende. Imidlertid er ikke KI-drevet dataanalyse gjennomgående integrert i kritisk infrastruktur[15.] Samlet sett vurderes konsekvenser for kritisk infrastruktur til høy.

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse - MIDDELS RISIKO

Teknologifeltet er i stadig vekst og får voksende betydning for verdiskaping innenfor en rekke ulike sektorer. Uten tilstrekkelig kunnskap og kompetanse svekkes den nasjonale evnen til å beskytte verdifulle dataressurser, effektivisere arbeidsprosesser og drive innovasjon i både offentlig og privat sektor. Dette kan føre til mindre produktivitet og mindre verdiskaping, tapte muligheter for utvikling av nye tjenester og forretningsmodeller, og redusert konkurransekraft i en digital økonomi. Utviklingen går i retning av at stadig flere samfunnsfunksjoner blir avhengige av KI dataanalyse-teknologier, og manglende kapasitet på feltet nasjonalt vil kunne føre til økt avhengighet av til ikke-allierte. KVAST-undersøkelsen peker på moderat tilgang på kandidater fra EU/EØS og NATO. Samlet tilsier dette middels risiko, da forskningsaktivitet på feltet er høy, men tilgang på kandidater fra trygge partnerland moderat, og det knyttes tydelig sårbarheter for økonomisk sikkerhet dersom kompetanse forvitrer.

Respekt for menneskeverd – SVÆRT HØY RISIKO

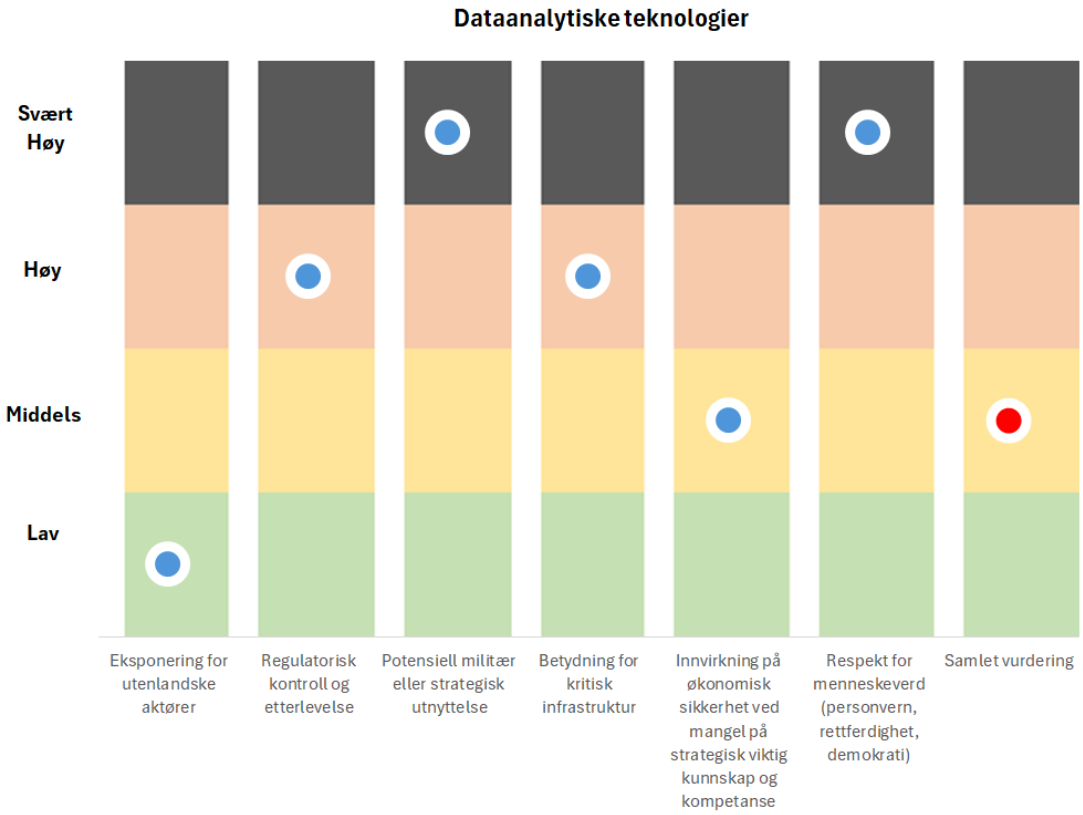
Misbruk av teknologien kan få store konsekvenser for menneskeverd og menneskerettigheter. Datadrevet analyse kan behandle store mengder personopplysninger, som blant annet personsensitive og biometriske data, til bruk i overvåking, sporing, profilering eller beslutningsstøtte i forvaltning/arbeidsliv/rettshåndhevelse. Datadrevet analyse muliggjør prediktiv profilering, mønstergjenkjenning og beslutninger som vil ha direkte konsekvenser for individers livssituasjon. Risikoen for urimelig overvåking, feilaktige avgjørelser og utilbørlig inngripen er taler for høy risiko, særlig der hjemmelsgrunnlaget for inngripen er svakt eller fraværende. Risikoen øker imidlertid til svært høy når man ser på potensialet for undergraving av menneskeverd- og rettigheter ved misbruk av teknologien av vondsinnede aktører. Dersom teknologien misbrukes, kan den brukes både til å skade systemer og til å skade mennesker. Risikoen er særlig høy fordi teknologien ligger tett på operativ drift, beslutningsstøtte og beredskapsprosesser. Misbruk kan gi rask eskalering og vanskelig oppdagelse.

Samlet vurdering – MIDDELS RISIKO

Samlet risikonivå vurderes som middels. Risikoen er høyest der teknologien er tett integrert i operative beslutninger, kritisk infrastruktur eller sentrale forsvars- eller sikkerhetsfunksjoner. Dette følger av at teknologien er svært bredt muliggjørende og allerede i operativ bruk i forsvars- og beredskapskontekster, samtidig som EOS-tjenestene peker på målrettede innhentingsforsøk fra trusselaktører som utnytter KI til angrep. Faktisk militær og strategisk verdi er svært stor. Regelverket er i gang med å styrkes, men etterlevelsen er fortsatt krevende i praksis. I kritisk infrastruktur er teknologien viktig i flere kjeder med kaskadepotensial ved svikt eller misbruk, og vedvarende kompetansegap vil kunne svekke omstillingsevne og konkurransekraft. I person- og beslutningsnære bruksområder er rettighetsrisikoen reell. Operativ nærhet og flerbrukspotensialet til teknologien trekker opp risikoen, i tillegg til potensialet for store brudd på rettigheter dersom teknologien

[15] Meld. St. 14 (2024–2025) viser at KI i offentlig sektor fortsatt er lite i bruk, at grunnforutsetninger mangler, og at kontrollmekanismer for ansvarlig bruk må på plass.

misbrukes. Ettersom Norge har liten aktivitet på dataanalyseteknologier, vurderes risikoen per i dag som middels. Det vil være viktig å bygge opp kompetanse på området for å sikre norsk kompetanse og fremtidig konkuranseevne.



Figur 2 Grafisk fremstilling av den samlede risikoen for Dataanalytiske teknologier

3. Maskinlæring og dyplæring

Maskinlæring og dyplæring er bredt muliggjørende og grunnleggende for moderne digitale tjenester. Maskinlæring bruker algoritmer for å lære mønstre fra data og deretter gjøre prediksjoner eller beslutninger. Når modellene trenes på mer data, forbedres ytelsen, og resultatet av treningen blir en maskinlæringsmodell klar for bruk. Dyplæring er en undergren av maskinlæring som bruker nevrale nettverk med mange lag for å lære komplekse representasjoner i data. Dette er særlig effektivt for bilde-, lyd-, tekst- og sensorstrømmer. Teknologien er kjernekomponent i systemer for bilde- og taleforståelse, prediktiv analyse, cybersikkerhet, autonome kjøretøy, medisinsk diagnostikk, prosessindustri og beslutningsstøtte. Teknologiene brukes i flere grunnleggende nasjonale funksjoner og utvikler seg raskt mot økende autonomi og kritiske funksjoner.

Eksponering for utenlandske aktører — HØY RISIKO
Maskinlæring og dyplæring bygges og driftes på globale plattformer, rammeverk og skytjenester, ofte levert av aktører i USA eller Kina. Det kan gi eksponering gjennom leverandørkjeder, åpne modellarkiver og immateriell overføring av kode, data og modeller. De norske EOS-tjenestene peker på dokumenterte trusler knyttet til KI-teknologi. Ifølge NIFUs analyse er Kina den største

samarbeidspartneren for norske miljøer innenfor maskinlæring og dyplæring, etterfulgt av USA, Storbritannia, Tyskland og India, målt i antall sampublikasjoner[16].

Regulatorisk kontroll og etterlevelse — MIDDELS RISIKO
Det finnes ennå ikke et helhetlig, modent regelverk som dekker hele livsløpet for maskinlæring og dyplæring. GDPR og sikkerhetsloven dekker deler av feltet, mens EUs KI-forordning er i innfasing med trinnvise plikter for forbudte praksiser, grunnleggende modeller (GPAI) og høyrisikosystemer i perioden 2025–2027. Inntil implementering og tilsyn er modnet, gjenstår flere gråsoner. Dette samsvarer med middels risiko.

Potensiell militær eller strategisk utnyttelse — SVÆRT HØY RISIKO
Maskinlæring og dyplæring gir direkte kapasitetsløft i etterretning, overvåking og rekognosering, cyberforsvar og -angrep, målutvelgelse, autonomi og logistikk. FFI beskriver at slike kapasiteter allerede brukes operativt til automatisk tolkning av satellitt- og dronebilder, signal- og endringsdeteksjon og språkbehandling/ beslutningsstøtte. Dette viser høy sannsynlighet for bruk, høy overførbarhet i programvare, metoder og data, og at maskinlæring og dyplæring er kritisk i kjeden av kapabiliteter. Tap eller misbruk vil derfor kunne gi alvorlig svekkelse av forsvarsevne og beredskap, som treffer indikatorene for svært høy risiko [17].

Konsekvenser for kritisk infrastruktur — HØY RISIKO
Maskinlæring og dyplæring brukes i drift, styring og overvåking på tvers av ekom, energi, transport, helse og finans, blant annet til anomalideteksjon, last- og trafikkprognoser og prediktivt vedlikehold. Feil eller angrep som modellforgiftning, datamanipulasjon eller svikt i validering kan gi gale beslutninger og kaskadeeffekter mellom funksjoner. Alternative løsninger og manuelle prosedyrer demper risikoen noe, men der maskinlæring og dyplæring styrer kjernefunksjoner og det er få eller ingen reservesystemer, kan konsekvensene bli svært høye lokalt. Nasjonalt vurderes konsekvensene som høye.

Innvirkning på økonomisk sikkerhet ved mangel på kompetanse — MIDDELS

Kompetansegap i maskinlæring og dyplæring vil svekke konkurransekraft og omstillingsevne, redusere innovasjon i energi, industri, helse, transport og finans, og øke avhengigheten av utenlandske aktører for utvikling, drift og vedlikehold av kritiske systemer. Norske fagmiljøer er små og rapporterer rekrutteringsfriksjon fra trygge partnerland, mens nye satsinger kan dempe risiko dersom de faktisk styrker kapasiteten. Dette treffer indikatorene for robust nasjonal kompetansebase og tilgang via trygge partnerland, og begrunner middels til høy risiko (FFI, 2025; NIFU, 2025). Norge står for en liten andel av verdens totale publisering innen KI, sammenlignet med stormakter som Kina og USA. Det har vært en kraftig vekst i norsk KI-forskning de siste ti årene, både i antall publikasjoner og i deltakelse i EU-finansierte prosjekter. Norske KI-publikasjoner har svært høye siteringstall. Norge har mottatt en betydelig andel EU-midler til KI-prosjekter og har høy

[16] NIFU Rapport 2025:17
[17] FFI (2025) Forsvarsanalysen 2025

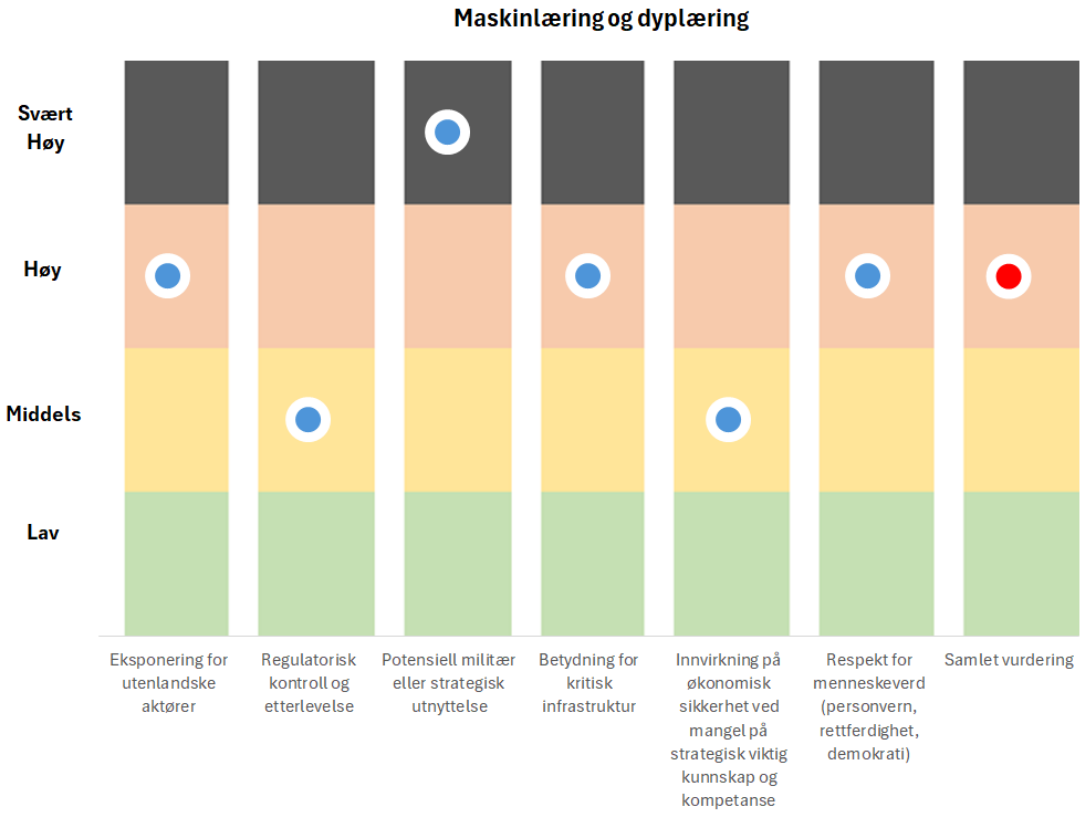
koordineringsgrad i slike prosjekter sammenlignet med andre europeiske land. De mest aktive norske institusjonene i prosjekter er NTNU, UiO og SINTEF[18].

NIFUs rapport konkluderer med at KI er det området der Norge står sterkest blant de sensitive teknologiene, både i volum, kvalitet og internasjonalt samarbeid. På kunstig intelligens har Norges internasjonale samarbeid blitt stadig mer konsentrert rundt Kina, og dette kan tolkes som en mulig sårbarhet[19].

Respekt for menneskeverd — HØY RISIKO
Maskinlæring og dyplæring kan brukes til individuell prediksjon, identifikasjon og beslutningsstøtte i sammenhenger som påvirker liv, helse, arbeid, kreditt og rettigheter. Uten klar hjemmel, transparens, innsyn/klage og menneske-i-sløyfen øker risiko for inngrep i privatliv, diskriminering og nedkjølende effekter på ytring og deltakelse. EUs KI-forordning adresserer dette gjennom forbud mot enkelte praksiser, krav til dokumentasjon og styring i høyrisiko-systemer, men faktisk risiko avhenger av etterlevelse og datakvalitet mens rene ikke-personlige bruksområder med robust anonymisering og rettferdighetstesting kan være lavere.

