Et helhetlig forskningssystem for åpen, skjermet og gradert forskning

Vedlegg til rapport

Svar på oppdrag til Forskningsrådet, Forsvarets forskningsinstitutt og Nasjonal sikkerhetsmyndighet i supplerende tildelingsbrev av 15.12.2023 fra Forsvarsdepartementet og Kunnskapsdepartementet.

Vedleggsoversikt

Vedleggene til rapporten er navngitt og nummerert etter spørsmålene i oppdraget.

Vedlegg A: Innretning av et helhetlig forskningssystem

Vedlegget beskriver forslag til innretning av et helhetlig, nasjonalt forskningssystem for å håndtere Norges totale kunnskapsbehov slik at skjermingsverdig og gradert kunnskap, herunder forsvars- og sikkerhetsrelatert forskningssamarbeid, kan sees i sammenheng med den åpne forskningen.

Vedlegg B: Vurdering av fag- og teknologiområder

Vedlegget beskriver innenfor hvilke fag- og teknologiområder er behovet for samarbeid størst i dag, og hvilke områder antas å utvikle seg til å bli viktige samarbeidsarenaer de kommende årene.

Vedlegg C: Rammer for sivil-militært samarbeid

Vedlegget beskriver hvordan sivil-militært samarbeid kan rammes inn på en måte som ikke står i veien for den åpne forskningen.

Vedlegg D: Investeringer i infrastruktur

Delleveranse fra 16. februar 2024 om hvilke investeringer i infrastruktur er nødvendig for å understøtte et nasjonalt forskningssystem for åpen, skjermingsverdig og gradert FoU.

Vedlegg E: Økonomiske og administrative konsekvenser

Vedlegget beskriver økonomiske og administrative konsekvenser av ulike løsninger, med henvisning til forvaltningsverdiene i staten.

Vedlegg F: Risiko

Vedlegget beskriver risiko knyttet til ulike løsninger.

Vedlegg G: Behov for kompetanse

Vedlegget beskriver kompetansebehov som må dekkes på kort og lang sikt for at a) et helhetlig nasjonalt forskningssystem for åpen, skjermingsverdig og gradert FoU skal kunne fungere i praksis, og b) at enkelte nye leverandører skal kunne bidra innenfor sensitivt, skjermingsverdig og gradert forsknings- og teknologisamarbeid? Skisser hvordan en slik kompetanseheving kan gjennomføres.

Vedlegg H: Bakgrunnsnotat om forskningssystemet

Dette notatet beskriver hvem som i sivil sammenheng er aktørene og brukerne i forskningssystemet, og hvordan relasjonene mellom dem påvirkes av finansiering gjennom Forskningsrådet. Det pekes også på noen elementer i dagens system som kan videreutvikles med tanke på forskning relevant for sikkerhet og beredskap. Notatet beskriver også hvordan forskningssystemet innenfor forsvarssektoren fungerer i dag, både hvem som er aktørene og hvordan de samhandler.

Vedlegg A: Innretning av et helhetlig forskningssystem

Notatet beskriver forslag til innretning av et helhetlig, nasjonalt forskningssystem for å håndtere Norges totale kunnskapsbehov slik at skjermet og gradert kunnskap, herunder forsvars- og sikkerhetsrelatert forskning, kan sees i sammenheng med den åpne forskningen.[1]

1. Innledning

Åpenhet og akademisk frihet er hjørnesteiner i et velfungerende, sivilt forskningssystem.[2] Forskningen må være basert på god vitenskapelig praksis og i tråd med etiske standarder. I et helhetlig forskningssystem som er utformet for å håndtere Norges totale kunnskapsbehov, både åpent, skjermet og gradert,[3] er det avgjørende at åpenhet og uavhengighet forblir normen for hvordan sivil forskning skal gjennomføres. Samtidig påvirker sikkerhetspolitiske spenninger forskningssystemet, blant annet ved at ambisjonen om åpenhet i økende grad må balanseres mot hensynet til nasjonal sikkerhet.[4] Dette krever økt bevissthet om forskningssikkerhet hos norske forskningsinstitusjoner og enkeltforskere. Internasjonalt forsknings- og innovasjonssamarbeid er grunnleggende for å sikre kvalitet, fornyelse og relevant kompetanse i forskningen. Økt kompetanse om forskningssikkerhet er nødvendig for at forskere og institusjoner skal kunne kartlegge hvilke typer informasjon, verdier og sårbarheter som må beskyttes, og hva som kan deles åpent.

Forskningssikkerhet

- uønsket overføring av kritisk kunnskap, kunnskap og teknologi som kan påvirke nasjonal sikkerhet,
- uønsket innflytelse på eller påvirkning av forskning som krenker akademisk frihet og forskningsintegritet
- etiske eller integritetsbrudd, der kunnskap og teknologi brukes til å undertrykke eller undergrave grunnleggende verdier.

European Commission 24.1.24 "COUNCIL RECOMMENDATION on enhancing research security" e82a2fd9-ac12-488a-a948-87639eef10d4_en (europa.eu)

Den foreslåtte løsningen for et helhetlig forskningssystem vil styrke og klargjøre samordningen mellom den åpne sivile forskningen og den forsvars- og sikkerhetsrelaterte forskningen. Dette skal understøtte kunnskapsbehovet for en styrking av nasjonal sikkerhet.

2. Forslag til et helhetlig forskningssystem

Et helhetlig nasjonalt forskningssystem må bygge på dagens forskningssystem for åpen forskning og på forsvarssektorens forskningssystem som i tillegg håndterer lukket forskning, se figur 1.[5] Dette innebærer at et utvidet forskningssamarbeid om forsvar, sikkerhet og beredskap må være basert på frivillighet og gjensidig interesse fra aktørene og forskerne som deltar.

---

[1] Langtidsplanen for forsvarssektoren (2025-2036) peker på at også *forsvarssektorens* forskningssystem skal videreutvikles. Dette diskuteres ikke nærmere her, men arbeidet bør sees i sammenheng med dette forslaget til en mulig løsning for et felles forskningssystem. Se også mer utfyllende fotnote i avsnitt 3.3.

[2] Med *sivile* forskningsmiljøer og det *sivile* forskningssystemet mener vi her de delene av forskningssystemet som normalt ikke arbeider med militære og/eller graderte problemstillinger.

[3] Vi har i dette notatet brukt ordene *skjermet* og *gradert* flere steder. Vi viser til rapportens avsnitt med definisjoner for nærmere definisjon av disse ordene. Vi understreker at vi med *gradert* primært mener gradering på nivå *begrenset*, og vi har være tydelige når vi omtaler høyere graderingen enn det.

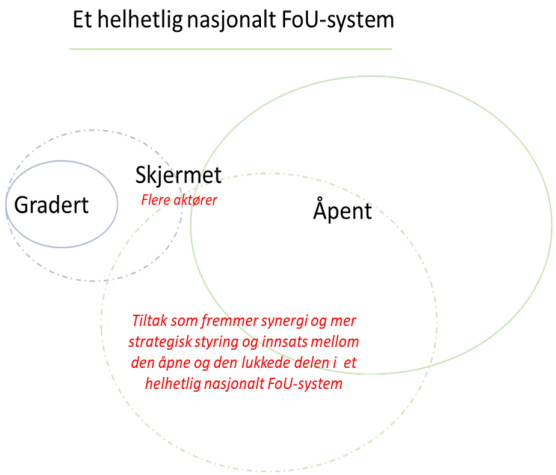
[4] *Nasjonal sikkerhet* defineres som statssikkerhetsområdet og en avgrenset del av samfunnssikkerhetsområdet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser, Meld. St. 5 (2020–2021) - regjeringen.no, side 13. De nasjonale sikkerhetsinteressene er angitt i sikkerhetslovens § 1-5.

[5] Se eget bakgrunnsnotat om forskningssystemet som beskriver nærmere aktørene og brukerne, og hvordan relasjonene mellom dem påvirkes av finansiering gjennom Forskningsrådet, og hvordan forskningssystemet innenfor forsvarssektoren fungerer i dag.

Forskning er i sin natur internasjonal, og et helhetlig nasjonalt forskningssystem må samspille godt med det internasjonale forskningssystemet. EUs pågående rammeprogram, Horisont Europa, er Norges viktigste finansieringskilde for internasjonalt samarbeid om forskning og innovasjon. I det kommende rammeprogrammet vil forskningssikkerhet og forskning og innovasjon som støtter opp under sikkerheten og konkurranseevnen til EU, være sentrale prioriteringer. Dette kan føre til restriksjoner i deltagelsen sammenlignet med Horisont Europa. For Norge er det viktig å bruke EØS-avtalen og vårt nære samarbeid med EU innenfor sikkerhets- og forsvarspolitikk som argumenter for å bli behandlet på linje med EU-landene når det gjelder deltakelse.[6] Samspillet med det europeiske forskningssystemet vil ikke bli videre utdypet i dette notatet, men et slikt samspill er en viktig forutsetning for at det nasjonale systemet som beskrives nedenfor skal kunne fungere best mulig.

Det overordnede forslaget til hvordan vi kan etablere et helthetlig nasjonalt forskningssystem er:

- Tydelig definisjon av skillet mellom den åpne og den lukkede delen i et helhetlig forskningssystem.
- Øke antallet aktører (noe) i den lukkede delen, herunder etablere flere og mer fleksible muligheter for at forskere skal kunne ta del i skjermet og gradert forskning.
- Styrke den strategiske kapasiteten og styringen av den sivile FoU-innsatsen på forsvar, sikkerhet og beredskap.
- Benytte Forskningsrådets rolle som finansiør og forskningspolitisk rådgiver for å bringe sammen aktører fra ulike sektorer og fagområder. Utvikling av ny forskningsbasert kunnskap gjennom samarbeid mellom ulike aktører er avgjørende for endring og mer synergi mellom den åpne og lukkede forskningen.



Figur 1. *Illustrasjon av et helhetlig nasjonalt forskningssystem*

Målet er å gjøre forskningssystemet bedre i stand til å understøtte nasjonal sikkerhet med forsterket strategisk koordinering, prioritering og utvikling opp mot sikkerhets- og forsvarspolitiske interesser gjennom en god utnyttelse av samfunnets ressurser. Dette inkluderer å:

- utnytte og videreutvikle den nasjonale kunnskapsbasen for å møte det nødvendige kunnskapsbehovet innen forsvar, sikkerhet og beredskap,
- utvikle og koordinere løsninger som styrker nasjonal sikkerhet og forsvarsevne,
- beskytte kunnskap og løsninger som kan utnyttes av fremmede stater til å svekke nasjonal sikkerhet.

Et nasjonalt forskningssystem og nasjonale forskningsmiljøer må samspille med internasjonale initiativer og samordninger. Dette skjer i dag både i den åpne og lukkede forskningen. Det

[6] I tillegg trengs en videreutvikling av eksisterende mekanismer for kvalifisering og ordninger som kompenserer for ulike økonomiske rammevilkår for forskningsinstitutter i Norge og resten av Europa slik at norske miljøer kan fortsette å delta i relevante partnerskap og forskningssamarbeid gjennom arenaer som EUs rammeprogram, Det europeiske forsvarsfondet (EDF) og NATO Science & Technology Organization.

foreslåtte systemet ivaretar dette samspillet, men det er det nasjonale systemet som beskrives i løsningen.