Samlet vurdering — HØY RISIKO
Maskinlæring og dyplæring fremstår samlet som et teknologiområde med høy risiko. Metodene er i ferd med å bli grunnleggende infrastruktur i etterretning, cybersikkerhet, autonome systemer, medisinsk diagnostikk og beslutningsstøtte i forvaltning og næringsliv, slik at svakheter eller kompromittering direkte kan påvirke nasjonal sikkerhet og kritiske samfunnsfunksjoner. Avhengighet av globale plattformer og tette forsknings- og industribånd til stormakter forsterker eksponeringen for innhenting, manipulasjon og teknologisk «lock-in». Samtidig er norske fagmiljøer små, og regelverk og tilsyn er fortsatt under oppbygging. Dette gir et risikobilde der gevinstene er store, men hvor styring, transparens og nasjonal kompetanse blir avgjørende for å holde risikoen på et akseptabelt nivå.

[18] Prosjektdeltakelser med midler fra Norges forskningsråd, Horisont Europa og European Defence Fund (2020-2024).
[19] NIFU Rapport 2025:17



Figur 3 Grafisk fremstilling av den samlede risikoen for Maskinlæring og dyplæring

4. Kvantesensorer og -radar

Kvanteteknologier omfatter kvanteberegning, kvantekryptografi, kvantekommunikasjon og kvantesensorer og -radar. Kvantesensorer kan gi svært presise målinger og mulighet for navigasjon uten GNSS, samt bedre identifisering av underjordiske og undersjøiske mål. Kvanteberegning truer dagens offentlige-nøkkel-kryptografi på sikt, mens kvantekommunikasjon kan gi nye måter å beskytte samband. Feltet er i rask utvikling, med tydelig flerbruk og uferdig standardisering.

Eksponering for utenlandske aktører – LAV RISIKO

Det pågår et globalt kappløp om kvanteteknologier der store makter som Kina, EU og USA investerer milliarder i utvikling. Norge er avhengig av internasjonal leverandørkjede for laboratorieutstyr, spesialiserte komponenter og datamaskiner, og må samarbeide med utenlandske forskningsmiljøer for å holde tritt. Åpne forskningsmiljøer, datadelingsinitiativer og foreløpig få etablerte standarder gjør at aktører med andre interesser kan skaffe seg kunnskap. Det advares i SIPRI-rapporten om at åpne kvanteverktøy og fallende kostnader kan gjøre teknologien tilgjengelig for ikke-statlige aktører. Derfor vurderes eksponeringen som høy. I Web of Science finner NIFU svært få publikasjoner innen *kvanteteknologi*. Det har vært en vekst fra 5 publikasjoner i 2015 til 30 publikasjoner i 2024. Det generelle bildet for teknologiområdet er at norske institusjoner har siteringstall under verdensgjennomsnittet. Det er lite sannsynlig at Norge er et veldig attraktivt samarbeidsland for å få tilgang til kompetanse på kvanteteknologi. Dette kan imidlertid endre seg, og det må følges med på utviklingen fremover. Våren 2025 lyste Forskningsrådet ut midler til Senter for kvanteteknologisk

forskning. Midlene i utlysningen skal gå til forskningssentre med tyngdepunkt i grunnleggende forskningsaktiviteter innenfor matematisk, naturvitenskapelig og/eller teknologisk forskning. Forskningssentrene skal utføre forskning av høy kvalitet innenfor kvanteberegning, kvantekommunikasjon og kvantesensorer. I løpet av 2025 skal nasjonal forskningsinfrastruktur oppgraderes for å tilpasses kvanteforskning

Regulatorisk kontroll og etterlevelse – MIDDELS RISIKO

Internasjonal styring for kvanteteknologier er fragmentert og i stor grad i utvikling. Eksportkontroller og forskningsregimer forsøker å adressere dual-use-risikoen, men det finnes foreløpig få spesifikke regler for kvantesensorer og -radarer. Nasjonale strategier varierer, og standardiseringsarbeid i organisasjoner som ISO og ITU er preget av geopolitiske interessekonflikter. Regulatorisk kontroll vurderes som middels fordi det finnes enkelte mekanismer, men regelverk og håndheving ikke dekker hele feltet.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Kvantesensorer kan gi presis navigasjon i GPS-frie miljøer, forbedre radar og identifisering, og potensielt avsløre lavsignatur-teknologier. Kvantedatamaskiner kan på sikt knekke kryptering og gi en strategisk etterretningsfordel, mens kvantekommunikasjon kan sikre ekstremt robuste samband. Disse egenskapene gir store offensive og defensive militære gevinster og derfor vurderes risikoen som svært høy.

Betydning for kritisk infrastruktur – HØY RISIKO

Kvantesikker kommunikasjon og presis posisjonering kan bli integrert i kraftnett, finanssystemer og transport. Et angrep på kvantebaserte nøkkeldistribusjonssystemer eller kvantesensorer kan svekke tillit til kritisk infrastruktur. Samtidig kan kvantedatamaskiner på sikt knekke offentlig-nøkkelbaserte systemer og true samfunnets digitale grunnmur. Risikoen vurderes derfor som høy.

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – HØY RISIKO

Hvis Norge ikke opparbeider og beholder eksperter innen kvantemekanikk, algoritmeutvikling og sensorfysikk, vil vi bli avhengige av utenlandske leverandører og gå glipp av nye verdikjeder. Store investeringer i kvanterelaterte gründermiljøer gir allerede konkurransefortrinn i andre land. Manglende kompetanse kan begrense norsk næringsutvikling og verdiskaping. Evalueringen av naturvitenskap (2022-2024) pekte på at den norske posisjonen innen kvantevitenskap og -teknologi er svak. Dette fremheves som bekymringsfullt, gitt behovet for kunnskap på dette området. Innenfor kvanteteknologier er kvanteberegning det underområdet med størst publiseringsvolum, mens kvantesensorer og -radar er det minste. Når det gjelder EU-midler tildeles Norge kun ca. en tredjedel av det europeiske gjennomsnittet innen *kvanteteknologier*. Norge har i perioden 2020-2024 deltatt i bare fire prosjekter, noe som er langt færre enn andre nordiske land. Det er heller ikke noe samarbeid med de nordiske landene[20]. Gitt det lave volumet på publiseringen og prosjektdeltakelser er dette et område Norge bør har mer kompetanse på, og det satses nå på dette teknologiområdet.

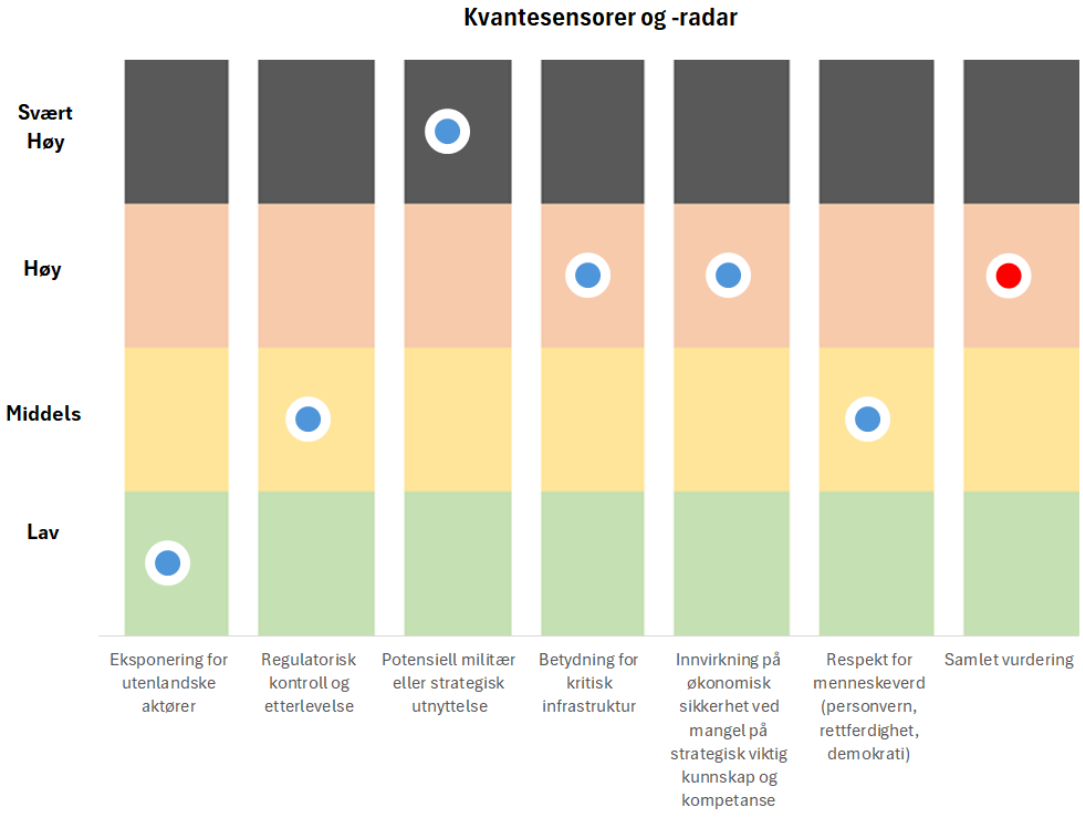
[20] NIFU Rapport 2025:17

Respekt for menneskeverd – MIDDELS RISIKO

Kvantesensorer og kvantebasert radar kan overvåke bevegelser og identifisere objekter uten tradisjonell signatur. Dette åpner for mer omfattende overvåking og målsporing, men teknologiene er foreløpig lite utbredt i sivile applikasjoner. Risikoen for personverninngrep vurderes som middels, men kan øke dersom sensorer kombineres med andre datakilder.

Samlet vurdering – HØY RISIKO

Kvantesensorer og kvantebasert radar vurderes samlet som et teknologiområde med høy risiko, til tross for at feltet fortsatt er i tidlig fase. Teknologien har potensial til å gi gjennombrudd i presis navigasjon, deteksjon og situasjonsforståelse, særlig i GPS-frie eller sterkt konkurranseutsatte domener, og vil kunne gi betydelige militære og strategiske fordeler til aktører som ligger i front. Samtidig er den internasjonale styringen fragmentert, og norsk posisjon svak med få prosjekter og begrenset kompetanse, noe som øker sårbarheten for avhengighet av utenlandske leverandører og kunnskapsmiljøer. Summen av høyt potensial, uferdig regulering, begrenset nasjonal kapasitet og mulig fremtidig bruk i overvåking og målsporing tilsier at området bør anses som spesielt viktig for nasjonale interesser og følges nøye.



Figur 4 Grafisk fremstilling av den samlede risikoen for Kvantesensorer og - radar

5. Syntetisk biologi

Syntetisk biologi er bredt muliggjørende og har kritisk potensial i medisin (forbedret terapi, vaksiner, diagnostikk), industri (bioproduksjon, grønne prosesser), landbruk, miljø og forsvar. Teknologien muliggjør utvikling av nye organismer og biologiske systemer, og gir tilgang til funksjoner som tidligere ikke var mulig (f.eks. «gendrivere», tilpassede mikrober og virus).

Eksponering for utenlandske aktører – MIDDELS RISIKO

Syntetisk biologi har stor interesse for både allierte og ikke-allierte aktører (USA, Kina, Russland m.fl.). Norsk og europeisk FoU, laboratorier og biotekindustri er attraktive mål for spionasje, kunnskaps- og prøveleveranser, spesielt innen avanserte genredigeringsmetoder og biofabrikkering. Leverandøravhengighet på DNA-biosyntese samt deling av digitale genbanker øker sårbarheten for innhenting og misbruk. For bioteknologier som helhet er publiseringsvolumet lavt, og har økt lite i perioden 2015-2024, fra 18 til 58 publikasjoner ifølge NIFUs analyse. Selv om Norge har et moderat antall vitenskapelige publikasjoner innen bioteknologi sammenlignet med de største landene internasjonalt, har norske publikasjoner relativt gode siteringstall. Dette indikerer at kvaliteten på norsk forskning er god. Tyskland er det landet Norge sampubliserer mest med innenfor bioteknologier. Kina med på listen over de ti viktigste samarbeidslandene for Norge innen bioteknologi i perioden, men ikke blant de aller største partnerne. Tyskland, USA, Nederland, Storbritannia og Frankrike er større samarbeidspartnere.

Regulatorisk kontroll og etterlevelse – HØY RISIKO

Bioteknologiloven og internasjonale avtaler gir formelle rammer, men syntetisk biologi utfordrer eksisterende regulering – særlig knyttet til «dual-use» (fredelig/farlig anvendelse), ikke-tradisjonell organismeskaping, digital bioinformatikk og immateriell, programmatisk kunnskapsoverføring. Kontroll på egen håndtering, biologiske datasett og biologisk materiale er ressurskrevende og kan være mangelfull, særlig internasjonalt.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Syntetisk biologi åpner for utvikling av nye former for biologisk våpen, styrkebeskyttelse, diagnostikk, ressurskontroll og helhetlig bioforsvar. Teknologien gir direkte strategisk mulighet for skjult påvirkning og produksjon av stoffer/organismer som kan være vanskelige å oppdage, attribuere eller kontrollere. Muliggjør både defensiv og offensiv kapasitetsutvikling. Norsk militære og beredskapsmiljøer følger feltet tett.

Betydning for kritisk infrastruktur – SVÆRT HØY RISIKO

Syntetisk biologi kan påvirke helseberedskap, matproduksjon, diagnostikk, forsyningskjeder, og miljø. Manipulasjon, svikt eller misbruk kan føre til utbrudd av sykdom, tapt matvareproduksjon, tap av kritiske ressurser og svekket beredskap. Systemrisiko for smitte, miljøskade og feil i industrielle bioprosesser kan ha nasjonalt alvorlige følger.

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – HØY

Manglende nasjonal kompetanse og kunnskapsutvikling innen syntetisk biologi vil kunne redusere muligheten til å utvikle innovative løsninger for norsk helse-, mat-, miljø- og bioteknologisektor.

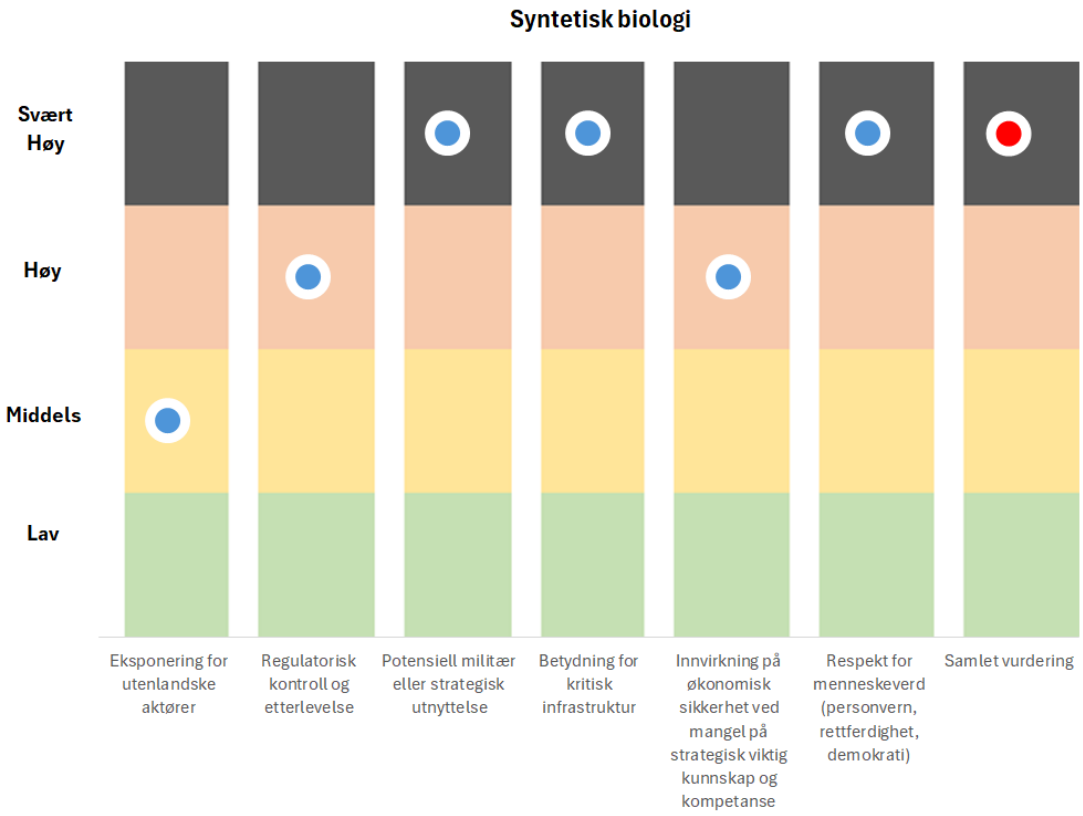
Dette kan svekke evnen til å nyttiggjøre seg det hurtig voksende markedspotensialet innen alt fra bærekraftig produksjon til medisinske gjennombrudd, biologisk sikkerhet, og industriell omstilling. Begrenset tilgang på eksperter og FoU-miljøer kan føre til at Norge blir avhengig av utenlandske leverandører og ferdigprodukter når det gjelder kritiske bioteknologiske komponenter og tjenester, og miste kontroll over egne biogenetiske ressurser. På sikt kan dette føre til at norske virksomheter får dårligere vilkår i globale verdikjeder, går glipp av nye forretningsmuligheter og investeringer, og mister kapasitet til krisehåndtering eller rask innovasjon ved behov. Dermed kan manglende kompetanse på dette området bidra til tapte arbeidsplasser, lavere omstillingsevne, og en svekket økonomisk sikkerhet. Norge gjør det bra i EU innen bioteknologi, spesielt målt i tildelte midler per innbygger og koordineringsgrad. Volumet av prosjekter er lavere enn i de andre nordiske landene, men kvaliteten og gjennomslagskraften er god. Innenfor bioteknologi er imidlertid syntetisk biologi den underkategorien med lavest publiseringsvolum, og det kan være verdt å følge med på dette teknologiområdet.

Respekt for menneskeverd – SVÆRT HØY RISIKO

Syntetisk biologi åpner for direkte og indirekte påvirkning av livsgrunnlag, arvemateriale, helse og velferd. Feil eller utilsiktet spredning eller bruk i befolkning kan ha stor inngripen på menneskers rettigheter og tillit til myndigheter.

Samlet vurdering – SVÆRT HØY RISIKO

Syntetisk biologi vurderes samlet som et område med svært høy risiko. Teknologien muliggjør direkte inngrep i arvemateriale, utvikling av nye organismer og omfattende manipulasjon av biologiske systemer, med potensielt store konsekvenser for helse, miljø, matforsyning og biosikkerhet ved feil, uhell eller misbruk. Svikt i forskningspraksis, sikkerhet eller styring kan gi hendelser med langvarige og vanskelig kontrollerbare effekter nasjonalt og globalt. Samtidig er kompetanse og aktivitet konsentrert i relativt få miljøer, og internasjonale normer og regelverk er fortsatt under utvikling. Dette gir et risikobilde der selv et begrenset antall aktører kan skape svært store skadevirkninger, og hvor krav til ansvarlig forskning, sikkerhetskultur, hemmelighold og internasjonal koordinering er særlig strenge.



Figur 5 Grafisk fremstilling av den samlede risikoen for Syntetisk biologi

6. Cybersikkerhetsteknologier, inkludert cyberovervåkning og sikkerhets- og inntrengningssystemer, og digital etterforskning

Cybersikkerhetsteknologier, inkludert cyberovervåkning og sikkerhets- og inntrengningssystemer, og digital etterforskning er muliggjørende og kritiske for all digital infrastruktur. Teknologiene er sentrale i beskyttelse av konfidensialitet, integritet og tilgjengelighet for offentlige, industrielle, militære og samfunnskritiske systemer. Teknologiene inkluderer blant annet postkvantekryptografi er kryptografiske algoritmer som er under innføring for å motvirke fremtidige trusler fra kvantedatamaskiner. Teknologien er kjerne i digital suverenitet.

Eksponering for utenlandske aktører – HØY RISIKO

Cybersikkerhetsteknologier er i stort avhengige av globale verdikjeder (programvare, sky, modellarkiver, kryptomoduler), og avhengigheten til ikke-allierte leverandører er reell. Innenfor postkvantekryptografi skjer anskaffelser av kryptokomponenter og biblioteker gjennom internasjonale kjeder. NSM viser i Risiko 2025 til funn av mange usikre KI-modeller og at KI-utviklere selv angripes. Dette øker eksponeringen der virksomheter gjenbruker tredjeparts modeller eller pakker uten full kontroll. EOS-tjenestenes årlige trussel- og risikovurderinger beskriver at statlige aktører, særlig Russland og Kina, forsterker cyberoperasjoner med KI og samtidig forsøker å anskaffe teknologi, data og kompetanse via mellommenn og fordekte løp. Det peker på dokumenterte trusler,

og leverandørkjedesårbarhet. Risiko vurderes som høy. Innenfor avansert samband, navigasjon og digitale teknologier, er volumet på publikasjoner mer enn tidoblet i perioden 2015-2024, fra 8 til 92 publikasjoner. Innenfor avansert samband, navigasjon og digitale teknologier er India, Saudi-Arabia og Kina er de mest aktive partnerne når det gjelder sampublisering. Artiklene fra de mest aktive norske institusjonene er høyt sitert internasjonalt ifølge NIFUs analyse. Dette kan indikere at Norge er en attraktiv samarbeidspartner. Cybersikkerhetsteknologier, inkludert cyberovervåkning og sikkerhets- og inntrengningssystemer, og digital etterforskning er den nest største underkategorien under avansert samband, navigasjon og digitale teknologier i NIFUs analyse.

Regulatorisk kontroll og etterlevelse – MIDDELS RISIKO

Regelverk for cybersikkerhet er under løpende utvikling, men implementering varierer og regelverk som dekker ny teknologi som KI og postkvantekryptografi er ikke fullt modne i praksis. EU AI Act trer inn trinnvis, og tidlige bestemmelser har begynt å gjelde, men veiledning og tilsyn bygges fortsatt opp. Dette gir gråsoner i dokumentasjon, ansvar og etterprøvbarhet.
For postkvantekryptografi er noen standarder etablert. Migrasjonen er flerårig og teknisk krevende, og myndigheter anbefaler planlagte overganger og styrket styring for å unngå «kryptoteknisk gjeld». Dette peker på håndterbare, men reelle etterlevelsesutfordringer i overgangsfasen. Risiko vurderes som middels.

Potensiell militær eller strategisk utnyttelse — HØY RISIKO

Cybersikkerhet er sentralt for etterretning, militære beslutningsprosesser, kommunikasjon, navigasjon og ledelse av kritiske systemer (kontroll, styring). Svekkede eller kompromitterte cybersikkerhetssystemer muliggjør digitale angrep, informasjonsoperasjoner, sabotasje og hybridkrigføring. Samlet vurdering er høy.

Konsekvenser for kritisk infrastruktur — HØY RISIKO

Feil, svakheter eller kompromittering av cybersikkerhet gir umiddelbare og alvorlige effekter på samfunnets kritiske funksjoner: Strømforsyning, vann, telekom, transport, helse, navigasjon og sikkerhet. Mangel på postkvantemigrasjon kan føre til brudd på langsiktige konfidensialitetsgarantier, mens KI-sårbarheter i automatiserte sikkerhetssystemer kan føre til uoppdagede eller forsterkede angrep. Samlet er systemiske kaskadeeffekter sannsynlige ved hendelser.

Innvirkning på økonomisk sikkerhet ved mangel på kompetanse — MIDDELS RISIKO

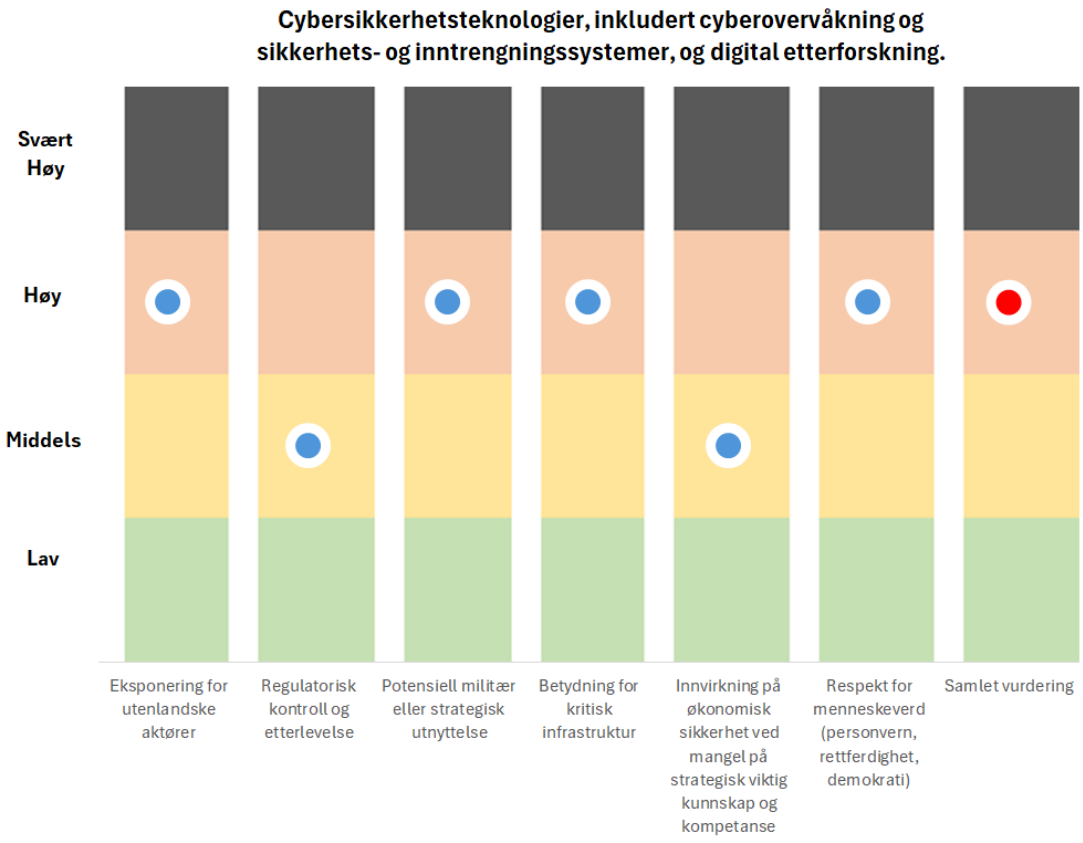
Uten tilstrekkelig nasjonal kunnskap og kompetanse på cybersikkerhet, særlig med hensyn til postkvantekryptografi og bruk av kunstig intelligens i sikringsarbeidet, vil Norge bli mer sårbar for digitale angrep, datainnbrudd og sabotasje mot kritisk infrastruktur og næringsliv. Mangel på ekspertise kan føre til økt avhengighet av utenlandske leverandører og løsninger, redusere evnen til å oppdage og håndtere nye trusselbilder, og gi lavere motstandsdyktighet i møte med stadig mer komplekse cybertrusler. Dette kan også svekke tilliten til norske digitale tjenester, hemme innovasjon og gjøre norske virksomheter mindre konkurransedyktige i eksport- og teknologimarkeder. Langsiktig kan det føre til tap av investeringer, økte kostnader til gjenoppretting etter hendelser, og redusert evne til både økonomisk vekst og nasjonal sikkerhet i en stadig mer digitalisert økonomi. Når det gjelder EU-midler ligger Norge noe under det europeiske gjennomsnittet for tildelte midler og grad av koordinering innenfor avansert samband, navigasjon og digitale teknologier.

Respekt for menneskeverd — HØY RISIKO

Cybersikkerhet beskytter personopplysninger, informasjonsflyt, ytringsfrihet og demokratiske institusjoner. Svikt eller misbruk i teknologi (særlig KI i sikkerhetsløsninger, overvåking og prediktiv analyse) kan føre til urimelig overvåking, diskriminering, tap av rettssikkerhet og undergraving av demokratisk deltagelse. Overgang til nye teknologier kan redusere privatlivsbeskyttelse og true tilliten til digitale tjenester hvis ikke godt ivaretatt.

Samlet vurdering – HØY RISIKO

Samlet vurderes cybersikkerhetsteknologier som et område med høy risiko. Teknologiene utgjør selve beskyttelseslaget rundt digital infrastruktur og er kritiske for konfidensialitet, integritet og tilgjengelighet i både sivile og militære systemer. Svikt, sårbarheter eller kompromitterte løsninger kan gi umiddelbare kaskadeeffekter på strømforsyning, ekom, finans, transport og beredskap, og åpne for spionasje, sabotasje og hybridoperasjoner. Avhengighet av globale leverandørkjeder, inkludert komponenter fra ikke-allierte, forsterker eksponeringen. Samtidig er regelverket i utvikling, og migrasjon til postkvantekryptografi og KI-baserte sikringsløsninger skaper nye overgangsrisikoer. Det samlede risikobildet tilsier et område som krever kontinuerlig oppmerksomhet, kompetansebygging og nasjonal kontroll.



Figur 6 Grafisk fremstilling av den samlede risikoen for Cybersikkerhetsteknologier, inkludert cyberovervåkning og sikkerhets- og inntrengningssystemer, og digital etterforskning

7. Styring, navigasjon og kontrollteknologier, inkludert avionikk og maritim posisjonering

Bredt muliggjørende og kjerne for sikker og effektiv drift av luftfart, sjøfart, logistikk, forsvar, industriell automasjon og nødetater. Avionikk og maritim posisjonering utgjør sentrale funksjoner for styring og navigasjon i moderne systemer – særlig der automasjon, autonomi og digital samhandling er tatt i bruk.

Eksponering for utenlandske aktører – MIDDELS RISIKO

Systemene benytter ofte globale komponenter, internasjonale leverandører (særlig GNSS, INS, avionikkmoduler), og kan være sårbare for påvirkning, spionasje eller manipulasjon, særlig fra ikke-allierte aktører. Satellittbasert navigasjon er spesielt utsatt for spoofing/jamming hvis ikke godt sikret. FoU og systemeksport er attraktive mål internasjonalt. Styrings, navigasjons- og kontrollteknologier, inkludert avionikk og maritim posisjonering har lav aktivitet ifølge NIFUs analyse. Innenfor avansert samband, navigasjon og digitale teknologier generelt er India, Saudi-Arabia og Kina er de mest aktive partnerne når det gjelder sampublisering. Norge har et betydelig forskningssamarbeid med Kina innen avansert samband, spesielt på områder som tingenes internett og digital teknologi.

Regulatorisk kontroll og etterlevelse – MIDDELS RISIKO

Omfattende sektorregelverk (f.eks. luftfartsmyndigheter, International Maritime Organization (IMO), IKT-lovgivning, sikkerhetsloven), men nye autonome/plattformintegrerte styringsløsninger utfordrer eksisterende regelverk, spesielt der digitalisering, datadeling og internasjonal interoperabilitet er nødvendig.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Teknologien har kritisk strategisk betydning for nasjonalt forsvar, kontroll over transport og logistikk, beskyttelse samt anvendelse i offensive/defensive kapasiteter (kampfly, droner, fartøy, missilstyring).