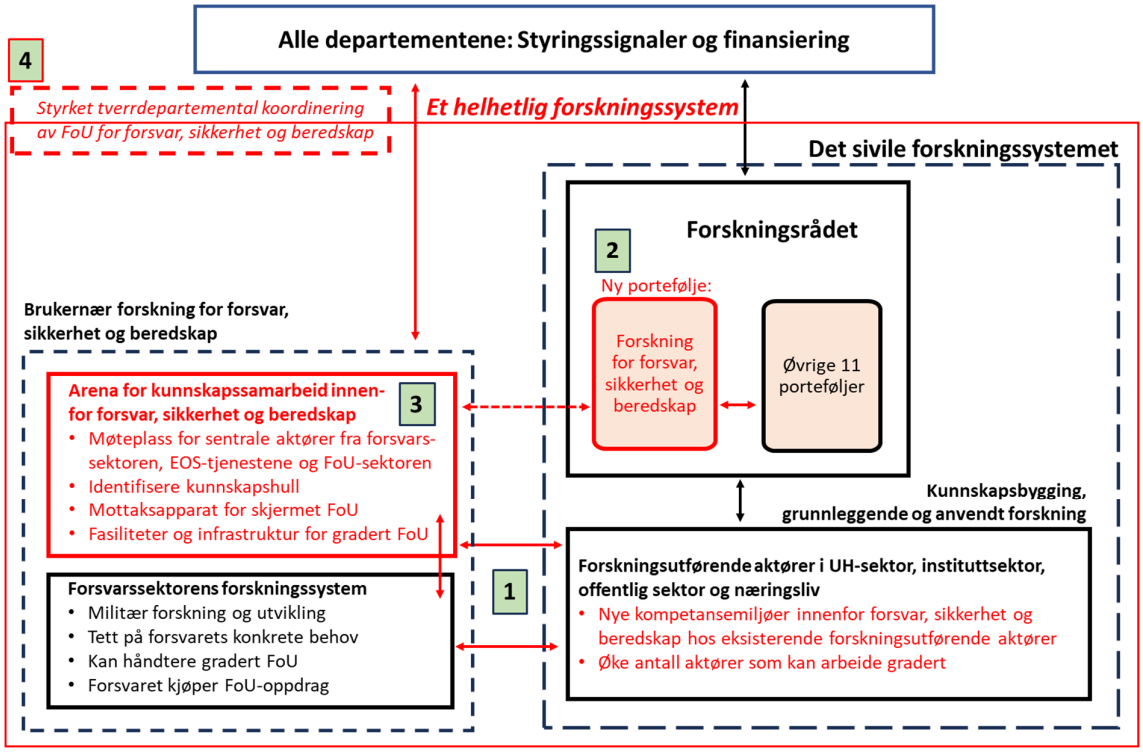
Vi foreslår fire tiltak som vil bidra til et helhetlig FoU-system der grenseoppgangene og samspillet mellom åpen, skjermet og gradert forskning fortsatt er avklart og tydelig slik at den åpne og frie forskningen har gode vilkår. De fire tiltakene er:

Tiltak 1: Økt bruk av sivile forskningsmiljøer innenfor forsvar, sikkerhet og beredskap. Et viktig element i dette er å etablere en systematikk for å identifisere flerbruksmuligheter *(dual-use)* og skjermet forskning.[7] I tillegg må antall forskningsutførende aktører som kan utføre gradert forskning øke noe.

Tiltak 2: Opprettelse av en ny portefølje i Forskningsrådet for å styrke forskning relevant for forsvar, sikkerhet og beredskap.

Tiltak 3: Etablering av en arena for kunnskapssamarbeid innenfor forsvar, sikkerhet og beredskap.

Tiltak 4: Styrket tverrdepartemental koordinering av FoU for forsvar, sikkerhet og beredskap.



Figur 2. *Illustrasjon av et helhetlig, nasjonalt forskningssystem for Norges totale kunnskapsbehov innenfor skjermet og gradert kunnskap. Nye tiltak er nummerert og endringer sammenlignet med dagens forskningssystem er markert med rødt. Nummereringen svarer til den brukt i brødteksten.*

De fire tiltakene er illustrert i figur 2 der nummeret i de grønne firkantene peker på hvert av tiltakene. Endringer sammenlignet med dagens forskningssystem er markert med rødt. Tiltakene inkluderer mekanismer som sikrer samhandling mellom forsvarssektorens forsknings-

[7] *Dual use can be defined as research conducted for legitimate purposes that generates knowledge, information, technologies, and/or products which could be utilized for both benevolent and harmful purposes.* På norsk kalles dette ofte for flerbruks*teknologi.* Men siden vi her tenker bredere enn "bare" teknologi, har vi valgt å oversette *dual use* med flerbruks*muligheter,* som for øvrig ligger tettere opp mot den engelske termen. Men også begrepet flerbruks*teknologi* er brukt i teksten der vi mener dette er mest dekkende.

system, kunnskapsarbeidet knyttet til nasjonal sikkerhet, og det sivile forskningssystemet. De er nærmere beskrevet i det følgende. I tillegg sier vi litt om hvordan samspillet mellom disse nye elementene i forskningssystemet kan bidra til at overgangene mellom åpen, skjermet og gradert forskning blir tydeligere. Vi peker også på noen tiltak som styrker muligheten for at forskere kan bidra fleksibelt i den åpne og den lukkede delen av et helhetlig forskningssystem.

3. Fire tiltak

3.1 Økt bruk av sivile forskningsmiljøer

Historisk har store statlige investeringer i forsvarsrelatert FoU hatt betydelig overføringsverdi til sivil utvikling. I dag går derimot slik kompetanseoverføring i større grad begge veier. Spesielt innenfor IKT har den sivile utviklingen nå en sterk overføringsverdi til forsvarssektoren. Kunstig intelligens, autonomi, stordata, kvanteteknologi, kommunikasjonssystemer, romteknologi, energiløsninger, materialteknologi, sensorer og modellering og simulering kan fremover forventes å ha store sivil-militære synergieffekter.

Forsvarssektorens ekspertise på militære operasjoner, fremtidens krigføring og mulighetene og konsekvensene av militær teknologi må vurdere synergieffektene. Ved å identifisere flerbruks-teknologier og videreutvikle disse for militære formål, kan innovasjonsevnen styrkes. Faglig relevante og sikkerhetskvalifiserte aktører må da inviteres inn i forsvarssektorens forsknings-, utviklings- og innovasjonsarbeid.

Forsvar, sikkerhet og beredskap

Økt overføringsverdi av kunnskap utviklet i sivil sektor gjelder bredere enn forsvarssektoren. Også innenfor øvrige deler av arbeidet med sikkerhet og beredskap ser vi økende behov for samarbeid med sivil FoU. Flere av teknologiene nevnt ovenfor har brede anvendelser.

Det er med andre ord behov for en bred styrking av forskning, utvikling og innovasjon innenfor forsvar, sikkerhet og beredskap. Flere sivile fagmiljøer med relevant kompetanse må trekkes inn i forskning og innovasjon relevant for militære og andre sikkerhetsmessige anvendelser, spesielt på områder hvor sektorene mangler kompetanse og løsninger. Dette innebærer også at antallet aktører som kan levere gradert forskning må økes, og det må legges til rette for et bredere sivil-militært samarbeid mellom forsvarssektorens forskningssystem, den nasjonale kompetansebasen og virkemiddelapparatet.

Vilje til deltagelse i forskningsmiljøene

Sivile forskningsmiljøer kan være skeptiske til å involvere seg i forskning som kan ha militære anvendelser. Like fullt er det vår erfaring at flere forskningsmiljøer, særlig i instituttsektoren, men også ved universitetene, signaliserer vilje til å arbeide med problemstillinger relevante for forsvar, sikkerhet og beredskap.[8] Samme signal kommer fra Næringslivets hovedorganisasjon.

Institutt- og UH-sektoren fremholder altså at samarbeid kan og bør utvides, ikke minst når det gjelder generisk metodeutvikling innenfor den åpne forskningen. Forskningsinstitusjonene og næringslivet signaliserer samtidig forståelse for at dette kan innebære utvikling av teknologi og kunnskap som bør skjermes eller graderes. Økt involvering av sivile aktører må skje innenfor

[8] Som del av dette arbeidet har vi hatt flere møter på strategisk nivå med ledere og seniorforskere i institutt- og UH-sektoren og med NHOs ledelse. Signalene fra samtalene entydige: De sivile FoU-miljøene ønsker å bidra.

rammen av et forsvarlig sikkerhetsnivå etter kravene i sikkerhetsloven, der nye aktører må godkjennes av Nasjonal sikkerhetsmyndighet (NSM) eller annen relevant myndighet.

Institusjoner må ha tilgang til sikre graderte systemer og ha en sikkerhetsorganisasjon på plass dersom de skal utføre forskning som inneholder gradert informasjon. Hvis nye aktører ikke kan inngå i eksisterende sikkerhetssystemer, har de behov for å etablere en sikkerhetsorganisasjon, sikkerhetskultur og tilgang til sikkerhetsgodkjent infrastruktur. Det er også behov for å drifte denne over tid. Det vil da være behov for å etablere og drifte områdesikring, personellsikkerhet og informasjonssikkerhet. Dette har også en kostnadsside, og det må vurderes hvordan slike kostnader skal finansieres i en heterogen sektor der ulike forskningsinstitusjoner har svært ulike økonomiske rammevilkår. I tillegg kan tiden det ofte tar å få personell sikkerhetsklarert forsinke samspillet. Nasjonal kapasitet til å sikkerhetsklarere kan utfordres med en stor vekst i behovet fremover. Det anbefales derfor i størst mulig grad å bygge videre på og utnytte allerede etablerte sikkerhetssystemer og organisasjoner.

Samspillet må uansett håndtere grenseoppgangene mellom ugradert, skjermet og gradert.

Behov for opplæring

Forskningssikkerhet og flerbruksmuligheter har to ulike sider ved seg som begge får konsekvenser for det åpne forskningssystemet. Det ene er å bidra til å videreutvikle kunnskap og teknologi som kan anvendes innenfor forsvarssektoren. Det andre er å bidra til beskyttelse av nasjonal sikkerhet ved å identifisere forskningens muligheter for å true nasjonal sikkerhet. Kunnskap og teknologiske fremskritt er en del av det globale militære kappløpet, og sterke forskningsnasjoner legger forskningsbasert kunnskap til grunn for militære formål. Veien fra grunnleggende forskning til anvendelse *kan* være svært kort, og dette krever god innsikt i bruksområder av egen forskning. I en krevende internasjonal sikkerhetssituasjon krever disse utfordringene opplæring og omlegging av måten man er bevisst egen forskning.[9]

For å bevare den åpne forskningen og samtidig å kunne trekke flere kompetansemiljøer inn i skjermet eller gradert forskning, er det viktig å etablere kultur, systemer og kapasitet for å kunne håndtere overgangene fra åpent til skjermet eller gradert.[10] Figur 3 illustrerer hva vi mener med slike overganger og indikerer blant annet at det vil være behov for økt forståelse og praktisk håndtering av forskningssikkerhet, som i lys av en stadig mer krevende sikkerhets-politisk utvikling har fått økende oppmerksomhet.[11]

Det er i stigende grad behov for retningslinjer og systemer som hindrer at forskning og innovasjon blir misbrukt til andre staters militære formål. Det er særlig interesse for produkter, programvare og teknologi med flerbruksmuligheter. For å møte denne økende utfordringen er det nødvending med felles og løpende vurderinger av mulige synergieffekter; overveielser som bør foretas i samspill mellom forsvarssektoren, EOS-tjenestene og Forskningsrådet.[12]

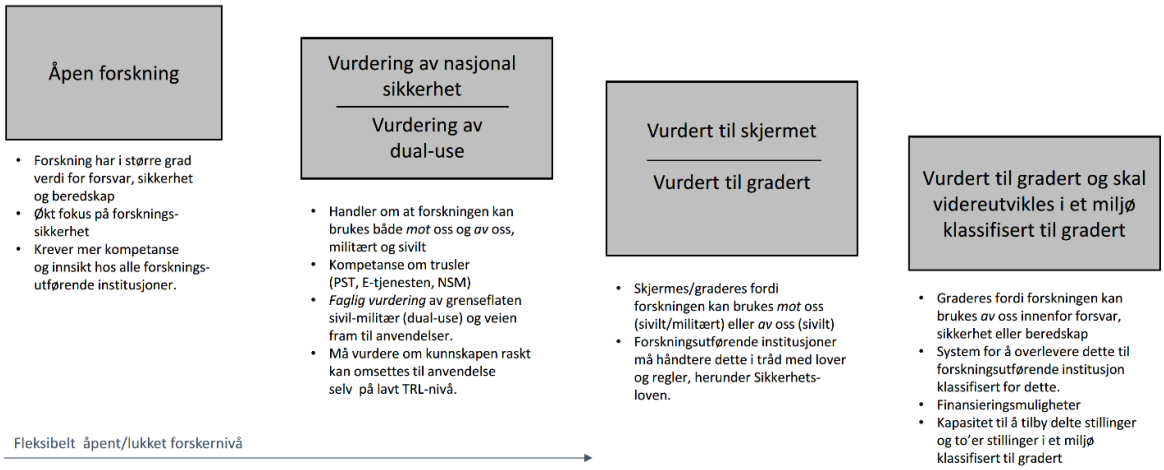
[9] Retningslinjene for Ansvarlig internasjonalt samarbeid (AIS) gir en rettesnor i dette arbeidet.