Betydning for kritisk infrastruktur – SVÆRT HØY RISIKO

Svikt i styrings-, navigasjons- og kontrollsystemer kan gi omfattende og umiddelbare konsekvenser: havari, transportstans, tap av styring/posisjonering, tap av effektiv beredskap/samfunnstjeneste. Feil kan føre til store kaskadeeffekter særlig på tvers av luftfart, sjøfart og nødinfrastruktur.

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – MIDDELS RISIKO

Dersom Norge ikke opprettholder tilstrekkelig kompetanse og kunnskapsutvikling innen styring, navigasjon og kontrollteknologier, vil det kunne ramme konkurranseevnen innenfor sentrale næringer som maritim sektor, luftfart, energi og transport. Dette kan føre til økt avhengighet av utenlandske systemer og leverandører, noe som gjør norske verdikjeder mindre robuste mot endringer, markedssvingninger eller hendelser som påvirker tilgang på teknologi eller tjenester. Manglende kunnskap på området begrenser evnen til å drive teknologiutvikling, digitalisering og sikkerhetsforbedring i egen infrastruktur. De mest aktive norske institusjonene innen avansert samband, navigasjon og digitale teknologier er NTNU, SINTEF og UiO. Artiklene fra de mest aktive norske institusjonene er høyt sitert internasjonalt ifølge NIFUs analyse, noe som indikerer at

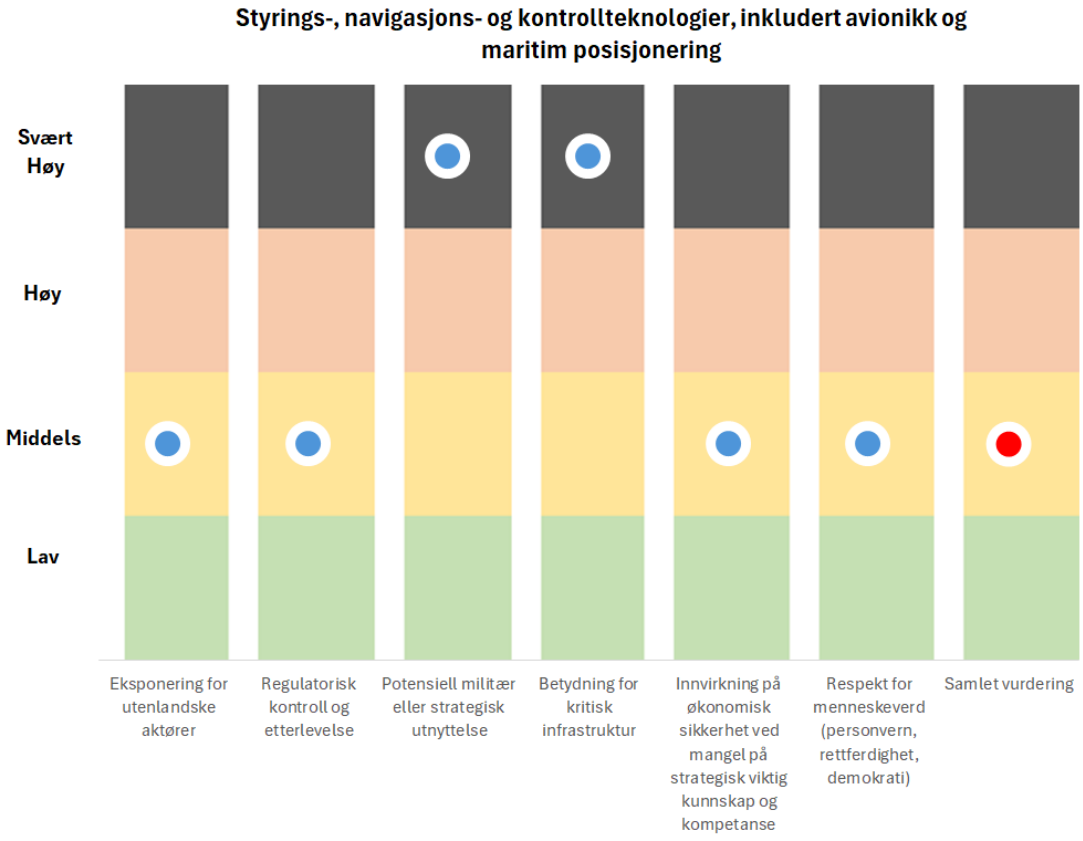
kvaliteten er god. Når det gjelder EU-midler ligger vi noe under det europeiske gjennomsnittet for tildelte midler og grad av koordinering innenfor avansert samband, navigasjon og digitale teknologier. Norges styrke ligger i høy kvalitet på forskningen, men det er potensial for å øke volumet og næringslivets deltakelse i prosjekter sammenlignet med de andre nordiske landene.

Respekt for menneskeverd – MIDDELS RISIKO

Systemer kan lages for å samle inn bevegelses- og lokasjonsdata. Feil, manipulasjon eller urimelig overvåking/analyse kan ramme personvern og skape tillitskrise. Uten tydelig hjemmel og dataminimering kan teknologien føre til urettmessig overvåking, brudd på personvern og risiko for svekket rettssikkerhet, særlig ved bruk i sivile plattformer og kollektivtransport.

Samlet vurdering – MIDDELS RISIKO

Styrings-, navigasjons- og kontrollteknologier vurderes samlet som middels risiko. Teknologien er kjerne for sikker og effektiv drift i luftfart, sjøfart, logistikk, forsvar og nødetater, slik at feil, manipulasjon eller bortfall raskt kan gi ulykker, tap av liv og omfattende driftsstans. Systemene bygger ofte på globale komponentkjeder og er avhengige av satellittbaserte tjenester som kan være utsatt for jamming og spoofing, noe som gir både direkte og indirekte sårbarheter. Samtidig er norsk publiserings- og prosjektaktivitet relativt lav, med betydelig samarbeid med land utenfor tradisjonelle sikkerhetspartnerskap på nærliggende områder. Kombinasjonen av områdets viktighet, eksponering og begrenset nasjonal kontroll tilsier at dette bør prioriteres i både sikkerhets- og kompetansearbeid.



Figur 7 Grafisk fremstilling av den samlede risikoen for Styring, navigasjon og kontrollteknologier, inkludert avionikk og maritim posisjonering

8. Avanserte sensorteknologier, Elektro-optisk, radar, kjemisk, biologisk, stråling og distribuert sensorer

Bredt muliggjørende på tvers av sektorer. Avanserte sensorer benyttes i en rekke anvendelser, inkludert helseovervåking, miljøovervåking, industriell automasjon, sikkerhetssystemer og autonome kjøretøy. Teknologien «samler inn sanntidsmålinger med høy presisjon» som forbedrer ytelse, sikkerhet og effektivitet. Kritisk i forsvar/beredskap. Elektro-optiske, 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. Norsk kontekst: stor aktivitet og moden kompetanse. Norske miljøer rapporterer høy aktivitet og sensitivitet i advanced sensing (20 enheter oppgir aktivitet; flertallet vurderer området som sensitivt), og mange vurderer høy sannsynlighet for militær bruk. Dette underbygger høy verdi/utbredelse på tvers av bruksområder.

Eksponering for utenlandske aktører – HØY RISIKO

Avanserte sensorer har høy militær og strategisk verdi og norske FoU- og industrimiljøer er attraktive mål for fordekte anskaffelser, spionasje, kunnskapsoverføring og leverandørpåvirkning. E-tjenesten beskriver i FOKUS 2025 at Russland, Kina, Iran og Nord-Korea benytter forskningssamarbeid og komplekse innkjøpsnettverk for å skaffe vestlig teknologi; norsk sensorteknologi nevnes uttrykkelig som et attraktivt mål. PST skriver i sin nasjonale trusselvurdering for 2025 at det forventes fortsatt fordekte anskaffelsesforsøk mot norske virksomheter i 2025. NSM peker i Risiko 2025 på sårbarhet i leverandørkjeder/ anskaffelser. Volumet på publiseringer innenfor avanserte sensorteknologier i perioden 2015-2024 er lavt, og blant de områdene som har hatt lavest vekst, fra 24 til 54 artikler. Elektrooptiske, kjemiske, biologiske og distribuerte sensorer, radar- og strålingssensorer er den største underkategori under avanserte sensorteknologier i NIFUs analyse. Når det gjelder siteringer ligger Norge godt under verdensgjennomsnittet innenfor dette teknologiområdet. Kina er blant de viktigste samarbeidspartnerne, men samarbeidet er sterkest med USA og Tyskland. Samarbeidet med andre europeiske land (Nederland, Storbritannia, Finland, Frankrike, Italia, Polen) er også betydelig.

Regulatorisk kontroll og etterlevelse – MIDDELS RISIKO

Regelverket er på plass og i utvikling, men gråsoner og operasjonell kompleksitet gjør at vi ikke kan karakterisere etterlevelsen som fullt ut moden på tvers av hele feltet. Det finnes etablerte rammer for regulering av avanserte sensorteknologier (Wassenaar, ITAR/EAR, norsk eksportkontroll) som omfatter store deler av sensorfeltet. Norge har i tillegg sikkerhetsloven og arbeider med oppdatering av eksportkontrollforskriften. Samtidig skaper dual-use og kunnskapsoverføring i forskning reelle gråsoner (særlig immateriell overføring) og det blir stadig vanskeligere å skille sivil/militær bruk – noe som øker feilmarginen i praktisk etterlevelse.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Avanserte sensorer er kjernekapasiteter i moderne militære operasjoner (ISR, målfølging, presisjonsleveranse, tidlig varsling) og i CBRN-beredskap. Avanserte sensorteknologier spiller en kritisk rolle i moderne militære operasjoner, inklusive integrasjon på ubemannede systemer (UAS/UGV/USV) for autonom effekt.

Betydning for kritisk infrastruktur – SVÆRT HØY RISIKO

Avanserte sensorer brukes bredt i samfunnskritiske funksjoner (overvåking/varsling, industriell drift, helse, miljø, transport). Svikt, manipulasjon eller bortfall vil kunne gi store forstyrrelser på tvers av flere kritiske kjeder; enkelte delområder kan være systemkritiske (ATC-radar, radiologisk varsling, store distribuerte sensornett).

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – MIDDELS RISIKO

Nasjonal sikkerhetsstrategi fremhever at Norge skal søke teknologisk lederskap på blant annet sensorteknologi, Avanserte sensorer er muliggjørende på tvers av verdikjeder (energi, transport, industri, helse) og løftes av EU nettopp fordi de påvirker økonomisk sikkerhet/konkurranseevne og avhengigheter i forsyningskjeder. Misbruk (IP-lekkasje, manipulasjon av måledata, komponentmangel) kan gi store direkte tap og forstyrre markeder på tvers av sektorer. Enkeltdeler av feltet (radar, radiologisk varsling, store distribuerte sensornett) kan, ved alvorlige hendelser, nærme seg systemisk risiko.

Hurtig teknologisk utvikling og global leverandørkjede øker risiko for forstyrrelser/kostnadsstøt ved misbruk eller bortfall.

Innenfor *avanserte sensorteknologier* har Norge en relativt liten aktiv rolle i Europa. Vi deltok i 10 prosjekter i perioden 2020-2024, noe som er litt under halvparten av andre nordiske land. Norge er tildelt merkbart mindre midler enn andre europeiske land. Norges prosentandel tildelte midler er over 10 prosentpoeng under hva som er tilfellet for alle tildelte midler totalt. Sagt annerledes: hadde Norge satset, eller lyktes, på linje med andre land innenfor dette teknologiområdet, skulle vi ha blitt tildelt nesten tre ganger så mye midler som hva vi har mottatt. Dette er noe å følge med på for å sikre at Norge har den kompetansen det er behov for fremover. SINTEF og NTNU er de mest aktive institusjonene når det gjelder prosjektdeltakelser.

Respekt for menneskeverd – HØY RISIKO

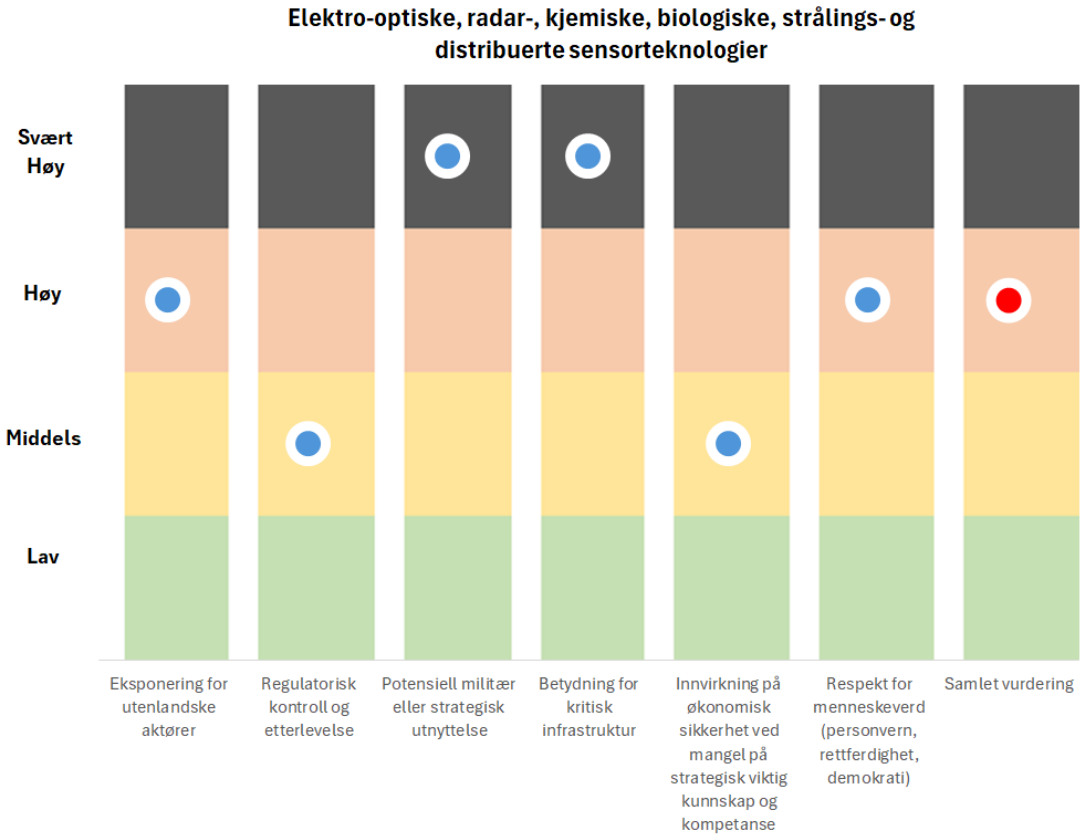
Det er en høy samlet risiko for undergraving av menneskeverd dersom avanserte sensorer brukes uten tydelig hjemmel, nødvendighets-/forholdsmessighetsvurdering og innebygde personvernmekanismer.

Avanserte sensorer kan gi store gevinster (liv/helse, sikkerhet, beredskap), men kombinasjonen av utbredt sensing, lagring og analyse (biometri, mønstergjenkjenning, datafusjon) gir betydelig risiko for urimelig inngripen i privatliv, skjevheter i behandling og nedkjølende effekt på ytring og demokratisk deltakelse. Risikoen øker ved bruk i offentlige rom, ved biometrisk identifikasjon og i distribuerte nett med lite innsyn og svak styring.

Samlet vurdering – HØY RISIKO

Samlet vurderes disse avanserte sensorteknologiene som høyrisiko. De er sentrale for overvåking, måloppdagelse, situasjonsforståelse og miljø- og strålingsovervåkning, og er derfor tett koblet til forsvars- og beredskapskapasiteter. Svikt eller kompromittering kan gi blindsoner, feilaktig situasjonsbilde eller uoppdagede hendelser, og dermed svekke nasjonal suverenitet og krisehåndteringsevne. Omfattende datainnsamling fra distribuerte sensornettverk kan i tillegg gi personvern- og rettighetsutfordringer, særlig dersom data gjenbrukes på tvers av sektorer uten

tilstrekkelig hjemmel og kontroll. Global etterspørsel og internasjonale leverandørkjeder bidrar til eksponering for innhenting og teknologioverføring. Summen er et felt med stor operativ betydning og tydelig behov for kontroll med både teknologi, data og eierskap.