[10] Dette er mer utførlig diskutert i vedlegg C om hvordan sivil-militært samarbeid kan rammes inn på en måte som ikke står i veien for den åpne forskningen. I dette bakgrunnsnotatet har vi kortfattet drøftet noen utfordringer for den åpne forskningen i sivil-militært samarbeid, og vi skisserer tiltak som i noen grad vil kunne håndtere utfordringene. Utfordringene vi drøfter er knyttet til: forskningssikkerhet, internasjonalt samarbeid, deltagelse i gradert forskningssamarbeid, begrensninger i forskningsagendaen og forskningsprioriteringer, åpenhet og transparens i forskningen, samt merittering og karrierebygging.

[11] For en mer presis omtale av begrepene brukt i Figur 3 viser vi til sluttrapporten.

[12] EOS-tjenestene består i dag av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets sikkerhetsavdeling (FSA).

FoU-miljøene må i større grad enn i dag klare å fange opp og håndtere forskning med skjermede elementer, og foreta vurderinger av om og i så fall hvordan slike elementer skal videreføres. Forskere, forskningsledere og forskningsadministrativt personell vil derfor trenge opplæring i hvordan forskningssikkerhet skal ivaretas, og det vil være behov for rutiner for å kunne identifisere og sikre at kun ugradert forskning deles og publiseres. Videre må det utvikles retningslinjer og rutiner for hvordan man skal sikre overgangene mellom åpen og lukket forskning slik at forskningen kan videreføres i et forsvars- og sikkerhetsperspektiv.



Figur 3. *Illustrasjon av overgangene mellom åpen, skjermet og gradert forskning.*

Mye gjenstår å operasjonalisere i tilknytning til dette, og involverte aktører vil trenge tid på å etablere ny praksis. Vi kan derfor ikke gå detaljert inn i dette nå utover å indikere at ett mulig tiltak kan være at den som søker om forskningsmidler selv aktivt flagger elementer som eventuelt kan være skjermet. Det bør også vurderes om det kan være hensiktsmessig at *alle* FoU-prosjekter finansiert av Forskningsrådet, anmodes om å redegjøre for om forskningen kan ha anvendelser innenfor forsvar eller sikkerhet.

Hovedutfordringen ligger i å veie forskningens grunnleggende verdier om åpenhet og bred deling opp mot hensynet til nasjonal sikkerhet. Selv om *ansvaret* for opplæring og utvikling av rutiner er, og må være, den enkelte institusjons ansvar, vil den enkelte vurdering i praksis måtte gjøres av forskerne selv og deres nærmeste ledere og kolleger. Det er derfor et åpenbart behov for nasjonal samordning og rutiner som legger best mulig til rette for enhetlig praksis. I dette arbeidet har NSM en sentral rolle, og det bør trekkes veksler på erfaring og praksis etablert ved Forsvarets forskningsinstitutt (FFI) og andre forskningsmiljøer som over tid har samarbeidet nært med Forsvaret og våre allierte eller andre aktører med ansvar for sikkerhet og beredskap. Andre stikkord er mer systematisk involvering av forskningsmiljøene og arbeid med eksport-kontroll knyttet til *forskning og kunnskap* i den nye etaten for Eksportkontroll og sanksjoner som blir etablert og samlokalisert med NSM fra 1. januar 2025.

Økt samarbeid må baseres på frivillighet og må tilrettelegges karrieremessig og praktisk

For å styrke Norges totale kunnskapstilfang knyttet til åpen og skjermet forskning, må forskningssystemet i stort styrke muligheten enkeltforskere og enheter ved forsknings-institusjoner har for å delta i skjermet og gradert forskning. Samtidig må slike muligheter være basert på frivillighet. Ingen bør være eller føle seg tvunget, verken av myndigheter eller egen institusjon, til å ta del i forskning der det kan legges begrensninger på åpenheten utover de begrensninger vi er vant til innenfor nåværende sivil forskning.

Å bygge nettverk, samarbeide med andre forskere og publisere forskningsresultater er avgjørende for å opparbeide seg en akademisk karriere. Når forskere deltar i skjermet eller gradert forskningssamarbeid, kan de i mindre grad enn i "åpne" forskningssamarbeid publisere i tradisjonelle kanaler. Likevel vil det være mulig for forskere som har jobbet med slik forskning å opparbeide seg en akademisk karriere, for eksempel ved at deler av ugraderte forsknings-resultater publiseres åpent. Forskere kan for eksempel gå "inn og ut" av forsvarsforskning ved å kombinere midlertidig ansettelse ved FFI med en "toer-stilling" ved en sivil forskningsinstitusjon.

Av åpenbare økonomiske grunner bør vi unngå at flere forskningsutførende institusjoner enn nødvendig godkjennes for gradert arbeid. Særlig gjelder dette på nivåer over begrenset.[13] Et helhetlig forskningssystem bør i stedet tilby arbeidssteder der sikkerhetsklarerte og autoriserte forskere kan videreføre skjermede eller graderte elementer av egen forskning. For å utnytte synergiene mellom det åpne og lukkede må et helhetlig forskningssystem legge til rette for en systematisk fleksibilitet og mobilitet slik at enkeltforskere skal kunne dele sin karriereutvikling mellom det åpne og lukkede delen av forskningssystemet, for eksempel gjennom økt bruk av bi- og delte stillinger.

For å lykkes med økt bruk av sivil forskning innenfor forsvar, sikkerhet og beredskap er det også behov for økt antall forskere som kan bidra. De siste årene har det vært en økning i rekruttering av utenlandske statsborgere til stipendiat- og forskerstillinger i institutt- og UH-sektoren. For å sikre tilgang på relevant rekruttering, særlig innenfor teknologifag, bør det settes i verk tiltak for å sikre at flere personer med norsk statsborgerskap rekrutteres til stipendiat- og forskerstillinger. Vi går ikke videre inn i dette her, men minner om at såkalte forskerlinjer innenfor særskilt "utsatte" fagfelt ved norske universiteter har vært prøvd med hell, for eksempel for å få rekruttert flere leger inn i et PhD-løp tidlig i utdannelsen. Videre har FFI fått i oppdrag å opprette et pilotprosjekt der PhD-studenter utfører pliktarbeid ved FFI, og blir sikkerhetsklarert og får opplæring i verdi- og skadevurdering.

3.2 Ny portefølje i Forskningsrådet

Det er behov for både å utnytte og styrke den sivile kompetansebasen innenfor forskning relevant for forsvar, sikkerhet og beredskap. For at forskere i det sivile systemet i større grad skal bidra til forskning som kan være relevant for forsvar- og sikkerhetsinteresser, må denne aktiviteten finansieres. En god mekanisme for å organisere deler av denne finansieringen er å etablere en ny portefølje i Norges Forskningsråd.

For å få til en raskere og sterkere synergi mellom det åpne og lukkede systemet foreslår vi å benytte Forskningsrådets rolle i forskningssystemet som finansiør og forskningspolitisk rådgiver. Det er behov for å tildele offentlige forskningsmidler på en måte som både bygger ny kunnskap og som insentiverer tettere kobling enn i dag mellom forskningsmiljøene og samfunnsaktører som anvender den nye kunnskapen.[14] Derfor anbefaler vi at det etableres en egen portefølje i Forskningsrådet for forskning relevant for forsvar, sikkerhet og beredskap. Porteføljen bør tilføres tilstrekkelige FoU-midler til å kunne skape ny kunnskap, bidra til kompetansebygging og etablere mer samspill rundt bruken av kunnskapen.

[13] Gitt det betydelige og økende presset fra utenlandsk etterretning mot norske forskningsmiljøer er det også en sikkerhetsmessig begrunnelse for å begrense antallet forskere, forskergrupper og institusjoner som godkjennes for gradert arbeid. Dette må imidlertid veies opp mot den risiko som ligger i en *for* sterk begrensning i dette antallet, noe som i sin tur vil kunne begrense kunnskapstilfanget.

[14] Se vedlagt bakgrunnsnotat om Forskningssystemet.

Vi foreslår et tredelt formål for den nye porteføljen: Den skal i) styrke den forskningsbaserte kunnskapen innenfor forsvar, sikkerhet og beredskap og ii) bidra til mer samspill enn i dag mellom forskergrupper ved forskningsinstitusjonene og relevante brukere av den nye kunnskapen. I tillegg skal porteføljen iii) bidra til å bygge opp forskningsmiljøer og kompetanse hos enkeltforskere som kan være aktuelle for senere å kunne samarbeide innenfor gradert forskning.

Porteføljen må svare på tydelige styringssignaler

Den ugraderte kompetansebyggingen i Forskningsrådets nye portefølje må rettes mot problemstillinger som vil avdekke og understøtte potensialet for anvendelser i forsvarssektoren eller i andre sammenhenger knyttet til sikkerhet og beredskap. For at denne porteføljen skal virke etter hensikten og *få effekter* av FoU-innsatsen, må det være særlig tett dialog om departementenes styringssignaler. Departementene bør derfor også gi koordinerte styringssignaler om porteføljens innretning og tematiske prioriteringer slik at porteføljestyret får nødvendige styringssignaler fra forsvarssektoren og andre aktører med ansvar for nasjonal sikkerhet. Disse aktørene må gjennom egne systemer vurdere konsekvenser og muligheter samt identifisere flerbruksmuligheter.

Sammen med rammeverket for eksportkontroll vil forsvarssektorens arbeid gi grunnlag for å vurdere skjermingsbehov og gradering. Det skal også legges til rette for sivile innovasjoner knyttet til samfunnssikkerhet og flerbruk.

Porteføljestyring for kompetansebygging, samspill og for å ta kunnskapen i bruk

En portefølje i Forskningsrådet er en samling prosjekter avgrenset av nærmere definerte kriterier og tematikk som er redegjort for i en porteføljeplan og i utlysningene av midler. Slike kriterier må tilpasses særegenheten til porteføljen. Det overordnede ansvaret for porteføljen ligger i eget styre, kalt porteføljestyret. Dette styret har ikke bare det overordnede ansvaret for porteføljens egne midler, men skal også se disse i sammenheng med prosjekter i norske forskningsmiljøer med relevans for den aktuelle porteføljen finansiert gjennom Forskningsrådets øvrige porteføljer eller av EU. I tillegg bør den nye porteføljen inkludere NATOs ugraderte forskning i analysen av Forskningsrådets nye portefølje.

Porteføljestyret innretter virkemidlene etter hvilke strategiske behov de ser for samarbeid med næringslivet, offentlig sektor, relevante forskningstema, behov for grunnforskning, anvendt forskning, forskning og innovasjon. Dette er satt i system ved at Forskningsrådet merker alle prosjekter ut ifra hvilke fag og tema de er relevante for og etablerer fortløpende statistikk. Analyse av finansiert forskning opp mot identifiserte behov og eventuelt samspill i forskningssystemet, gir porteføljestyret grunnlag for å lyse ut midler på områder der behovene er størst, og med virkemidler som gir de beste resultatene. Analysene ligger også til grunn for Forskningsrådets årlige rådgivning og FoU-budsjettinnspill til departementene.

Forskningsrådets porteføljestyring innebærer at den nye porteføljen rettet mot forsvar, sikkerhet og beredskap også vil omfatte prosjekter med relevant tematikk i andre av Forskningsrådets porteføljer. Porteføljestyret skal dermed gi råd om innhold og innretning i Forskningsrådets samlede portefølje relevant for forsvar, sikkerhet og beredskap. Porteføljen vil omfatte både åpne og skjermede prosjekter, og i noen utstrekning også graderte, og vil utgjøre et viktig kunnskapsgrunnlag for porteføljestyrets prioriteringer.