Figur 8 Grafisk fremstilling av den samlede risikoen for *Elektro-optiske, radar-, kjemiske, biologiske, stråling og distribuerte sensorteknologier*

9. Romovervåkning og jordobservasjonsteknologier

Romteknologi gir grunnlaget for observasjon, måling, kontroll og drift av rombasert utstyr – essensielt for romfartens sikkerhet, situasjonsforståelse, navigasjon, miljø- og ressursovervåkning, militære og sivile operasjoner. Bred anvendelse i kommunikasjon, beredskap, forsvar, forskning, høy teknisk modenhet og muliggjørende for nasjonale kapasiteter.

Eksponering for utenlandske aktører – MIDDELS RISIKO

Romteknologi – særlig avanserte sensorer – er etterspurt globalt av både allierte og ikke-allierte aktører. Prosjekt- og leverandørkjeder strekker seg ofte over landegrenser, med avhengighet til internasjonal teknologi, komponenter og tjenesteleverandører. Romsektoren har økt risiko for spionasje, anskaffelsesmanipulasjon og avhengighet av strategisk viktige land (f.eks. for bakkesegment/software). Romfart og fremdriftsteknologier er et område hvor Norge publiserer relativt lite, men publikasjonene er høyt sitert. Det indikerer at kvaliteten er god, og at Norge kan være attraktiv å samarbeide med. NIFUs analyse viser at Norge i hovedsak samarbeider med

europeiske land på dette området. I tillegg er det noen sampublikasjoner med USA, Australia og Japan. Men det er snakk om svært få publikasjoner i perioden 2015-2024. Romovervåkning og jordobservasjons-teknologier er den nest største underkategorien under romfarts- og fremdriftsteknologier i NIFUs analyse.

Regulatorisk kontroll og etterlevelse – MIDDELS RISIKO

Internasjonale romtraktater, satellitt- og eksportkontroll, samt norske og europeiske lover gir formelle rammer. Likevel finnes regulatoriske hull i praktisk håndheving, særlig der dual-use, dataoverføring og skybaserte tjenester benyttes. Overgangen til kommersielle plattformer og internasjonale samarbeidsprosjekter utfordrer eksisterende nasjonal kontroll.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Romteknologi er kjerne for militær overvåking, etterretning, målsporing, fremdrift, navigasjon, trusselmonitorering og strategisk varsling fra rommet. De utgjør kritisk kapasitet både for offensive (målfølging, oppdagelse av trusler) og defensive (beredskap, tidlig varsling) operasjoner. Romteknologi forsterker nasjonal og internasjonal strategisk kontroll.

Betydning for kritisk infrastruktur – SVÆRT HØY RISIKO

Rombaserte sensorer er avgjørende for driften av samfunnskritisk infrastruktur: navigasjon, kommunikasjon, værvarsling, ressursorientering, monitorering og beredskap. Feil eller kompromittering kan ramme flere sektorer samtidig, med kaskadeeffekter nasjonalt/internasjonalt (f.eks. GNSS-svikt, overvåkingsfeil, tap av romkommunikasjon).

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – HØY RISIKO

Nasjonal sikkerhetsstrategi fremhever at Norge skal søke teknologisk lederskap på blant annet romteknologi Dersom Norge ikke har tilstrekkelig nasjonal kunnskap og kompetanse innen romovervåkning og jordobservasjons-teknologier, risikerer landet å miste evnen til å utvikle, anvende og forvalte informasjon om vær, klima, ressursforvaltning, miljøovervåking, beredskap og kontroll over norske interesser i nordområdene. Manglende kompetanse øker avhengigheten av utenlandske aktører for kritiske data og tjenester, noe som kan gi høyere kostnader, dårligere tilpasningsmuligheter ved geopolitisk uro og redusert nasjonal kontroll over strategisk viktig informasjon. Manglende evne til å innovere og drive egen teknologiutvikling kan svekke konkurranseevne for norske bedrifter innenfor rom- og jordobservasjonstjenester, samt føre til tapte eksportmuligheter og redusert attraktivitet for investeringer. På lengre sikt kan dette føre til svekket beredskap, en mer sårbar økonomi. Norge gjør det ikke spesielt bra innenfor romfarts- og fremdriftsteknologier når det gjelder deltakelse i EUs rammeprogrammer. Norge har kun mottatt en sjettedel av midlene sammenlignet med et europeisk gjennomsnitt. Teknologiområdet er et stort felt i europeisk sammenheng. Ifølge NIFUs analyse kan det virke litt rart at Norge mottar relativt få midler, gitt de gode siteringstallene Norge har på dette området. Norge deltok kun i tre EU-prosjekter i perioden 2020-2024.

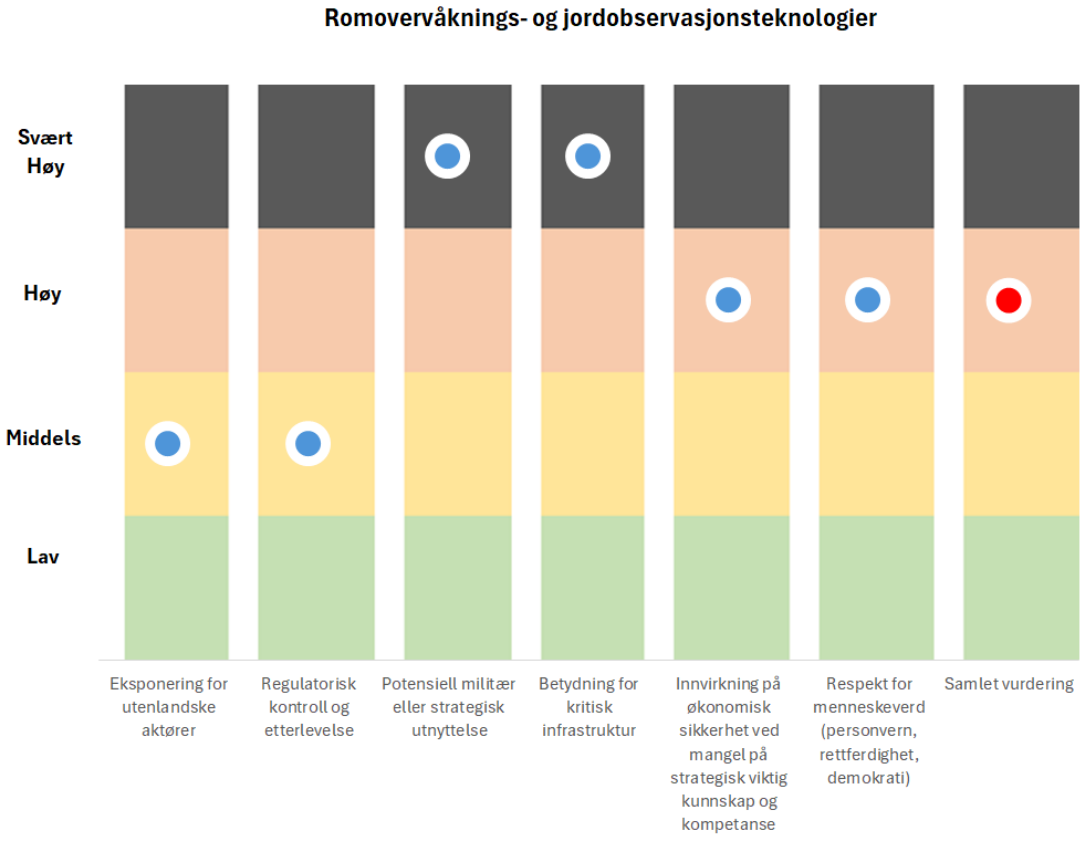
Respekt for menneskeverd – HØY RISIKO

Bred datainnhenting fra rombaserte sensorer kan gi mulighet for omfattende overvåking, profilering og kartlegging av aktiviteter/miljøer. Risiko for urimelig overvåking og misbruk av rombasert

biometrisk/gis-data er betydelig – spesielt der sivile og militære formål glir over i hverandre og det er svake kontrollmekanismer.

Samlet vurdering – HØY RISIKO

Romovervåkings- og jordobservasjonsteknologier vurderes samlet som høyrisiko. De utgjør grunnlaget for overvåking av rom- og bakkebaserte aktiviteter, navigasjon, miljø- og klimaovervåkning, ressurskartlegging og militær situasjonsforståelse. Avhengigheten av internasjonale samarbeid, kommersielle plattformer og utenlandske komponenter gir betydelig eksponering for både teknologioverføring, dataavhengighet og mulige skjulte sårbarheter. Samtidig kan høyoppløselige og hyppige observasjoner gi inngrep i personvern og suverenitet dersom bruken ikke er klart regulert og transparent. Selv om norsk volum er relativt lite, er kvaliteten høy og systemene ofte tett koblet til kritisk infrastruktur og beredskapsfunksjoner, noe som samlet trekker risikonivået opp.



Figur 9 Grafisk fremstilling av den samlede risikoen for Romovervåkings- og jordobservasjonsteknologier

10. Kraftteknologier, inkludert smarte strømnett, energilagring og batterier

Energiteknologier spenner fra smarte nett, batterier og andre lagringsløsninger til hydrogen og små modulære reaktorer. De muliggjør integrasjon av fornybar energi, fleksibel styring og elektrifisering av kjøretøy og baser. Smart-grid digitaliserer kraftsystemet og gjør det mulig å overvåke og korrigere feil før de oppstår, forbedre kapasitetsutnyttelsen og integrere sol-, vind- og bølgeenergi. Energilagring gir forsyningssikkerhet og beredskap for militære operasjoner og sivilsamfunn ved å

sikre strøm til bærbar elektronikk, kjøretøy og kommunikasjonssystemer. Utviklingen av avanserte batterier og brenselceller krever store mengder sjeldne jordartsmetaller, litium, nikkel og kobolt. EU er i dag svært avhengig av import fra Kina: rundt 98 % av Europas sjeldne jordarter og over 90 % av permanente magneter kommer fra kinesiske leverandører, og Kina kontrollerer 70 % av gruveproduksjonen og 85–90 % av raffineringen. Etterspørselen etter sjeldne jordarter forventes å øke seks ganger og etterspørselen etter litium tolv ganger innen 2030. Denne avhengigheten gjør energiteknologier sårbare for geopolitisk press og leveranseforstyrrelser. Samtidig skaper økt digitalisering av kraftnettet nye angrepsflater og gjør cybersikkerhet til en viktig del av smart-grid-arbeidet.

Eksponering for utenlandske aktører – HØY RISIKO

Leverandørkjeden for smart-grid-utstyr, kontrollsystemer og batterikomponenter er global. Norge og Europa importerer mesteparten av sine sjeldne jordarter, litium og andre råvarer fra Kina. Også mye av programvaren og maskinvaren til styringssystemer utvikles i USA eller Asia. Denne avhengigheten kan utnyttes til spionasje, sabotasje eller leveranseboikott. Økt bruk av IoT-komponenter og åpne standarder i smart-grid øker eksponeringen for aktører med andre interesser. Derfor vurderes risikoen som høy. Innenfor energiteknologier er antall publikasjoner fem ganger så mange i 2024 som i 2015 (213 mot 41 artikler). Kraftteknologier, inkludert smarte strømnett, energilagring og batterier er den største underkategorien under energiteknologier i NIFUs analyse. Generelt er artikler med deltakelse fra de mest aktive norske institusjonene høyt sitert. Det er grunn til å anta at Norge er et attraktivt samarbeidsland på dette området. Kina er Norges viktigste samarbeidspartner innen energiteknologier, målt i antall felles publikasjoner. Samarbeidet med Kina har økt over tid og er særlig sterkt innen underområdene smarte nett, energilagring og nullutslippsteknologier. India er nest viktigste samarbeidspartner, og har også et betydelig antall felles publikasjoner med Norge. Norske institusjoner som SINTEF og NTNU er de mest sentrale aktørene i prosjekter og publikasjoner innen energiteknologier.

Regulatorisk kontroll og etterlevelse – MIDDELS RISIKO

Energisektoren er regulert av nasjonale og europeiske regelverk som energiloven, elsikkerhetsforskrifter, NIS-direktiv og sikkerhetsloven. Disse dekker deler av digital sikkerhet, leveransesikkerhet og personvern. Likevel utvikles regelverket i etterkant av den teknologiske utviklingen, spesielt for distribuerte lagringssystemer, mikronett og IoT i kraftnett. Det er behov for harmoniserte standarder og tilsyn for cybersikkerhet og for håndtering av råvareleveranser. Derfor vurderes Regulatorisk kontroll som middels.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Energi- og kraftsystemer er strategiske mål i konflikter. Ved å kontrollere eller forstyrre smart-grid og lagringssystemer kan en angriper lamme militære baser, radarer, kommunikasjon og industri. Moderne våpensystemer som laser- og mikrobølgevåpen er avhengige av høy effekt og stabil krafttilførsel, og avansert batteriteknologi er nødvendig for elektrifiserte kjøretøy og droner. Sabotasje eller manipulasjon av energiforsyningen kan derfor gi en betydelig strategisk fordel. Risikoen vurderes som svært høy.

Betydning for kritisk infrastruktur – SVÆRT HØY RISIKO

Strømforsyningen er grunnmuren i alle samfunnsfunksjoner. Feil, cyberangrep eller bortfall i smart-grid, lagring eller batterier kan føre til omfattende strømstans, stans i transport, helse- og kommunikasjonstjenester og svekket beredskap. I takt med økt elektrifisering vil samfunnets avhengighet av stabile energisystemer bare øke, og kaskadeeffektene av et avbrudd blir større.

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – MIDDELS RISIKO

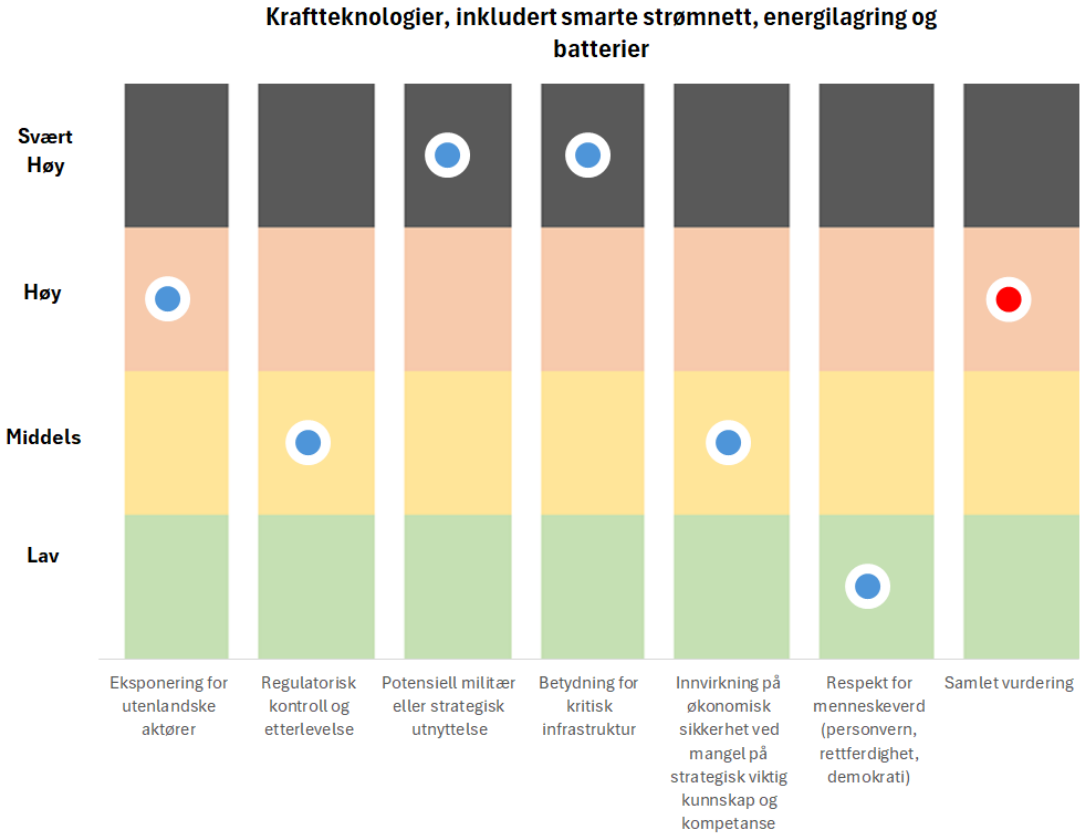
Norge har begrenset industriell kapasitet innen avanserte batterier, brenselceller og smart-grid-programvare. Dersom vi ikke bygger opp kompetanse i FoU-miljøer og næringsliv, kan vi bli fastlåst i importavhengighet av råvarer og teknologi fra land som Kina. Manglende investeringer i forskning, resirkulering og produksjon av batterimaterialer kan føre til tapt verdiskaping og økt sårbarhet for pris- og leveransesjokk. For å sikre økonomisk sikkerhet og konkurransekraft må Norge utvikle egne verdikjeder og fagmiljøer. Norge har sterk kompetanse innenfor energiteknologier. Energiteknologier er det nest største området etter kunstig intelligens når det gjelder tildeling av EU-midler innenfor sensitive teknologier. Det er fem prosent over det europeiske gjennomsnittet. Dette er det eneste teknologiområdet der Norge har det høyeste antallet prosjekter i Norden.