I oppdraget er det understreket at samordningen av sivil og militær forskning ikke må komme i veien for den åpne forskningen. Vi foreslår derfor at utlysninger, søknadsbehandling, tildeling

og prosjektoppfølging i den nye porteføljen *som hovedregel* skal innrettes ugradert (men ikke utelukkende, se nedenfor). Følgelig vil Forskningsrådets nye portefølje kun i begrenset grad gjøre det nødvendig å utvikle Forskningsrådet for gradert arbeid. Forskning og løsninger som viser seg for eksempel å kunne ha stort militært potensial skal i stedet inviteres inn til gradert forskning og innovasjonsarbeid i forsvarssektoren og med allierte. Det aller meste som foregår av forskning i Norge vil derfor være uberørt av samordningen.

Forskningsmiljøene må likevel være forberedt på systematisk å kunne identifisere flerbruks-muligheter og skjermede elementer i forskningen, og behandle dette i henhold til sikkerhets-loven. Likeledes må de være forberedt på at det vil være begrensinger knyttet til deling og offentliggjøring av eventuelle skjermede elementer.

Den nye porteføljen skal ikke bare styrke forskningsbasert kunnskap, men også bidra til mer samspill og til at *kunnskapen tas i bruk*. Forskningsrådet har muligheten til å sette sammen ulike finansieringsordninger som fanger dette opp ved å stille krav om samarbeid mellom relevante aktører fra ulike deler av forskningssystemet og brukere av kunnskap. For eksempel kan det stilles krav om kjøp av FoU-oppdrag fra forskningsinstitusjoner ved tildeling av FoU-midler til offentlige aktører med ansvar innenfor nasjonal sikkerhet, eller private bedrifter som tilbyr løsninger relevante for forsvar, sikkerhet og beredskap på kommersiell basis.[15] I slike sammenhenger kan det bli aktuelt at søknader kan inneholde gradert informasjon, og at søknadsprosessen (i alle ledd) må ta høyde for dette.

En annen mulighet er at Forskningsrådet i en utlysning stiller krav om at (minst) én av aktørene i et samarbeidsprosjekt skal kunne håndtere gradert informasjon, og på den måten bidra til økt utnyttelse av flerbruksmuligheter og til at flere forskere og miljøer får kompetanse om hva som kreves for å kunne arbeide med graderte problemstillinger. Porteføljestyrets utlysninger vil dermed kunne insentivere ønsket samspill og nye koblinger i et helhetlig forskningssystem som håndterer åpen og skjermet, men også gradert, kunnskap.

Porteføljen vil også gi en mulighet til å kartlegge, identifisere, bygge opp og koordinere aktører for samarbeid i NATO og EU gjennom forsvarssektoren. Det mest aktuelle er forsknings- og innovasjonssamarbeid i NATO Science and Technology Organization, European Defence Agency, Det europeiske forsvarsfondet og NATO DIANA.[16]

Kompetent og sikkerhetsklarert porteføljestyre og -administrasjon

Porteføljestyret må kunne ta del i kommunikasjonen om spesifikke utfordringer med myndigheter ansvarlige for den nasjonale sikkerheten. Dette for å sikre at kunnskapshull og prioriteringer knyttet til dette blir godt ivaretatt og at sikkerhetspolitiske signaler fra departementene blir forstått og bygget inn i porteføljens utlysninger. Porteføljestyret bør ha faglig kompetanse til å kunne vurdere og evaluere utviklingen i prosjektene i porteføljen og behovet for skjerming. Porteføljestyret må bidra til identifiseringen av forskning som bør skjermes eller graderes og vurdere hvordan slike elementer tas videre i tett samarbeid med aktører med ansvar for forsvar, sikkerhet og beredskap. Vi anbefaler derfor at porteføljestyrets medlemmer er sikkerhetsklarerte. Videre bør noen av styremedlemmene nomineres av departementer med særskilt ansvar for vår nasjonale sikkerhet, og som bidrar finansielt til den nye porteføljen.

[15] Slikt samspill er omtalt i noe større detalj i vedlagt bakgrunnsnotat om forskningssystemet.
[16] NATO Science & Technology Organization, European Defence Agency (europa.eu), Det europeiske forskningsfondet, DIANA – Forsvarsfondet.

Forskningsrådet må utvikle et internt støtte- og rådgivningssystem for å finne og vurdere prosjekter med sikkerhetsgraderte og skjermede elementer. Det trengs generelle mekanismer og veiledning som kan hjelpe søkere i å vurdere om forskningen bør skjermes, og dette vil gjelde bredere enn prosjekter finansiert innenfor den nye porteføljen. Utvalgte medarbeidere i Forskningsrådets porteføljeadministrasjon må derfor sikkerhetsklareres for å kunne håndtere søknader og prosjekter med skjermingsverdige elementer.

3.3 Arena for kunnskapssamarbeid innenfor forsvar, sikkerhet og beredskap

Flere utredninger fra de senere årene er tydelige på at arbeidet med totalforsvar og samfunnets motstandskraft bør styrkes.[17] Det pekes på betydelige hull både i kartleggingen av behovene og i den nasjonale kompetansebasen for å bedre nasjonal sikkerhet og beredskap, og det etterlyses et løft i hver sektor og en målrettet helhetlig tilnærming på tvers av sektorer. Det er behov for å identifisere, prioritere og utvikle nødvendig kompetanse og å utvikle helhetlige løsninger for tverrsektorielle problemstillinger. Det er også et kritisk tidsperspektiv knyttet til den sikkerhetspolitiske utviklingen som tilsier at et løft bør skje raskt.

Hvert departement har et ansvar for sikkerhet og beredskap innenfor egen sektor. Det sivile samfunnet og Forsvaret samarbeider og er gjensidig avhengige i krise og krig. Forsvarets evner vil fort reduseres ved manglende støtte fra det øvrige samfunnet. Samfunnets motstandskraft og utholdenhet er vesentlig for nasjonal sikkerhet. Det militære forsvaret og den sivile beredskapen betegner vi totalforsvaret. Vertslandsstøtte fra allierte forsterkninger inngår også i hva samfunnet må understøtte. Dette er en tverrsektoriell utfordring.

Logikken bak sammensatte trusler er ofte å utnytte manglende modenhet i sektorene, spesielt hva angår koordineringsutfordringer mellom sektorer. Sammensatte trusler kan bli mer alvorlige fremover og sabotasje og terror er utfordringer som kan treffe mange sektorer.

Disse utfordringene er også omtalt i den nylig fremlagte langtidsplanen for forsvarssektoren.[18] Planen forslår bl.a. etablering av en "arena på tvers av militær og sivil sektor som bidrar til at relevante aktører kan koordinere og utvikle sitt kunnskapssamarbeid relatert til totalforsvaret […] med tilrettelagt digital og fysisk infrastruktur tilpasset åpen, skjermet og gradert kunnskaps-samarbeid".[19] Vi vil her ikke gå inn i hvordan en slik arena bør operasjonaliseres, utover å nevne at sentrale kunnskapsmiljøer som NSM og FFI, bør kunne spille viktige roller, både i arenaen som sådan, men også i hvordan den bør organiseres. Arenaen må basere sitt arbeid på forskningsbasert kunnskap, og vi mener den vil ha en viktig funksjon for å få til et helhetlig forskningssystem.

Arenaens rådgivingsfunksjon

Arenaens ovenfor omtalte koordineringsfunksjonen bør inkludere *rådgivning om kunnskaps-behovet og kunnskapsberedskap til departementene,* ikke minst knyttet til sammensatte, og derfor oftest tverrsektorielle, trusler og samfunnets motstandskraft og utholdenhet. Rådene kan dreie seg om hvordan departementene og deres underliggende organer selv involverer seg

[17] Forsvarskommisjonen, Totalberedskapskommisjonen - regjeringen.no.
[18] Langtidsplanen for forsvarssektoren (2025-2036) peker på at forsvarssektorens forskningssystem skal videreutvikles blant annet gjennom å innføre porteføljestyring og ved at flere aktører skal kunne bidra på sektorens graderte arenaer. Prosjektet Forsvarssektoren 2024 (F24) skal bl.a. gjennomgå roller, ansvar og myndighet for sektorens FoU-behov. Det er naturlig at den videre utviklingen av forsvarssektorens forskningssystem gjøres som en del av F24.
[19] Langtidsplanen for forsvarssektoren (2025-2036), side 128.

i kunnskapsoppbygging, både gjennom oppdragsforskning og ved å bidra til å finansiere Forskningsrådets nye portefølje.

Departementenes innhenting av kunnskap bør baseres på en gjennomtenkt bruk av styring, tilskudd og tildeling av oppdrag til kunnskapsmiljøer, samt finansiering gjennom Forskningsrådet, slik at mulighetene ulike typer kunnskapsaktører representerer, blir best mulig utnyttet.[20] Vi minner i denne sammenhengen om at Forskningsrådets utlysninger (beskrevet i avsnitt 3.2) ikke bare vil kunne rette seg mot oppbygging av ny kunnskap i forsknings-institusjonene, men også mot brukere av FoU som i sin tur kjøper oppdrag eller samarbeider på annet vis med forskningsinstitusjonene.

Rådgivningsfunksjonen må ta utgangspunkt i behovet for å ta kunnskap i bruk for å styrke den nasjonale sikkerheten. Den vil dermed ha et annet utgangspunkt enn de råd Forskningsrådets nye porteføljestyre vil gi. Sistnevnte styre vil primært være opptatt av hvordan vi mest effektivt kan bygge nødvendig forskningsbasert kunnskap. Samtidig er det viktig at rådgivningen gitt fra arenaen er godt samkjørt med den gitt av Forskningsrådet ved sitt nye porteføljestyre (jf. stiplet pil i figur 2).

Arenaens mottakerrolle

Kunnskapen aktørene produserer må brukes i sektorene, og løsninger må utvikles for å faktisk *realisere* en styrking av nasjonal sikkerhet. Et kjennetegn ved forsvarssektorens forsknings-system er et brukernært samspill for å målrette forskningen mot behov og omsette forskningen til effekt i sektoren. Også næringslivet er viktig for evnen til å realisere slike effekter, og en satsing på utvikling av relevant forsvarsindustri er en del av dette.[21] I et helhetlig forskningssystem vil Innovasjon Norge og virkemidler for bedriftsetablering og skalering bli enda viktigere.

Overordnet sett kan man si at forsvarssektorens mottaksapparat for forskning med flerbruks-muligheter fyller to funksjoner. Den ene er å bistå kunnskapsmiljøene i å identifisere og sortere hva flerbruksmulighetene består i, og hvordan de eventuelt kan tas videre. Den andre består i å forholde seg til kunnskap som enten er viktig å verne eller som i seg selv kan true vår nasjonale sikkerhet. FFI har i stort denne funksjonen i forsvarssektoren i dag og utvikler samarbeids-nettverk nasjonalt og internasjonalt, vurderer samarbeidspotensial opp mot nasjonale interesser og inngår i stor grad i samarbeidene.

En slik *mottakerrolle* er i dag ikke etablert i samme grad innenfor øvrige deler av arbeidet med sikkerhet og beredskap som den er i forsvarssektoren. I en del sammenhenger vil det være nødvendig for at ny kunnskap skal kunne komme til anvendelse og nytte og dermed gi varig effekt for nasjonal sikkerhet. Det er med andre ord viktig å ha strukturer som kobler aktører med ansvar for forsvar, sikkerhet og beredskap med kunnskapsaktørene slik at forskning igangsatt på åpent nivå blir videreført i regi av dertil egnet nasjonal myndighet, eventuelt med graderte elementer. Det vil blant annet være nødvendig å følge opp og videreføre resultater fra forskningen i Forskningsrådets portefølje for forsvar, sikkerhet og beredskap.

Kontaktpunkt for sentrale aktører og sikkerhetsgodkjent infrastruktur

[20] Jf. det sjette elementet i Veileder for sektoransvaret: "Departementene skal være bevisst på hvilken kanal som velges for forskningsfinansiering".

[21] Også Forskningsrådet og Innovasjon Norge samarbeider om å dekke behovene i hele verdikjeden både nasjonalt og internasjonalt.

Arenaen bør også tjene som *kontaktpunkt for sentrale aktører fra forsvarssektoren, EOS-tjenestene og FoU-sektoren*. Aktører med roller innenfor forsvar, sikkerhet og beredskap må ha møteplasser for læring og samordning. Forskning finansiert gjennom Forskningsrådet må sees i sammenheng med forskning finansiert av andre aktører, for eksempel oppdragsforskning finansiert av statlige organer med beredskapsansvar, forskning finansiert over universitetenes grunnbudsjett og forskning i næringslivet. Involverte aktører har et selvstendig ansvar for å se koblingene, men like fullt et behov for å dele kunnskap, også den graderte, på en trygg måte.

Den fjerde funksjonen vi her løfter frem er en følge av at flere forskere og forskergrupper skal kunne arbeide med gradert informasjon. Norge har tunge kunnskapsmiljøer fra nord til sør. Det fordrer *tilgang til sikkerhetsgodkjent infrastruktur* på litt flere steder i landet enn i dag. Særlig viktig er dette dersom graderingen er på et nivå høyere enn begrenset.

Vi mener det er naturlig at de fire funksjonene beskrevet ovenfor ligger utenfor Forskningsrådet. Ikke minst bidrar det til at øvrig åpen forskning i liten grad berøres av økt satsing på samarbeid innenfor gradert forskning.

3.4 Styrket tverrdepartemental koordinering av forsvar, sikkerhet og beredskap

Forsvar, sikkerhet og beredskap er et tverrsektorielt felt som krever at man lykkes med å se utfordringer, løsninger og behov for prioriteringer samlet. Totalberedskapskommisjonen og Forsvarskommisjonen peker også på disse tverrsektorielle utfordringene. Et effektivt og velfungerende helhetlig forskningssystem, som initierer, koordinerer og finansierer FoU relevant for sektorovergripende problemstillinger, krever styring også på overordnet politisk nivå. For å lykkes med regjeringens forskningspolitiske ambisjoner om et helhetlig forskningssystem som dekker Norges totale kunnskapsbehov, finner vi det derfor riktige å understreke betydningen av økt og tettere samarbeid på tvers av departementer, både i budsjettsammenheng og i design og implementering av slike tverrgående satsinger.[22]

Vi går ikke mer inn i denne problemstillingen, utover å slå fast at vi foreslår som et eget tiltak å styrke den tverrdepartementale koordineringen av forsvar, sikkerhet og beredskap. Tiltaket knytter an til utfordringene vi omtalte innledningsvis til avsnitt 3.3. Videre er det viktig at de som skal forta slik koordinering også har den nødvendige autoriteten til å gjennomføre samordningen.

[22] Det er Justis- og beredskapsdepartementet som har ansvar for koordinering av nasjonal sikkerhet på tvers av departementer. Ansvaret for den tverrsektorielle koordineringen innenfor forskning ligger i Kunnskapsdepartementet.

Vedlegg B: Vurdering av fag- og teknologiområder

Notatet drøfter følgende spørsmål fra oppdragsbrevet: Innenfor hvilke fag- og teknologi-områder er behovet for samarbeid størst i dag, og hvilke områder antas å utvikle seg til å bli viktige samarbeidsarenaer de kommende årene?

1. Innledning

For å besvare oppdragets spørsmål om på hvilke områder det er størst behov for samarbeid, i dag og fremover, må det gjøres konkrete og omfattende vurderinger. Vurderingene må ta utgangspunkt i identifiserte kunnskaps- og teknologibehov for å ivareta forsvar, sikkerhet og beredskap, sett opp mot status på mange ulike fag- og teknologiområder.

Det foreligger en rekke ulike vurderinger av hvilke fag- og teknologiområder som er viktige for nasjonal sikkerhet og forsvarssektoren, og mange av disse oppdateres jevnlig. Internasjonalt har EU, NATO og flere enkeltland, som USA, har laget lister over forsknings- og teknologi-områder som vurderes å være viktige. Nasjonalt gjør også en rekke aktører vurderinger av slike områder. Siste del av notatet gir en oversikt over utvalgte vurderinger og lister.

Identifiserte fag- og teknologiområder som vurderes som viktige for egen sikkerhet og forsvars-evne, er dermed også av interesse for trusselaktører. Dette betyr at det er behov for å vurdere skjerming av deler av forskningen innenfor disse områdene for å sikre at trusselaktører ikke får tilgang, ref. eksportkontrollforskriften og forskningssikkerhet.

I en norsk sammenheng har både Forsvarskommisjonen og Totalberedskapskommisjonen pekt på behovet for økt tverrsektorielt samarbeid og anbefaler at det etableres ytterligere mekanismer for å utvikle og ivareta relevant kunnskap på tvers av samfunnsområder, skjermingsbehov og gradering. Den nye langtidsplanen for forsvarssektoren lister opp grunnleggende kunnskapsbehov i forsvarsektoren, og omtaler prioriteringer innenfor forskning og utvikling. I planen foreslår regjeringen fire konkrete FoU-satsinger som understøtter prioriteringene og optimaliserer Norges forsvarsevne, samtidig som mulighetene innenfor sivilt-militært og offentlig-privat samarbeid utnyttes. Regjeringen har bestemt at det i 2024 skal legges frem en stortingsmelding om totalberedskap, som også vil inneholde analyser og tiltak for arbeidet med motstandskraft og totalforsvar.

2. Behov for løpende vurderinger

Innenfor rammen av arbeidet med dette oppdraget har det ikke vært rom for å gjøre nye og selvstendige vurderinger av fag- og teknologiområder. Både behov for kunnskap og teknologi rettet inn mot nasjonal sikkerhet, og relevante fag- og teknologiområder er i dynamisk utvikling. Derfor er det viktig å ha funksjoner og løsninger som kan gjøre løpende vurderinger av viktige fag- og teknologiområder, sett opp mot identifiserte behov, og hvordan FoU-satsinger best kan innrettes for å møte behovene.

Løsninger for dette er beskrevet i hovedrapporten og i vedlegg A. Den anbefalte nye porteføljen i Forskningsrådet for forskning for forsvar, sikkerhet og beredskap må bygge på vurderinger av behov for ny kunnskap og økt samarbeid innenfor relevante fag- og teknologiområder. Tilsvarende må også den anbefalte nye arenaen for kunnskapssamarbeid innenfor forsvar, sikkerhet og beredskap ha som oppgave å kartlegge sammenhengen mellom FoU-behov og status på relevante fag- og teknologiområder som grunnlag for å gi råd til myndighetene om nye FoU-satsinger.

3. Grunnlag for vurderingene

I det videre arbeidet med å etablere løsninger som muliggjør åpent-skjermingsverdig, ugradert-gradert og sivil-militært FoU-samarbeid i større skala enn i dag bør det tas utgangspunkt i identifiserte kunnskapsbehov og FoU-prioriteringer i langtidsplanen for forsvarssektoren, og i den kommende stortingsmeldingen om totalberedskap.

I etableringen og utviklingen av de fire konkrete FoU-satsingene som omtales i langtids-planen for forsvarssektoren er det viktig å gjøre en vurdering av kunnskaps- og teknologi-status på relevante områder og behov for samarbeid, for å innrette satsingene på en måte som best møter identifiserte behov. De fire FoU-satsingene er:

- Brobyggende kunnskapsutvikling på tvers av forsvar, sikkerhet og beredskap
- Et datadrevet forsvar
- Banebrytende teknologier
- Klimaomstilling, gjenbruk og ombruk

Innenfor identifiserte kunnskapsbehov og FoU-prioriteringer bør det gjøres vurderinger av fag- og teknologistatus, og også vurderinger av hvordan disse best kan møtes med økt samarbeid. Det er også behov for å gjøre prioriteringer av på hvilke områder det skal settes inn tiltak for å øke samarbeidet. Det må også vurderes hvilken type samarbeid som best kan understøtte behovene. Dette kan være behov for tverrsektorielt, sivilt-militært og offentlig-privat samarbeid.

4. Foreliggende vurderinger av og lister over forsknings-, fag- og teknologiområder som er viktige for sikkerhet og forsvarssektoren

Det finnes allerede en rekke ulike vurderinger av hvilke fag- og teknologiområder som er viktige for nasjonal sikkerhet og forsvarssektoren, og som trekkes frem i ulike sikkerhets- og trussel-vurderinger. Disse vurderingene viser at det er mange og brede fag- og teknologiområder som vurderes å være viktige.

Sist i dette notatet er det samlet slike vurderinger fra:

- Langtidsplan for forsvarssektoren 2025–2036
- Nasjonal trusselvurdering 2024
- Langtidsplanen for forskning og høyere utdanning
- Eksportkontroll i kunnskapssektoren
- Sikkerhetsfaglig råd
- Risiko 2024
- Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologiske og fremtidsrettet forsvar, Meld. St. 17 (2020–2021)
- EUs critical technology areas for the EU's economic security
- NATOs prioriterte forsknings- og teknologiområder
- Det hvite hus' National Science and Technology Council

Utvalgte vurderinger av, og lister, over forsknings-, fag- og teknologiområder som er viktige for sikkerhet og forsvarssektoren

Langtidsplan for forsvarssektoren 2025–2036

Følgende er hentet fra Langtidsplan for forsvarssektoren 2025–2036[1]:

Forsvarsektorens grunnleggende kunnskapsbehov

Langtidsplanen lister opp følgende grunnleggende kunnskapsbehov i forsvarsektoren:

- *Banebrytende kunnskapsutvikling* som utforsker teknologiske muligheter, nye operative evner, og nye konsepter som kan realisere operativ evne.
- *Langsiktig kunnskaps-, teknologi og kapabilitetsutvikling* knyttet til nisjekapasiteter som missil, sensor- og undervannsteknologi, utvikling av banebrytende teknologier som kunstig intelligens og kvanteteknologi, kapabilitetsanalyser, klima- og miljøregnskap, nordområdekunnskap, forskningsunderstøttet utvikling i hele materiellets levetid, konsekvenser for anvendelse og bruk av ny teknologi, og innovasjonspotensiale for nye teknologier.
- *Realisering av vedtatt politikk* knyttet til blant annet prioriterte materiellinvesteringer, analyser av trekantsamarbeid og industristøtte, personellordninger, og status i gjennomføring.
- *Situasjonsforståelse* til bruk i beslutningsunderlag slik som teknologiske trender, sentrale utviklingstrekk av betydning for sikkerhet og forsvarsevne, sikkerhetspolitiske analyser, demografiske og kompetanse analyser, nasjonal kapasitet på utvalgte forskningsområder, industriaktørers FoU-innsats og anvendelse av kunnskap.
- *Kunnskapsbaserte grunnlag for utvikling av ny politikk* og fastsettelse av mål slik som forskningsbaserte råd, analyser, metastudier, kunnskapsgjennomganger, tematiske kunnskapsgrunnlag og analyser av kapabilitetsgap.

Prioriteringer og satsinger innenfor forskning og utvikling

Langtidsplanen omtaler følgende prioriteringer innenfor forskning og utvikling:

Norge skal lede og delta i multidomeneoperasjoner og være fremst blant allierte på situasjonsforståelse i nord:

- Regjeringen prioriterer FoU-aktiviteter som integrerer og bygger bro mellom domenene, mellom sivil og militær sektor, utvikler evnen til situasjonsforståelse og utnytter data som ressurs for operative formål. Samtidig er det også nødvendig med kunnskaps-utvikling som integrerer teknologi, mennesker og organisasjon slik at overgangen til multidomeneoperasjoner kan skje gradvis.
- FoU-behovene knytter seg til å utvikle helhetlige og rettidige analyser og beslutnings-støtte fra stridsteknisk til strategisk nivå. Dette innebærer blant annet rombasert informasjonsinnhenting, teknologi for undervannsovervåking og informasjonsinnhenting fra sensorsystemer og ubemannede og autonome systemer. Videre innebærer det å utvikle hvordan informasjonen skal sammenstilles og presenteres for relevant personell på ulike nivåer.