Respekt for menneskeverd – LAV RISIKO

Smart-grid-systemer registrerer detaljerte forbruks- og bruksdata fra husholdninger og virksomheter. Misbruk av disse dataene kan avsløre livsmønstre og føre til overvåking eller diskriminering. Personvernregler som GDPR og energiloven gir beskyttelse, men innsamling av store datamengder krever transparente prosesser, informert samtykke og sikker lagring. Foreløpig vurderes risikoen for grove personvernbrudd som lav.

Samlet vurdering – HØY RISIKO

Samlet vurderes kraftteknologier som høyrisiko. Strømforsyning og energilagring er fundamentet for alle øvrige samfunnsfunksjoner, og feil, angrep eller bortfall i smartnett, styringssystemer eller lagringsløsninger kan gi omfattende og langvarige avbrudd med kaskadeeffekter på transport, helse, kommunikasjon og beredskap. Avhengighet av utenlandske leverandører av avanserte batterier, programvare og komponenter, særlig fra ikke-allierte, øker sårbarheten for leveransesjokk, prispress og skjulte svakheter. Samtidig gir smarte målesystemer og detaljerte forbruksdata personvernrisiko hvis styring og etterlevelse ikke er tilstrekkelig. Selv om Norge har sterke fagmiljøer og god tilgang på EU-midler, gjør kombinasjonen av hvor viktig området er, teknologiske endringer og avhengighet av leverandører at området bør regnes som spesielt viktig for nasjonale interesser.



Figur 10 Grafisk fremstilling av den samlede risikoen for Kraftteknologier, inkludert smarte strømnett, energilagring og batterier

11. Ubemannede farkoster (i luft, på land, på overflaten og under vann)

Bredt muliggjørende og kjerne for automatisering og effektivisering. Ubemannede farkoster som droner og autonome kjøretøy understøtter overvåking, inspeksjon, logistikk, redning, miljø og militære operasjoner, og er i bruk på tvers av energi, transport, forsvar, industri og landbruk. Modenheten sprer seg fra nisje til operasjonell bruk, særlig for beredskap, situasjonsforståelse og sanntids respons.

Eksponering for utenlandske aktører – HØY RISIKO

Teknologien er globalt etterspurt, og forsyningskjeder er ofte internasjonale – særlig for komponenter (sensorer, batterier, programvare). Produsenter fra ikke-allierte land (f.eks. Kina) er ledende, og risikoen for spionasje, manipulasjon/innhenting via leverandører og programvare er betydelig. Kunnskaps- og teknologioverføring skjer gjennom FoU, eksport og globale prosjekter. NTNU, SINTEF og UiO er de mest aktive norske institusjonene innenfor *robotikk og autonome systemer*. Norge har relativt høye siteringstall for *robotikk og autonome systemer,* noe som indikerer at kvaliteten er god og at Norge kan være attraktiv å samarbeide med. For *droner og kjøretøy* publiserte Norge mest sammen med USA og Kina i perioden 2015-2024. Sampublikasjonene med Kina er høyt siterte. I 2024 var Kina Norges viktigste samarbeidspartner innen *robotikk og autonome systemer* med 8 artikler, noe som er en nedgang fra 2023.

Regulatorisk kontroll og etterlevelse – HØY RISIKO

Sektorregelverk finnes (luftfart, veitransport, sjøfart, datasikkerhet, sikkerhetsloven), men feltet er i sterk utvikling og preget av manglende modenhet i nasjonalt og internasjonalt regelverk for autonomi, sensorbruk, integrasjon, datadeling og fjernstyring. Det er vesentlige gråsoner rundt datafangst, operativ ansvarfordeling og personvern.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Militær verdi er svært høy. Droner og autonome kjøretøy brukes til rekognosering, måloppdagelse, beredskap, kommunikasjon, offensive/defensive operasjoner og logistikk. Muliggjør skjult/risikofri innhenting, fjernstyrte angrep og styrkebeskyttelse. I hybridkonflikt, sivil bruk og beredskap spiller de økende strategisk rolle, med fare for eskalering og misbruk.

Betydning for kritisk infrastruktur – HØY RISIKO

Systemene brukes til drift/vedlikehold/overvåking av kritisk infrastruktur. Svikt, sabotasjer eller kompromittering kan ramme varsling, inspeksjon, leveranse og beredskap for strømnett, vann, transport, olje/gass og industrien. Feilbruk kan gi kaskadeeffekter, tap av kontroll og vanskelige hendelser på tvers av sektorer (f.eks. flyhavari, stopp i logistikk, miljøskade).

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – MIDDELS RISIKO

Dersom Norge mangler eller mister sentral kunnskap og kompetanse om droner og autonome kjøretøy, reduseres muligheten til å utvikle, tilpasse og produsere avanserte løsninger til både sivile og militære formål. Dette kan føre til at norske aktører blir mer avhengige av utenlandske teknologileverandører, med økt risiko for tap av kontroll over kritiske funksjoner, styringssystemer og data. Manglende kompetanse svekker muligheten til innovasjon og effektivisering i viktige næringer som energi, transport, maritim virksomhet, miljøovervåking og beredskap, og gjør det vanskeligere å konkurrere i markeder der digitale og autonome løsninger blir stadig viktigere. *Droner og kjøretøy* er den største underkategorien under *robotikk og autonome systemer* i NIFUs analyse, og utgjør om lag 85 prosent av publiseringen innen teknologiområdet. Norge har relativt høye siteringstall for *robotikk og autonome systemer,* noe som indikerer at kvaliteten er god. Publiseringsvolumet er imidlertid lavt, med 405 artikler i perioden 2015-2024. Når det gjelder EU-midler ligger den norske andelen litt over gjennomsnittet for EU-land for tildelinger innenfor *robotikk og autonome systemer.* Norge har også relativt høy grad av koordinering i prosjekter, noe som indikerer god kvalitet på forskningen. De nordiske landene har nokså likt aktivitetsnivå på dette teknologiområdet.

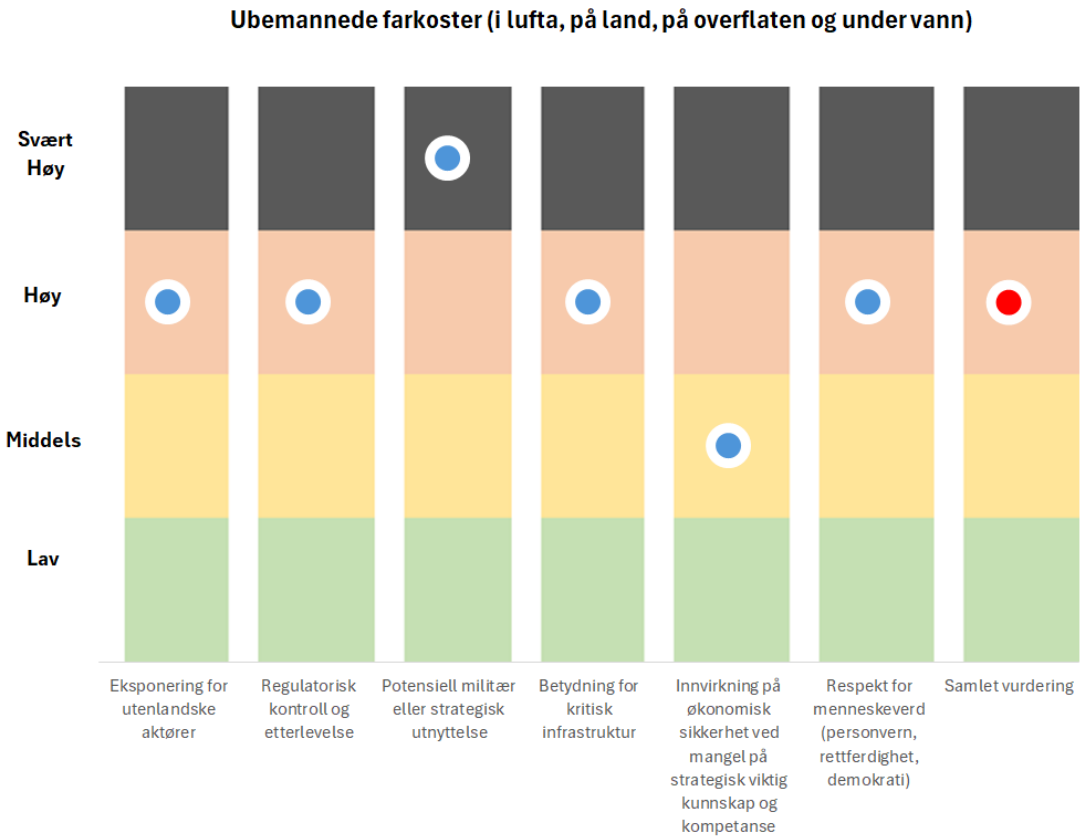
Respekt for menneskeverd – HØY RISIKO

Omfattende datainnsamling via sensorer/kameraer, posisjonering, og registrering av aktivitet – både offentlige og private – gir stor personvernsrisiko, særlig ved urimelig overvåking, profiling, eller feil/bevisst misbruk. Uklarhet i hjemler og databehandling, kombinert med manglende ansvarsdokumentasjon, kan gi krenkelser av rettigheter og tillitsbrudd.

Samlet vurdering – HØY RISIKO

Ubemannede farkoster vurderes samlet som et område med høy risiko. Teknologien er bredt muliggjørende og i rask overgang fra nisje til operativ bruk i både sivile og militære sammenhenger,

blant annet for overvåking, logistikk, inspeksjon og våpenlevering. Markedet domineres i stor grad av aktører fra land utenfor tradisjonelle sikkerhetspartnerskap, noe som gir betydelig eksponering for spionasje, manipulasjon, skjult datainnhenting og leverandørstyrt «lock-in». Integrasjon i luftrom, til sjøs og på land skaper i tillegg komplekse sikkerhets- og reguleringsutfordringer, der svikt eller misbruk kan gi raske og alvorlige hendelser. Selv om norske fagmiljøer er relativt sterke, tilsier kombinasjonen av operativ nærhet, internasjonal avhengighet og potensial for autonome våpen at området må håndteres som særlig sensitivt.



Figur 11 Grafisk fremstilling av den samlede risikoen for Ubemannede farkoster

12. KI-drevne systemer

KI-drevne drifts- og kontrollsystemer brukes i kritisk infrastruktur (kraft, vann, transport, helse, beredskap, industri). Feil, manipulasjon eller svikt kan gi alvorlige driftsstans, feilmanøvrering, tap av styring/tilgjengelighet – og kaskadeeffekter på tvers av GNF-sektorer. Automatisering og manglende menneskelig inngripen kan forsterke negative effekter ved hendelser.

Eksponering for utenlandske aktører – MIDDELS RISIKO

Dersom Norge ikke utvikler og opprettholder tilstrekkelig nasjonal kompetanse innen KI-drevne systemer, kan det begrense muligheten for å ta i bruk og videreutvikle intelligente og autonome løsninger i næringsliv, offentlig sektor og samfunnskritiske funksjoner. Manglende kapasitet på dette

området kan føre til at norske virksomheter blir avhengige av utenlandske leverandører for både programvare, vedlikehold og utvikling av KI-systemer. Dette øker risikoen for teknologisk "lock-in", tap av strategisk kontroll over egen verdikjede og muligheten til å oppdage og håndtere sikkerhetsutfordringer på egne premisser. Samtidig kan svak innenlandsk kompetanse gjøre det vanskelig å opprettholde konkurranseevne i markeder som i økende grad etterspør intelligente systemer og datadrevne tjenester. Over tid kan dette føre til lavere produktivitet, færre eksportmuligheter, tap av arbeidsplasser og reduserte investeringer, samt mindre evne til å håndtere teknologiske skift eller beskytte nasjonale interesser, noe som samlet svekker økonomisk sikkerhet. *KI-drevne systemer* er den nest største underkategori under *robotikk og autonome systemer* i NIFUs analyse. I perioden 2015-2024 har det kun vært 38 publikasjoner av totalt 554 innen *KI-drevne systemer*. Norge har heller ikke hatt en like stor vekst innen *robotikk og autonome systemer* som for de fleste andre teknologiområder. Dette indikerer at Norge kanskje ikke er så attraktiv å samarbeide med innen *KI-drevne systemer*.

Regulatorisk kontroll og etterlevelse – SVÆRT HØY RISIKO

Regelverk finnes for fysisk sikkerhet, datasikkerhet, personvern og autonomi, men KI-integrasjon utfordrer praktisk tilsyn og etterlevelse. Tydelige hull finnes rundt ansvar, transparens, algoritmekontroll, etikk, datakvalitet og robusthet mot manipulasjon/bias. Modenhet varierer mellom sektorer og applikasjoner, og regulatoriske rammer henger etter teknologiutviklingen.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

KI-drevne systemer gir svært høy operativ og strategisk verdi innen forsvar, beredskap, etterretning, cybersikkerhet, rekognosering, målutvelgelse og offensive/defensive operasjoner. Autonome våpen- og droner er i ferd med å redefinere fremtidens trussel- og forsvarsbilde, gir mulighet for skjulte, selektive og raske angrep, og kan spille en nøkkelrolle i hybridkrigføring.

Betydning for kritisk infrastruktur – HØY RISIKO

KI-drevne drifts- og kontrollsystemer brukes i kritisk infrastruktur (kraft, vann, transport, helse, beredskap, industri). Feil, manipulasjon eller svikt kan gi alvorlige driftsstans, feilmanøvrering, tap av styring/tilgjengelighet. Automatisering og manglende menneskelig inngripen kan forsterke negative effekter ved hendelser.