[1] https://www.regjeringen.no/no/dokumenter/prop.-87-s-20232024/id3032217/

- Regjeringen prioriterer FoU-aktiviteter som gjør Norge forberedt på økt gjennomføring av operasjoner i et kaldværsklima, i nord.

Norge skal utvikle fremtidige operative evner gjennom teknologisk fornyelse:

- Regjeringen prioriterer FoU-aktiviteter som utvikler fremtidige operative evner gjennom teknologisk fornyelse.
- Det skal legges særlig vekt på FoU som bidrar til å forsterke operative konsepter og store våpenplattformer. Samtidig skal det gis prioritet til FoU og teknologisk fornyelse som bidrar til økt evne til målbekjempelse med lavere kostnad. Teknologiske områder som autonomi og ubemannede plattformer, kombinert med banebrytende teknologier som kunstig intelligens, er eksempler på områder der FoU-aktiviteter kan bidra til å gi Norge økt operativ effekt både på kortere og lengre sikt.
- Regjeringen vil legge til rette for fire konkrete FoU-satsinger som understøtter prioriteringene og optimaliserer Norges forsvarsevne, samtidig som mulighetene innenfor sivilt-militært og offentlig-privat samarbeid utnyttes.
    - Brobyggende kunnskapsutvikling på tvers av forsvar, sikkerhet og beredskap
        - Regjeringen vil særlig prioritere kunnskapsutvikling om sammensatte trusler, nasjonale sårbarheter, og se sivil motstandskraft i sammenheng med Forsvarets operative evne. Temaets sektorovergripende natur gjør det spesielt viktig å utnytte mulighetene som ligger i tett sivilt-militært samarbeid.
    - Et datadrevet forsvar
        - Regjeringen vil utnytte potensialet i de store datamengdene som produseres til å videreutvikle forsvarssektoren og utvikle forsvarsevnen.
        - Regjeringens satsing på et datadrevet forsvar har høy prioritet og vil detaljeres videre i samarbeid med Forsvaret og relevante aktører.
    - Banebrytende teknologier
        - Regjeringen vil satse på forskning og utvikling innenfor banebrytende teknologier som kvanteteknologi og kunstig intelligens for å bidra til å bygge nasjonal kompetanse og kapasitet. Satsingen innebærer forskning og utvikling knyttet til teknologiene i seg selv, men også forskning som belyser konsekvenser og muligheter teknologiene gir for norsk forsvar og sikkerhet. Satsingen vil styrke viktig kompetanse og bedre forutsetningene for raskere utnyttelse av ny teknologi i Forsvaret, næringslivet og industrien.
    - Klimaomstilling, gjenbruk og ombruk
        - Regjeringen vil satse på forskning og utvikling knyttet til klimaomstilling og klimatilpasning.

Samarbeid for sikkerhet - Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar, Meld. St. 17 (2020–2021)

Regjeringen Solberg la fram stortingsmeldingen Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologiske og fremtidsrettet forsvar[2]. Strategiens mål er å videreføre og styrke en internasjonalt konkurransedyktig norsk forsvarsindustri, med evne til å utvikle, produsere og understøtte forsvarsmateriell, systemer og tjenester innenfor prioriterte

[2] https://www.regjeringen.no/no/dokumenter/meld.-st.-17-20202021/id2838138/

teknologi- og kompetanseområder som er viktige for å ivareta nasjonale sikkerhetsinteresser og Forsvarets behov. Følgende åtte teknologiske kompetanseområder legges til grunn for samarbeidet mellom forsvarssektoren og forsvarsindustrien:

- Kommando-, kontroll-, informasjons-, kommunikasjons- og kampledelsessystemer
- Systemintegrasjon
- Autonome systemer og kunstig intelligens
- Missilteknologi
- Undervannsteknologi
- Ammunisjon, rakettmotorer og militært sprengstoff
- Materialteknologi spesielt utviklet eller bearbeidet for militære formål
- Levetidsstøtte for militære systemer

Nasjonal trusselvurdering 2024, om fag- og teknologiområder

Følgende er hentet fra PSTs nasjonale trusselvurdering 2024[3]:

Akademiske institusjoner vil være utsatt for ulovlig kunnskapsoverføring

PST forventer at norsk forsknings- og utviklingssektor vil bli utsatt for forsøk på ulovlig kunnskapsoverføring i 2024. Overføring av kunnskap som kan sette stater i stand til å utvikle militær kapasitet, er like strengt regulert som fysiske varer.

Eksempler på forskningsfelt av særlig interesse for fremmede stater:

- Nanoteknologi
- Metallurgi
- Kryptografi
- Robotikk og autonomi
- Kjemi
- Mikroelektroniske systemer
- Akustikk
- Kjernefysikk og cybersikkerhet

Norge har flere ledende teknologiske fagmiljøer som flere fremmede stater ønsker å innhente kompetanse fra. Forskere og studenter fra stater vi mener utgjør en trussel, kan tilegne seg teknologikompetanse og benytte utstyr som er omfattet av sanksjoner og eksportkontroll under opphold i Norge. Eksempelvis har den kinesiske partistaten talentprogrammer og forskningsparker hvor de utnytter utenlandske forskeres kompetanse til å styrke egen militær kapasitet. *Institusjoner og virksomheter som driver forskning og utvikling, har derfor et særlig ansvar for å vurdere egen teknologis potensielle militære anvendelse.*

Langtidsplan for forskning og høyere utdanning 2023–2032

I langtidsplanen for forskning og høyere utdanning[4] er det definert et sett med brede tematiske prioriteringer:

[3] https://www.pst.no/alle-artikler/artikler/ntv-2024/
[4] https://www.regjeringen.no/no/tema/forskning/innsiktsartikler/langtidsplanen-for-forskning-og-hoyere-utdanning-2023-2032/id2929453/

- hav og kyst
- helse
- klima, miljø og energi
- muliggjørende og industrielle teknologier
- samfunnssikkerhet og beredskap
- tillit og fellesskap

Innenfor prioriteringen samfunnssikkerhet og beredskap er følgende trukket fram som hovedutfordringer og kunnskapsbehov:

- Globale helsetrusler
- Matsikkerhet, drikkevann og forsyningsrisiko
- Energiforsyningssikkerhet
- Alvorlige naturhendelser
- Atomsikkerhet og atomberedskap
- Sikkerhetspolitiske endringer og ansvarlig internasjonalt kunnskapssamarbeid
- Teknologi og samfunnssikkerhet
- Kunnskap i kriser

Og følgende prioriteringer trekkes frem under tiltak og oppfølging. Regjeringen vil særlig prioritere følgende områder innenfor forskning og forskningsdrevet innovasjon:

- effekten av smitteverntiltak og antibiotikaresistens
- internasjonalt forskningssamarbeid om klimasmart landbruk og global matsikkerhet
- utvikling av modeller og analyseverktøy for forsyningssikkerhet for energi, gjensidige avhengigheter og handelssystemer i en global, digital økonomi og samfunnsutvikling
- styrking av den norske forskningskapasiteten med hensyn til geopolitisk dynamikk, særlig i forbindelse med politiske, sikkerhetspolitiske og økonomiske endringer globalt
- konsekvenser av den sikkerhetspolitiske utviklingen og endringer i trusselbildet for den nasjonale sikkerheten i Norge
- effektiv bekjempelse av kriminalitet på internett og ulike former for påvirkning og desinformasjon
- styrking av synergier i teknologiutnyttelse og forbedring av evnen til å håndtere komplekse redningsoperasjoner og møte nye og sammensatte trusler
- legge til rette for forskning for dekommisjonering av norske atomanlegg

Eksportkontroll i kunnskapssektoren

Råd for samfunnssikkerhet og beredskap (Beredskapsrådet) skal gi støtte til virksomheter i kunnskapssektorens arbeid med sikkerhet og beredskap. En viktig oppgave for rådet er å legge til rette for en felles praksis i sektoren, og bidra til erfaringsdeling. Hovedmålet er at utdanningsinstitusjonene i Norge opparbeider seg nok kunnskap om sikkerhet og beredskap, slik at de selv kan jobbe med å gjøre universiteter og høyskoler trygge, både for studenter og ansatte.

Beredskapsrådet har laget et notat[5] med en kort innføring i norsk eksportkontroll og hvilken betydning regelverket har for kunnskapssektoren. Sensitive kunnskaps- og flerbruksvarer er ofte tilknyttet utstyr, materialer og teknologi som gjerne er å finne i ulike typer laboratorier.

[5] https://www.uis.no/nb/samarbeid/eksportkontroll-i-kunnskapssektoren

Det er ifølge UD innenfor disse nevnte fagområdene at den sensitive kunnskapen og teknologien helst er å finne:

- Biovitenskap, inkludert bioteknologi
- Maskinteknikk
- Biokjemi
- Materialteknologi
- Kjemi, herunder kjemisk prosessteknologi
- Kybernetikk
- Fysikk, inkludert nukleærfysikk
- Medisin/veterinærfag
- Luftfart og luftfartsteknologi
- Matematikk

Sikkerhetsfaglig råd, NSM

Følgende er hentet fra NSMs sikkerhetsfaglige råd fra 2023[6]:

NSM skriver at i sikkerhetsfaglig råd er utgangspunktet at fremmede staters og trusselaktørers bruk av teknologi kan komme til å utvikle seg raskere enn åpne demokratiers evne til å beskytte seg. Autoritære regimer vil kunne utnytte informasjonsteknologi på måter som rammer demokratier med åpne informasjonsmiljøer hardest.

Det foregår en geopolitisk konkurranse om teknologisk herredømme. Nye teknologier kan i økende grad – og uten særlig forvarsel – tas i bruk av en rekke land. Teknologiutviklingen gir ofte banebrytende og verdiskapende muligheter. Her ligger samtidig kimen til nye sårbarheter og trusler. Utfordringene handler om infrastrukturen teknologien er helt avhengig av, dataene teknologien baserer seg på, og delvis også om selve anvendelsen av teknologien.

Én og samme teknologi kan ha både sivil og militær anvendelse, såkalt «flerbruksteknologi». Det fører til at det ikke kun er vitenskapelige og kommersielle interesser som driver utviklingen, men også autoritære stater med geopolitiske ambisjoner. Disse kan bruke teknologien til å øke egen militær kapasitet. Spredning av avansert teknologi kan også gjøre den lettere tilgjengelig for ikke-statlige trusselaktører.

Fremvoksende teknologi er en viktig driver for utviklingen av Forsvarets operative kapasiteter. Teknologiutvikling er helt nødvendig for at Forsvaret fortsatt skal være relevant i et moderne og høyteknologisk stridsmiljø. Kommersialiseringen betyr også at skillet mellom militær og sivil teknologi blir stadig mindre. Forsvarets avhengighet av teknologiene og kommersielle aktører introduserer nye verdier og verdikjeder utenfor den tradisjonelle forsvarsindustrien.

Følgende sikkerhetsutfordringer knyttet til fremvoksende teknologier trekkes frem:

- Innsamlet data for andre formål kan utnyttes og true nasjonal sikkerhet
- Digitalisering gir trusselaktører flere angrepsflater
- Utvikling av kvanteteknologi påvirker sikkerhetsløsningene
- Trusselaktører bruker bioteknologiutvikling til militære formål
- Kunstig intelligens har stor sikkerhetsmessig innvirkning
- Virkeligheten blir manipulert

[6] https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglig-rad-et-motstandsdyktig-norge

- Droner og autonome våpensystemer truer befolkning og infrastruktur gjennom hele krisespekteret
- Mangel på sjeldne metaller og digitale komponenter medfører sikkerhetstruende avhengigheter

Risiko 2024, NSM

NSMs rapport «Risiko» er én av tre offentlige trussel- og risikovurderinger som utgis hvert år. Risiko 2024 beskriver hvordan trusselaktører kan utnytte sårbarheter hos virksomheter og i samfunnet, og hvilken risiko dette medfører. I rapporten peker NSM på hvordan myndigheter og virksomheter bør redusere sårbarheter for å gjøre trusselaktørenes jobb vanskeligere. Følgende er hentet fra NSMs rapport Risiko 2024[7]:

Land som Kina og Russland ønsker å endre dagens verdensorden. Det er fare for at fremmede staters og trusselaktørers bruk av teknologi kan utvikle seg raskere enn åpne demokratiers evne til å beskytte seg. Autoritære regimer vil kunne utnytte informasjonsteknologi på måter som rammer demokratier med åpne informasjonsmiljøer hardest, som for eksempel Norge.

Privat næringsliv har fått større betydning for nasjonal sikkerhet i lys av sikkerhetspolitiske og teknologiske utviklingstrekk. Derfor belyser Risiko 2024 spesielt situasjonsforståelse, beskyttelse av kritisk infrastruktur og cybersikkerhet som strategiske risikoområder med særlig betydning for nasjonal sikkerhet.

Cybersikkerheten i virksomheter og hos myndigheter utfordres av stadig mer avanserte cyberoperasjoner. Kunstig intelligens må tas i bruk for å styrke analyse og avdekking av cyberoperasjoner. Samtidig må brukere av kunstig intelligens-modeller være bevisst på sårbarheter i teknologien som kan utnyttes av trusselaktører. Kunstig intelligens gjør fabrikkerte nyheter stadig mer troverdige. Kombinert med at desinformasjon kan spres på en helt annen skala enn tidligere, utfordres grunnmuren i demokratiske styresett.

EUs critical technology areas for the EU's economic security

EU har laget en liste over kritiske teknologiområder for EUs økonomiske sikkerhet. Denne listen ble lansert i oktober 2023[8]. EU jobber videre, i dialog med medlemslandene, for å gjøre risikovurderinger av de identifiserte teknologiområdene.
Listen inneholder følgende teknologiområder, med underliggende teknologier:

Technology Area	**Technologies**
ADVANCED SEMICONDUCTORS TECHNOLOGIES	Microelectronics, including processors Photonics (including high energy laser) technologies High frequency chips

[7] https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2024
[8] https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

Technology Area	Technologies
	Semiconductor manufacturing equipment at very advanced node sizes
ARTIFICIAL INTELLIGENCE TECHNOLOGIES	High Performance Computing Cloud and edge computing Data analytics technologies Computer vision, language processing, object recognition
QUANTUM TECHNOLOGIES	Quantum computing Quantum cryptography Quantum communications Quantum sensing and radar
BIOTECHNOLOGIES	Techniques of genetic modification New genomic techniques Gene-drive Synthetic biology
ADVANCED CONNECTIVITY, NAVIGATION AND DIGITAL TECHNOLOGIES	Secure digital communications and connectivity, such as RAN & Open RAN (Radio Access Network) and 6G Cyber security technologies incl. cyber-surveillance, security and intrusion systems, digital forensics Internet of Things and Virtual Reality Distributed ledger and digital identity technologies Guidance, navigation and control technologies, including avionics and marine positioning
ADVANCED SENSING TECHNOLOGIES	Electro-optical, radar, chemical, biological, radiation and distributed sensing Magnetometers, magnetic gradiometers Underwater electric field sensors Gravity meters and gradiometers
SPACE & PROPULSION TECHNOLOGIES	Dedicated space-focused technologies, ranging from component to system level Space surveillance and Earth observation technologies Space positioning, navigation and timing (PNT)

Technology Area	Technologies
	Secure communications including Low Earth Orbit (LEO) connectivity Propulsion technologies, including hypersonics and components for military use
ENERGY TECHNOLOGIES	Nuclear fusion technologies, reactors and power generation, radiological conversion/enrichment/recycling technologies Hydrogen and new fuels Net-zero technologies, including photovoltaics Smart grids and energy storage, batteries
ROBOTICS AND AUTONOMOUS SYSTEMS	Drones and vehicles (air, land, surface and underwater) Robots and robot-controlled precision systems Exoskeletons AI-enabled systems
ADVANCED MATERIALS, MANUFACTURING AND RECYCLING TECHNOLOGIES	Technologies for nanomaterials, smart materials, advanced ceramic materials, stealth materials, safe and sustainable by design materials Additive manufacturing, including in the field Digital controlled micro-precision manufacturing and small-scale laser machining/welding Technologies for extraction, processing and recycling of critical raw materials (including hydrometallurgical extraction, bioleaching, nanotechnology-based filtration, electrochemical processing and black mass)

Prioriterte områder for NATO

Når det gjelder teknologiutvikling som er relevant for forsvaret, pekes det ofte på NATOs prioriterte Emerging and Disruptive Technologies. NATO har ni prioriterte teknologiområder[9]:

- kunstig intelligens
- autonomi
- kvanteteknologi
- bioteknologi og menneskelig ytelsesforbedring
- hypersoniske systemer
- rom
- nye materialer og produksjon

[9] https://www.nato.int/cps/en/natohq/topics_184303.htm?

- energi og fremdrift
- neste-generasjons kommunikasjonsnettverk.

Disse teknologiområdene komplementerer de ti prioriterte forskningsområdene for NATOs Science and Technology Organization (STO)[10], som har ligget fast siden 2018 (se tabell under).

***Table 2.3:** NATO S&T Priorities.*

Domain	NATO S&T Priority Areas	Targets of Emphasis
HUMAN	Advanced Human Performance & Health	Medical Solutions for Health Optimisation
		Human Resiliency
		Enhanced Cognitive Performance
		Human & Machine Interfaces
	Cultural, Social & Organisational Behaviours	Social Influence
		Political Influence
		Cultural Communications
		Group & Organisational Behaviour
INFORMATION	Data Collection and Processing	EM Sensors
		Non-EM Sensors
		Sensor Integration & Networks
		Advanced Signal Processing
	Information Analysis & Decision Support	Big Data & Long Data Processing and Analysis
		Big Data & Human Decision Making
		Multi-Domain Situational Awareness
		Planning and Managing Uncertainties
	Advanced Systems Concepts	Integrated Human - Machine Hybrid Force
		Clusters & Swarms
		Modular, Scalable Systems
		High Assurance Engineering & Validation
	Autonomy	Artificial Intelligence
		Mission Autonomous Systems
		Human-Autonomous Machine Teaming
	Communications & Networks	Secure and Resilient Communications
		Trusted Multi-Domain Information Sharing
		Ad hoc and Heterogeneous Networks
PHYSICAL	Precision Engagement	Precision Control
		Weapons - Techniques and Systems
		Weapons - Effects
		Active & Passive EM, Acoustic & Optical Countermeasures
	Platforms & Materials	Fast and Agile Platforms
		Unmanned Platforms
		Hypersonic Platforms
		Advanced and Adaptive Materials
		In-Theatre Fabrication & Production of Equipment
	Power & Energy	Power & Energy Storage
		Alternative & Renewable Energy Sources
		Propulsion
		Enhanced Energy Efficiency & Management

USAs National Science and Technology Council

Følgende skrives om rollen til the National Science and Technology Council[11]; The National Science and Technology Council (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure that science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized

[10] https://www.sto.nato.int/Pages/default.aspx
[11] http://www.whitehouse.gov/ostp/nstc

under committees that oversee subcommittees and working groups focused on different aspects of science and technology.

Critical and emerging technologies list

Følgende teknologiområder vurderes som spesielt viktige for USAs nasjonale sikkerhet i en i en vurdering fra februar 2024[12]. Hvert område har i tillegg et sett med underområder som spesifiseres.

- Advanced Computing
- Advanced Engineering Materials
- Advanced Gas Turbine Engine Technologies
- Advanced and Networked Sensing and Signature Management
- Advanced Manufacturing
- Artificial Intelligence
- Biotechnologies
- Clean Energy Generation and Storage
- Data Privacy, Data Security, and Cybersecurity Technologies
- Directed Energy
- Highly Automated, Autonomous, and Uncrewed Systems (UxS), and Robotics
- Human-Machine Interfaces
- Hypersonics
- Integrated Communication and Networking Technologies
- Positioning, Navigation, and Timing (PNT) Technologies
- Quantum Information and Enabling Technologies
- Semiconductors and Microelectronics
- Space Technologies and Systems

[12] https://www.whitehouse.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf

Vedlegg C: Rammer for sivil-militært samarbeid

Dette notatet peker først på noen utfordringer for den åpne forskningen i sivil-militært samarbeid. Deretter foreslår det noen viktige momenter som bør hensyntas for å kunne håndtere utfordringene. Spesifikke forslag til slike momenter er uthevet i kursiv.

1. Utfordringer knyttet til rammene for den åpne forskningen:

Forskningssikkerhet: Med «forskningssikkerhet» menes håndtering av risikoer knyttet til: a) uønsket overføring av kritisk kunnskap og kunnskap og teknologi som kan påvirke nasjonal sikkerhet, (b) uønsket innflytelse på eller påvirkning av forskning som krenker akademisk frihet og forskningsintegritet; (c) etiske eller integritetsbrudd, der kunnskap og teknologi brukes til å undertrykke eller undergrave grunnleggende verdier[1].

Forskningssikkerhet har blitt en betegnelse som har fått økt aktualitet med dagens geopolitiske situasjon. Forskningssikkerhet handler om å finne en balanse mellom åpenhet og beskyttelse, slik at vi kan fremme vitenskapelig kunnskap samtidig som vi ivaretar sensitiv informasjon. Med økende digitalisering og globalisering er det viktigere enn noensinne å beskytte forsknings-resultater, forhindre uautorisert tilgang og sikre at sensitiv informasjon ikke kommer på avveie. Dette gjelder spesielt innen områder av interesse for nasjonal sikkerhet. Forskning med potensiell sivil og militær bruk kan også skape dilemmaer hvor forskere må balansere potensielle positive bidrag til utvikling av forskningen og relevans for samfunnet mot risikoen for at forskningen havner i gale hender eller benyttes på en måte som skader nasjonal sikkerhet. Dette stiller store krav til forskernes vurderinger av potensielle konsekvenser.

Internasjonalt samarbeid: Internasjonalt forskningssamarbeid er grunnleggende for å sikre kvalitet og fornyelse i forskningen. Samtidig har slik internasjonal samhandling blitt mer komplisert og risikofylt, med økt fare for industrispionasje og uønsket overføring av kunnskap som kan være av kritisk viktighet for våre nasjonale interesser. Norske universiteter og forskningsinstitutter er attraktive mål. Internasjonalt samarbeid kan føre til at norsk teknologi og kunnskap utnyttes på måter som bryter med reglene for eksportkontroll.

For å møte behovene for kompetanse innen ulike fagfelt, er Norge avhengig av internasjonal forskermobilitet. Internasjonal forskningsmobilitet kan imidlertid medføre risiko for at vitenskapelig arbeid kompromitteres, at etiske standarder settes under press, ulovlig overføring av kunnskap og at norsk teknologi og kunnskap utnyttes på måter som bryter med reglene for eksportkontroll[2].

Forskningsmiljøene vi har konsultert i forbindelse med denne rapporten uttrykker at de i dag opplever flaskehalser i systemet knyttet til eksportkontrollvurderinger ved rekruttering og at ansettelsesprosesser som omfattes av dette er svært krevende og tar uforholdsmessig lang tid.

[1] European Commission 24.1.24 "COUNCIL RECOMMENDATION on enhancing research security" e82a2fd9-ac12-488a-a948-87639eef10d4_en (europa.eu)

[2] Se oversikt over kjente utfordringer i internasjonalt samarbeid om høyere utdanning og hva som bør kartlegges med hensyn til samarbeidsland og partnerinstitusjon her: Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid | HK-dir (hkdir.no)

Deltagelse i skjermingsverdig forskningssamarbeid: Deltagelse i forskningssamarbeid med skjermet eller gradert informasjon kan kreve sikkerhetsklarering av personell og beskyttelse av gradert informasjon gjennom sikkerhetssystemer og infrastruktur. Sikkerhetsklarering krever betydelige ressurser og tid, noe som kan være en belastning spesielt for mindre institusjoner. Det vil være kostbart å bygge opp forvaltnings- og forskningsinfrastruktur som tilfredsstiller nødvendige sikkerhetskrav. Dette kan føre til en situasjon hvor bare et fåtall, ofte større og etablerte institusjoner, får muligheten til å delta i slike prosjekter, noe som kan begrense mangfoldet og innovasjonen i forskningen.