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – MIDDELS RISIKO

Dersom Norge ikke utvikler og opprettholder tilstrekkelig nasjonal kompetanse innen KI-drevne systemer, kan det begrense muligheten for å ta i bruk og videreutvikle autonome løsninger i næringsliv, offentlig sektor og samfunnskritiske funksjoner. Manglende kapasitet på dette området fører til at norske virksomheter blir avhengige av utenlandske leverandører for både programvare, vedlikehold og utvikling av KI-systemer. Dette øker risikoen for tap av strategisk kontroll over egen verdikjede og muligheten til å oppdage og håndtere sikkerhetsutfordringer på egne premisser. Svak innenlandsk kompetanse gjør det vanskelig å opprettholde konkurranseevne i markeder som i økende grad etterspør autonome systemer. Over tid kan dette føre til lavere produktivitet, færre eksportmuligheter og reduserte investeringer, samt mindre evne til å håndtere teknologiske skift eller beskytte nasjonale interesser, noe som samlet svekker økonomisk sikkerhet. Norge publiserer relativt lite innen *KI-drevne systemer*. Generelt gjør Norge det godt i EUs rammeprogram innen

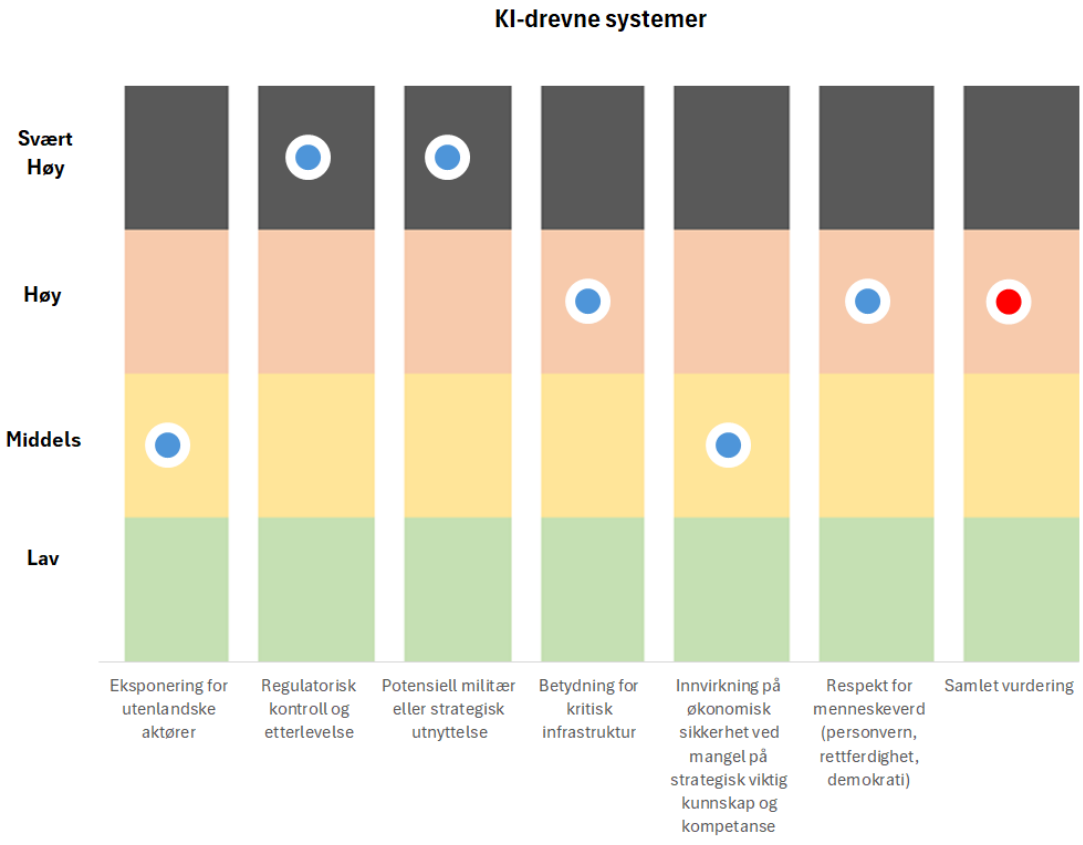
robotikk og autonome systemer, både når det gjelder tildelte midler og grad av koordinering i prosjekter. Det er imidlertid ikke mulig å si hvor mange av prosjektene som er innen *KI-drevne systemer*. Ut fra publiseringsstatistikken er det et mye høyere volum på forskningen på *droner og kjøretøy* innen *robotikk og autonome systemer*. Det kan være verdt å følge med på utviklingen innen *KI-drevne systemer*.

Respekt for menneskeverd – HØY RISIKO

KI-drevne systemer gir stor risiko for overvåking, datainnsamling, profilering og automatisert beslutningstaking med direkte effekt for individer og grupper. Manglende transparens, kontroll, etikk og ansvar kan gi feil, diskriminering og urimelig inngripen i privat- og arbeidsliv. Automatisk maktutøvelse og bias kan undergrave rettigheter og offentlig tillit.

Samlet vurdering – HØY RISIKO

KI-drevne systemer vurderes samlet som høyrisiko. De brukes i økende grad til styring, overvåking og optimalisering i kritisk infrastruktur, industri, transport og forvaltning, ofte med høy grad av autonomi og begrenset menneskelig inngripen. Feil, dataskjevheter eller målrettet manipulering kan derfor gi direkte utslag i form av driftsstans, feilprioriteringer, uønsket adferd eller sikkerhetsbrudd. Samtidig innebærer omfattende datainnsamling og automatisert beslutningstaking betydelig personvern- og rettighetsrisiko, spesielt der transparens, sporbarhet og ansvarslinjer er svake. Norske fagmiljøer er små og det internasjonale regelverket er i utvikling, noe som samlet gir et risikobilde hvor både teknisk og organisatorisk styring må forsterkes for å redusere sårbarhetene.



Figur 12 Grafisk fremstilling av den samlede risikoen for KI-drevne systemer

13. Teknologier for nanomaterialer, smarte materialer, avanserte keramiske materialer, lavsignaturmaterialer og trygge materialer utformet med tanke på sikkerhet og bærekraft

Disse materialene muliggjør store teknologiske sprang i forsvar, energi, transport, byggeindustri, elektronikk og helse. De er sentrale for innovative løsninger med lav vekt, økt robusthet, responsivitet og tilpasningsevne. Lavsignaturmaterialer gir beskyttelse mot oppdagelse eller identifisering, nanomaterialer gir nye egenskaper og funksjoner, smarte materialer gir aktiv respons og kontroll. Materialene utnyttes i flere GNF-sektorer og forsvar.

Eksponering for utenlandske aktører – HØY RISIKO

Utvikling, produksjon og bruk av disse materialene skjer ofte i globalt samarbeid, med tung avhengighet av internasjonale leverandører og patentmiljøer (USA, Kina, EU). Norske FoU-aktører og industri har høy eksponering for teknologioverføring, spionasje, og IP-lekkasjer. Viktige råmaterialer, bearbeidingsmetoder og testdata er ettertraktet av trusselaktører/labs utenfor alliansepartnerskap. Teknologier for nanomaterialer, smarte materialer, avanserte keramiske materialer, lavsignaturmaterialer og trygge materialer utformet med tanke på sikkerhet og bærekraft er den nest største underkategorien under avanserte materialer, produksjons- og resirkuleringsteknologier i NIFUs analyse. Det er nesten like stort som den største underkategorien, som er additiv produksjon.

Regulatorisk kontroll og etterlevelse – HØY RISIKO

Både miljø-, sikkerhets-, eksport- og arbeidsmiljøregelverk finnes, men det finnes betydelige regulatoriske hull for avanserte og «intelligente» materialer. Nanomaterialer kan ha risikable ukjente effekter/miljøpåvirkning, og lavsignatur/smarte materialer kan omgå eksisterende kontrollmekanismer. Regelverk utvikles langsomt etter innovasjonstakt; ansvar for sikkerhet/håndtering er utfordrende å følge opp.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Materialteknologier gir stor kapasitetsgevinst til forsvar (beskyttelse, skjuling, vektreduksjon, motstand, aktiv respons) og kan muliggjøre fremtidens våpensystemer, plattformer og militarisering av sivil infrastruktur. Lavsignatur-teknologi og avanserte materialer er strategiske kapabiliteter for allierte så vel som motparter; misbruk kan gi vesentlig makt/forsvarsbalanseforskyvning.

Betydning for kritisk infrastruktur – MIDDELS RISIKO

Materialteknologi muliggjør robuste, mer motstandsdyktig og miljøtilpasset infrastruktur, men også systemkritiske komponenter (sensorbeskyttelse, kabler, bygg, transport, energi). Svikt, sabotasje, rask nedbrytning eller feil/mangel på slike materialer kan gi store systemfeil, bortfall av forsvars- og beredskapskapasitet og kaskader for GNF-sektorer (spesielt energi, transport, bygg og forsvar).

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – HØY RISIKO

Mangel på nasjonal kompetanse og kunnskap innen avanserte materialteknologier kan føre til at Norge mister muligheten til å utvikle og levere innovative produkter og løsninger til sentrale

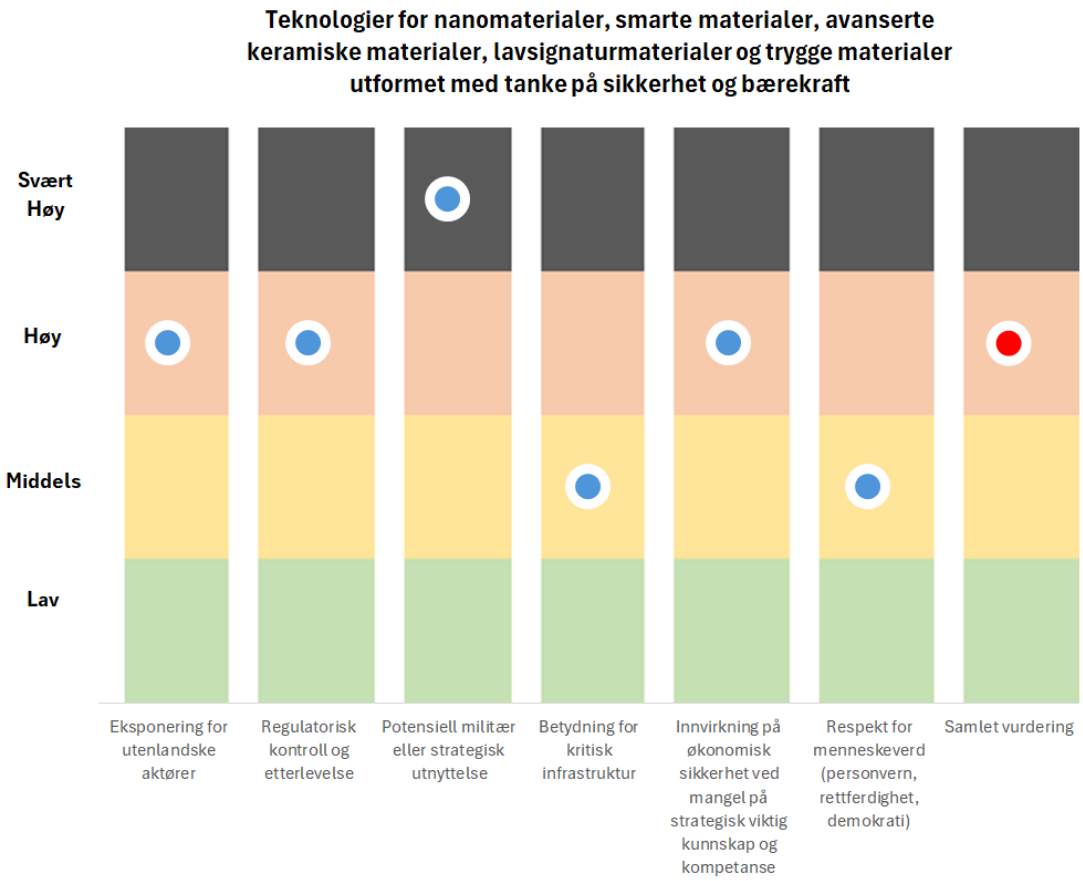
næringer som energi, forsvar, industri, transport og miljøteknologi. Dette kan gjøre norske virksomheter mindre konkurransedyktige i globale markeder, redusere muligheten for eksport og tiltrekke investeringer, og gjøre omstilling og grønn vekst vanskeligere. Uten sterke nasjonale fagmiljøer kan avhengigheten av utenlandske leverandører og forskningsaktører øke, noe som gjør norske produksjons- og verdikjeder mer sårbare for teknologiske endringer og geopolitiske hendelser. I tillegg kan manglende kontroll over utvikling og anvendelse av slike materialer begrense muligheten til å møte krav om sikkerhet, bærekraft og miljø, og svekke evnen til å drive teknologiutvikling som underbygger samfunnets beredskap, energieffektivisering og digitalisering. Over tid kan dette gi tapte arbeidsplasser, færre innovative oppstartsbedrifter og redusert økonomisk sikkerhet for Norge. *Avanserte materialer, produksjons- og resirkuleringsteknologier* er det tredje største området når det gjelder tildeling av EU-midler i perioden 2020-2024. Norge ligger litt over det europeiske gjennomsnittet for tildeling av midler innen dette området. Norge har også høy grad av koordinering av prosjekter. Norge ligger likevel bak de andre nordiske landene når det gjelder prosjektdeltakelser.

Respekt for menneskeverd – MIDDELS RISIKO

Materialteknologi har lav direkte personvernpåvirkning, men smarte/overvåkende materialer og nanoteknologi på kroppen/arbeidsplassen kan innebære risiko for usynlig overvåking/biometrisk datainnsamling. Miljø- og helsekonsekvenser er vanskelig å forutse, og ansvar og transparens er varierende, særlig ved ukjente effekter eller dårlig risikodokumentasjon.

Samlet vurdering – HØY RISIKO

Samlet vurderes disse materialteknologiene som høyrisiko. De er sentrale innsatsfaktorer i forsvar, energi, transport, elektronikk og helse, og kan gi betydelige militære og industrielle fortrinn, blant annet gjennom lav signatur, økt robusthet og nye funksjonelle egenskaper. Avhengigheten av internasjonale råvarer, patentmiljøer og leverandørkjeder øker sårbarheten for teknologioverføring, eksportkontrollbrudd og geopolitiske forstyrrelser. Samtidig er kunnskapsgrunnlaget om helse- og miljøeffekter for flere nanomaterialer begrenset, og smarte eller «overvåkende» materialer kan muliggjøre diskret datainnsamling og sporing. Kombinasjonen av strategisk betydning, regulatoriske hull og usikker risikoeksponering tilsier at området bør følges tett og håndteres restriktivt der bruksområdene er sikkerhetssensitive.



Figur 13 Grafisk fremstilling av den samlede risikoen for Teknologier for nanomaterialer, smarte materialer, avanserte keramiske materialer, lavsignaturmaterialer og trygge materialer utformet med tanke på sikkerhet og bærekraft

14. Undervannsposisjonering og navigasjon, inkludert sonarbasert navigasjon, terrengkorrelering og treghetsnavigasjon

Bredt muliggjørende og kritisk for drift av undervannsfarkoster, sensorer, rørledninger, energiinfrastruktur (olje/gass, vind, elkabler), forsvar (ubåter, USV/ROV), søk og redning, og miljøovervåking. Presis posisjonering/navigasjon er nøkkel for sikker og effektiv undervannsoperasjon – samfunnskritisk for energi, transport, miljø og beredskap. Høy modenhet på flere områder, men teknologien er utfordrende og ressurs-/kompetansekrevende.

Eksponering for utenlandske aktører – MIDDELS RISIKO

Høy interesse fra statlige, industrielle og militære aktører (både allierte og ikke-allierte) med stor etterspørsel etter sensorteknologi, akustikk, signalprosessering, styring- og navigasjonsløsninger. Leverandøravhengighet (spesielt for nøkkelelektronikk, akustiske moduler) og globale FoU-prosjekter gir høy risiko for teknologioverføring, spionasje, manipulasjon og uønskede investeringer/integrasjon. Dette er et veldig lite område internasjonalt, og sammenlignet med resten av verden har Norge en relativt sterk publiseringsaktivitet på dette området.

Regulatorisk kontroll og etterlevelse – MIDDELS RISIKO

Eksportkontroll, beredskaps-, miljø- og sikkerhetsregelverk dekker feltet, men innsatsområdene i undervannsteknologi har ofte gråsoner – særlig teknologi for dual-use/sensornett, immateriell kunnskapsoverføring, datadeling og systemintegrasjon. Uoversiktlig ansvar og varierende modenhet/tverretatlig kompetanse gir regulatoriske hull – særlig for integrerte systemer og autonome operasjoner.

Potensiell militær eller strategisk utnyttelse – SVÆRT HØY RISIKO

Teknologien er helt sentral for forsvarsoperasjoner, overvåking og sikring av nasjonale interesser – spesielt ubåtvåpen, minerydding, skjult inntrengen, ESM/ESF, og sikring av kritisk infrastruktur. Svikt, manipulasjon eller kompromittering kan gi tap av nasjonal kontroll, sviktende varsling, og strategisk handikap – muliggjør også avanserte offensive hybridoperasjoner mot norsk beredskap/forsyningslinjer.

Betydning for kritisk infrastruktur – SVÆRT HØY RISIKO

Undervannsposisjonering/navigasjon understøtter energiforsyning, rørledninger, elkabler, havvind, fiskeri, transport og beredskap. Feil, sabotasje eller kompromittering kan gi tap av styring, havari, stopp i drift, evakuering og skade på GNF-sektorer med mulig store kaskadeeffekter. Særlig sårbart for manipulerte eller målrettede systemangrep i undersjøiske nettverk. Sikkerhet og overvåkning av havbunnsinfrastruktur (gassrør, fiberkabler, energikabler) er et område som har fått økt fokus etter Nord Stream-sabotasjen.

Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse – HØY RISIKO

Nasjonal sikkerhetsstrategi fremhever at Norge skal fortsette å utvikle undervannsteknologi som styrker vår sikkerhet og sikrer vårt lederskap innenfor det maritime. Dersom Norge mangler den nødvendige kunnskap og kompetanse innen undervannsnavigasjon og -posisjonering, vil det kunne svekke sentrale konkurransefortrinn i havbasert næringsliv som olje og gass, havvind, maritim industri, fiskeri, sjøtransport og beredskap. Manglende ekspertise kan føre til økt avhengighet av utenlandske leverandører og teknologi, noe som gir dårligere kontroll over kritisk undersjøisk infrastruktur og gjør næringen mer sårbar for markedssvingninger, forsyningsforstyrrelser og teknologisk «lock-in». Uten sterke nasjonale fagmiljøer kan muligheten til å innovere, tilby nye tjenester eller delta i globale verdikjeder for undervannsteknologi bli redusert, og eksport- og investeringsmuligheter kan gå tapt. Over tid vil dette kunne føre til lavere sysselsetting, tapte markedsandeler, mindre evne til å møte nye sikkerhetsutfordringer og redusert samlet økonomisk sikkerhet for Norge som havnasjon.

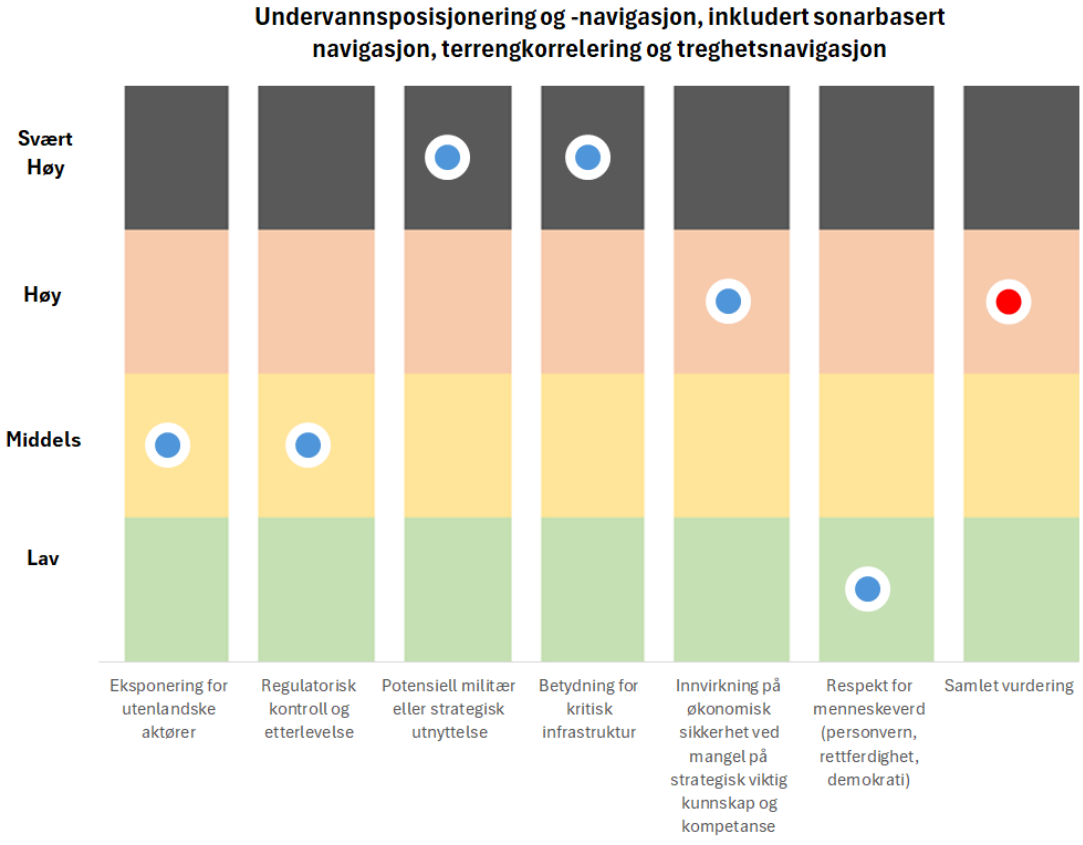
Undervannsteknologier er et lite teknologiområde for alle land EU-landene. Norge har likevel et svært lavt aktivitetsnivå, både i absolutte og relative tall når det gjelder EU-midler. Norge har et sterkt samarbeid med Tyskland i EU-prosjekter, men ikke med noen av de nordiske landene. Norsk næringsliv deltar ikke i prosjekter innen *undervannsteknologier,* i likhet med svensk næringsliv. Dette kan tyde på lavt aktivitetsnivå og kompetanse, men bildet hadde antakelig sett annerledes ut hvis vi hadde mer kunnskap om FoU i forsvarsindustrien. og ikke bare det som skjer gjennom publisering og prosjektdeltakelser. Norge har flere selskaper som leverer avanserte undervannsløsninger globalt.

Respekt for menneskeverd – LAV RISIKO

Teknologien har begrenset personvern- eller rettssikkerhetsrisiko direkte, men omfattende innsamling av drifts- og posisjonsdata, spesielt om autonomi, offshore arbeidskraft og sensitiv aktivitet, gir indirekte risiko hvis data misbrukes eller deles uten kontroll/hjemmel. Feil eller svikt kan indirekte true liv, helse og sikkerhet for mannskap/aktører.

Samlet vurdering – HØY RISIKO

Undervannsposisjonering og -navigasjon vurderes samlet som høyrisiko. Teknologien er kritisk for drift og sikring av undervannsfarkoster, rørledninger, kraft- og kommunikasjonskabler, havvind, olje- og gassinstallasjoner og militære kapasiteter, og svikt eller sabotasje kan gi alvorlige konsekvenser for energi-forsyning, beredskap og miljø. Feltet er preget av høy internasjonal interesse og tette leverandørkjeder, samtidig som norsk aktivitet innen sivil FoU er begrenset og til dels lite synlig, noe som øker sårbarheten for uønsket innhenting, avhengighet og skjulte svakheter. Samtidig kan teknologien, brukt offensivt, gi betydelige fordeler i militære operasjoner og hybridoperasjoner mot havbunnsinfrastruktur. Siden området er viktig, det finnes trusler og det er behov for mer kompetanse, bør det være en prioritet i arbeidet med nasjonal sikkerhet.



Figur 14 Grafisk fremstilling av den samlede risikoen for Undervannsposisjonering og navigasjon, inkludert sonarbasert navigasjon, terrengkorrelering og treghetsnavigasjon

Sammendrag og oppsummering av risikovurderingene

Risikovurderingene av de 14 teknologiområdene viser at sensitive teknologier favner både komplekse og sammensatte risikoer, ikke bare knyttet til mulig misbruk, men også til avhengigheter og kunnskapsbehov. Ingen av områdene vurderes å ha lav samlet risiko, og hovedbildet er at majoriteten havner i kategoriene «høy» og «svært høy» risiko, både når det gjelder risikovurderingen av hver kategori, og for den samlede vurderingen for hver teknologikategori.

Den samlede oversikten (figur 15) illustrerer alle de vurderte teknologiområdene som svært risikoutsatte og sensitive. Dette er ikke et overraskende resultat, når man tar med i vurderingen at teknologiene er hentet ut fra en oversikt over *sensitive teknologier for norske forhold.* Totalresultatene illustrerer allikevel utfordringen med å gjennomføre en overordnet risikovurdering på tvers av så ulike teknologi-områder. Dagens situasjonsbilde, med rask teknologisk utvikling, geopolitisk usikkerhet og fragmentert regulatorisk kontroll, gjør risikoen både dynamisk og vanskelig å fastsette presist. Den sammensatte karakteren til sensitive teknologier, der enkeltteknologier kan ha svært ulikt brukspotensial og risikoflater, betyr at vurderingene har svakheter. Samlet vurdering av området kan fange opp ytterpunkter, og flere teknologier bærer med seg latente risikoer som først materialiseres under visse forutsetninger.

Dette kan illustreres med å peke på at enkelte kriterier er vurdert med gjennomgående høy risiko. Særlig for «potensiell militær eller strategisk utnyttelse» er risiko satt til «svært høy» for nesten alle de vurderte teknologiene. Kriteriet fanger opp potensialet for militær og strategisk bruk i en situasjon der veldig mange teknologier er flerbruks-orienterte. De vurderte teknologiområdene er brede nok til å inneholde et stort antall ulike teknologier, som skiller seg fra hverandre i grad av militær og strategisk bruk. Resultatet uttrykker et øvre risikonivå innenfor kategoriene. Dermed blir nyansene i underliggende delteknologier ikke fullt ut synlige. Innen fotonikk kan for eksempel rettede energivåpen gi «svært høy» skår, mens lasere til medisinsk behandling ikke har samme militære og strategiske relevans. I praksis vil storparten av de mest sensitive delene av teknologiområdene allerede være underlagt nasjonale graderings- og kontrollregimer. Modellen synliggjør toppnivået av risiko i brede kategorier, men erstatter ikke mer finmasket vurdering.

Dette understreker behovet for at risikovurderinger ikke tolkes som endelige «fasitsvar», men som et dynamisk verktøy for bevisstgjøring, prioritering og løpende revurdering – med utgangspunkt i faktiske trusselbilder, nasjonale kompetansebehov og vår evne til å balansere hensynet til sikkerhet og kunnskapsutvikling. Den metodikken som er utarbeidet i prosjektet gir et strukturert rammeverk for slike vurderinger, men det forutsetter fortsatt uavhengig kvalitativ analyse og dialog mellom berørte aktører og miljøer.

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

Avsluttende kommentar

For delleveranse 4 er det utarbeidet en egen metode for risikovurdering av sensitive teknologier. Metoden er basert på en tilnærming til risikoanalyse der sannsynligheter og konsekvenser blir bestemt rent kvalitativt, og der det benyttes ord for å beskrive frekvens og alvorlighetsgrad. Metodikken måler risiko med seks kriterier. Begrensninger i tid og ressurser påvirket både hvor bred den foreslåtte modellen for risikovurdering ble, og hvor mange og brede kategorier risikovurderingen ble gjennomført på. I avsnittet som omhandler metodiske begrensninger påpeker vi at flere kriterier for risikovurdering ble foreslått, men at flere av disse ikke egnet seg for risikovurdering av kategorier som er av den bredde som vi har å gjøre med i denne rapporten. Dersom man skal gjøre en risikovurdering av teknologier eller teknologiområder som er *smalere* enn hva som er gjort i denne rapporten, vil teknologiens modenhet (TRL) kunne være modererende for øvrig risiko. Dette er noe som kan sees nærmere på i senere arbeid.

Teknologiene som vurderes er i utgangspunktet regnet som sensitive, ettersom de er foreslått å stå på en oversikt over sensitive teknologier for norske forhold. Risikovurderingen er ment å bidra til bevisstgjøring om hvorfor teknologiene vurderes som sensitive og på hvilke måter de kan være sårbare. Det at mange av teknologiene kommer ut med en samlet vurdering som «høy» eller «svært høy», betyr ikke nødvendigvis at det er ønskelig å begrense samarbeid om disse. Risikoen kan også knyttes til at det er viktig for norske sikkerhetsinteresser å tilegne seg kunnskap og kompetanse gjennom samarbeid. Spenningen mellom å beskytte og fremme er noe som ulike aktører innenfor forskningssystemet må forholde seg til. Metoden som er utarbeidet i prosjektet kan være et bidrag til å øke denne bevisstheten og en hjelp til å navigere i dette landskapet.

Figur 15 Samlet oversikt over risikovurderinger av sensitive teknologier

Teknologiområde \ Indikator	Eksponering for utenlandske aktører	Regulatorisk kontroll og etterlevelse	Potensiell militær eller strategisk utnyttelse	Betydning for kritisk infrastruktur	Innvirkning på økonomisk sikkerhet ved mangel på strategisk viktig kunnskap og kompetanse	Respekt for menneskeverd (personvern, rettferdighet, demokrati)	Samlet vurdering
Fotonikkteknologier, inkludert høyenergilaser	Middels	Middels	Svært høy	Høy	Middels	Høy	Middels
Dataanalytiske teknologier	Lav	Høy	Svært høy	Høy	Middels	Svært høy	Middels
Maskinlæring og dyplæring	Høy	Middels	Svært høy	Høy	Middels	Høy	Høy
Kvantesensorer og -radar	Lav	Middels	Svært høy	Høy	Høy	Middels	Høy
Syntetisk biologi	Middels	Høy	Svært høy	Svært høy	Høy	Svært høy	Svært høy
Cybersikkerhetsteknologier, inkludert cyberovervåkning og sikkerhets- og inntrengningssystemer, og digital etterforskning.	Høy	Middels	Høy	Høy	Middels	Høy	Høy
Styrings-, navigasjons- og kontrollteknologier, inkludert avionikk og maritim posisjonering	Middels	Middels	Svært høy	Svært høy	Middels	Middels	Middels
Elektro-optiske, radar-, kjemiske, biologiske, strålings- og distribuerte sensorteknologier	Høy	Middels	Svært høy	Svært høy	Middels	Høy	Høy
Romovervåknings- og jordobservasjonsteknologier	Middels	Middels	Svært høy	Svært høy	Høy	Høy	Høy
Kraftteknologier, inkludert smarte strømnett, energilagring og batterier	Høy	Middels	Svært høy	Svært høy	Middels	Lav	Høy
Ubemannede farkoster (i lufta, på land, på overflaten og under	Høy	Høy	Svært høy	Høy	Middels	Høy	Høy
KI-drevne systemer	Middels	Svært høy	Svært høy	Høy	Middels	Høy	Høy
Teknologier for nanomaterialer, smarte materialer, avanserte keramiske materialer, lavsignaturmaterialer og trygge materialer utformet med tanke på sikkerhet og bærekraft	Høy	Høy	Svært høy	Middels	Høy	Middels	Høy
Undervannsposisjonering og -navigasjon, inkludert sonarbasert navigasjon, terrengkorrelering og treghetsnavigasjon	Middels	Middels	Svært høy	Svært høy	Høy	Lav	Høy