Begrensninger i forskningsagendaen og forskningsprioriteringer: Når forskningsagendaer i større grad påvirkes, eller formes av forsvars- eller sikkerhetsmessige interesser, kan det ha en innvirkning på den akademiske friheten og prioriteringer av forskningsmidlene.

Åpenhet i forskningen: Forskningsetikk fremmer åpenhet i forskningsprosessen for å sikre troverdighet og etterprøvbarhet. I forsvarsforskning er det imidlertid ofte krav om beskyttelse av sikkerhetshensyn. Denne mangelen på åpenhet kan hindre uavhengig validering av forskningsresultater og begrense diskusjonen om forskningens etiske og sosiale konsekvenser. Sikkerhet er en sentral prioritet, der forskningsresultater ofte skjermes eller graderes for å beskytte nasjonal sikkerhet. Den grunnleggende verdien av åpenhet og deling i sivil forskning kan kollidere med behovet for sikkerhet og konfidensialitet i forsvarsforskning.

Merittering og karrierebygging: Publisering av forskningsresultater er viktige elementer i forskeres karriere. Akademisk frihet innebærer at forskere står fritt til å utføre og publisere sin forskning og velge forskningsmetoder og forskningspartnere fra hele verden, mens internasjonal mobilitet av forskertalenter er avgjørende for å fremme innovasjon og oppnå vitenskapelige gjennombrudd. Sivil-militært samarbeid kan legge begrensninger på "tradisjonell" karriereutvikling innen akademia ved at forskningsresultater graderes av hensyn til nasjonal sikkerhet. Arbeid med skjermet og spesielt gradert forskning kan også legge begrensninger på internasjonalt samarbeid og forskermobilitet.

2. Momenter for å kunne håndtere utfordringene

Forskningssikkerhet: Forskningsinstitusjoner i Norge og internasjonalt arbeider aktivt med å styrke forskningssikkerheten og opprettholde integriteten i vitenskapelig arbeid[3]. Forsknings-institusjoner må følge lover, forskrifter og instruksjoner på feltet[4]. Hver enkelt virksomhet må imidlertid selv vurdere hvordan de implementerer de overordnede kravene og prinsippene. I Rådsanbefalingen om å styrke forskningssikkerhet på nasjonalt- og sektornivå understreker Europakommisjonen at forskningssikkerhetstiltak bare kan være virkelig effektive hvis dette anvendes konsekvent på alle nivåer, både på EU-nivå, på nasjonalt, regionalt og institusjonelt nivå, for å unngå smutthull og omgåelse. *Det vil være behov for at systemer for opplæring, veiledning og rutiner innarbeides på forskningsinstitusjoner og forankres institusjonelt.* Opplæring av ansatte er viktig for å bygge sikkerhetskultur.

[3] EUs sikkerhetspakke legger vekt på å finne en balanse mellom åpenhet og sikkerhet. I tråd med Rådsanbefalingen om å styrke forskningssikkerhet på nasjonalt- og sektornivå, har en rekke land (f.eks. Sverige, Danmark, England, Tyskland, Nederland, Belgia, Østerrike, USA og Australia) utviklet overordnede retningslinjer for ansvarlig kunnskapssamarbeid.
[4] Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid | HK-dir (hkdir.no)

Riksrevisjonen[5] påpeker at det er behov for å styrke håndteringen av forskningsdata og IT-sikkerheten hos mange institusjoner. Institusjoner må ha tilgang til sikre systemer og ha nødvendige sikkerhetsrutiner på plass dersom de skal utføre forskning med skjermet eller gradert informasjon.

Internasjonalt samarbeid: I Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid nevnes en rekke konkrete råd for hvordan institusjoner kan gjøre verdivurderinger og organisere forsvarlig kunnskapssamarbeid. Selv om retningslinjer for forskningssikkerhet er på plass, er det den enkelte institusjon som må gjøre de konkrete vurderingene, noe som ofte er krevende. Det må utvikles tilpasset kompetanseheving på sikkerhet hos institusjonene som involverer alle ansatte som har behov for det slik at de blir mer bevisste og tar ansvar. Her vil det være forskjeller i ulike fagmiljøer.

Det vil være behov for å koordinere kompetanseheving på tvers av institusjoner og *det bør vurderes å etablere opplegg for kurs, opplæring og veiledning hos forskningsinstitusjonene for å ivareta forskningssikkerheten.*

Deltagelse i skjermingsverdig forskningssamarbeid: Institusjoner og enkeltforskere må ofte sikkerhetsklareres for å kunne arbeide med sikkerhetsrelaterte problemstillinger og infra-struktur og fasiliteter må beskyttes. *Samordnet tilgang til eksisterende sikker forsknings- og forvaltningsinfrastruktur for kvalifiserte forskningsmiljøer er en løsning som kan bidra til hurtigere involvering.* Dette innebærer at eksisterende sikker infrastruktur og anlegg, både internt hos forskningsinstitusjoner eller ved militære anlegg o.l., kan tas i bruk av sikkerhets-klarerte forskningsmiljøer, fremfor at det bygges opp ny hos hver enkelt aktør. *Kostnadsmessig og sikkerhetsmessig lønner det seg å begrense antall lokasjoner og systemer hvor det kan utføres gradert eller skjermet forskning.*

Begrensninger i forskningsagendaen og forskningsprioriteringer: I de forskningspolitiske føringene og i utlysninger bør det understrekes at utlysninger rettet mot sivil forskning fortsatt som hovedprinsipp skal gjennomføres åpent og dermed videreføre dagens praksis.

Åpenhet og transparens i forskningen: Det må fortsatt være et grunnleggende prinsipp at forskere skal kunne planlegge sine karrierer i tråd med prinsippet om akademisk frihet og deling. Det er en utfordring å finne en balanse der forskere kan dele generisk kunnskap og metoder og samarbeide internasjonalt, uten å sette den nasjonale sikkerheten i fare[6]. Forskningsinstitusjoner og fagmiljøer som jobber med oppdrag der oppdragsgivere har eierskap til prosjektresultatene, har ofte rutiner for skjerming og er vant til at publisering må avtales fra sak til sak. Flere av institusjonene vi har snakket med i forbindelse med denne rapporten uttrykker at de inngår i samarbeid med Forsvaret hvor de i stor grad kan jobbe med generisk kunnskap som kan deles og publiseres. Forsvaret kan siden videreutvikle forskning og teknologi på gradert nivå. Denne "arbeidsdelingen" krever imidlertid systemer og kompetanse på å skille generiske elementer fra det skjermingsverdige.

[5] Sensitive forskningsdata kan komme på avveie (riksrevisjonen.no)

[6] Ifølge Lov om universiteter og høyskoler kan styret ved UH-institusjoner samtykke til utsatt offentliggjøring av resultater når det er legitime hensyn til dette. Det kan ikke avtales eller fastsettes varige begrensninger i retten til å offentliggjøre resultater utover det som følger av lov eller i samsvar med lov. Dette er en lite utprøvd problemstilling opp mot for eksempel Sikkerhetsloven.

Data og infrastruktur:
Datasett som produseres i forsvarssektoren skal følge FAIR-prinsippene[7] i likhet med data som finansieres av for eksempel Forskningsrådet. Datasett skal gjøres tilgjengelig så bredt som mulig, men innsamling av data på tvers av etatene i forsvarssektoren må foregå innenfor lovmessige krav til blant annet sikkerhetsgradert informasjon, nødvendig autorisasjon og personvern. *Forskere og administrativt personell vil trenge mer opplæring i sikker håndtering av data.* Dette krever både tid og ressurser i tillegg til investeringer i teknologi og plattformer. *Det er behov for investeringer i infrastruktur som kan støtte sikker lagring og deling av forskningsdata*[8]*.*

Merittering og karrierebygging: Å bygge nettverk, samarbeide med andre forskere og publisere relevant forskning er avgjørende for å opparbeide seg en akademisk karriere. Når forskere deltar i skjermet eller gradert forskningssamarbeid kan de publisere i mindre grad enn i "åpne" forskningssamarbeid. Likevel vil det være mulig for forskere som har jobbet med slik forskning å opparbeide seg en akademisk karriere, for eksempel ved at deler av ugraderte forsknings-resultater publiseres åpent. *I den forsvars- og sikkerhetsrelaterte forskningen vil det i mange tilfeller være mulig å kunne jobbe ugradert helt fram til det utvikles løsninger. Dette vil imidlertid kreve gode rutiner for å identifisere og sikre at kun ugradert forskning blir delt og publisert i den grad dette er mulig.*

Det kan være hensiktsmessig å skille mellom studenter, som er avhengig av publisering og internasjonal mobilitet for å bygge opp en karriere, og etablerte forskere som er mindre avhengige av dette. Det vil være mer hensiktsmessig for etablerte forskere å delta i forskningssamarbeid der kunnskap og teknologi må skjermes enn for studenter. *Forskere kan gå "inn og ut" av forsvarsforskning ved å for eksempel kombinere midlertidig ansettelse i Forsvaret med en "toer-stilling" ved en sivil forskningsinstitusjon, eller motsatt.*

[7] Strategi for kunstig intelligens for forsvarssektoren (regjeringen.no)
[8] Det kan være muligheter innenfor såkalt "Zero Trust arkitektur" som vektlegger at robuste sikkerhetstiltak er like viktig internt i virksomheter som for systemer eksponert mot internett. Data og tjenester kan få en innebygget sikkerhet gjennom autentiserings og autorisasjonsmekanismer som beskytter dataene mot uautorisert tilgang. Denne arkitekturen kan være en mulighet for å fremme mer deling av skjermede og graderte data.

Forskningsrådet NSM FFI Forsvarets forskningsinstitutt

Kunnskapsdepartementet
postmottak@kd.dep.no

Vår saksbehandler / tlf.	Vår ref.	Deres ref.	Sted
Pål Sørgaard / 4812 7174	24/124	22/4421 (KD)	Oslo 16.02.2024

Felles oppdrag til Forskningsrådet, NSM og FFI
Del 2d – Infrastruktur: konsekvenser og forutsetninger

Vi viser til felles oppdrag til Forskningsrådet, NSM og FFI fra Forsvarsdepartementet og Kunnskapsdepartementet i supplerende tildelingsbrev datert 15.12.23. I oppdraget ber departementene om et felles innspill til hvordan forskningssystemet må innrettes for også å håndtere skjermingsverdig og gradert forsknings- og teknologisamarbeid. Det ønskes beskrivelser av risiko og økonomiske og administrative konsekvenser for de ulike løsningene.

Departementene ber om en felles rapport med frist 31. mai. Det bes videre om en egen forsendelse som svarer på oppdragets punkt 2.d med frist 16. februar 2024. Dette brevet med vedlagte rapport er vårt svar på bestillingen knyttet til punkt 2.d.

Vi vil aller først takke for oppdraget. Det er aktuelt og utfordrende, og gir oss en mulighet til å bidra til å styrke samfunnssikkerhet og skjerming av Norges verdier. Oppdraget har korte frister, særlig fristen 16. februar. Vi tilpasser ambisjonsnivået til tidsfristene, og usikkerheten i vurderingene påvirkes av rammene for oppdraget. Vi ser oppdraget som starten på en lengre prosess.

Oppdragets punkt 2.d:

> «Hvilke investeringer i infrastruktur er nødvendig for å understøtte et nasjonalt forskningssystem for åpen, skjermingsverdig og gradert FoU? Infrastruktur inkluderer forvaltningsinfrastruktur (for tildelinger, prosjektsøknader, oversikt osv.) og infrastruktur som støtter gjennomføringen av FoU. Løsningsalternativer må beskrives skalert utfra

Norges forskningsråd
Drammensveien 288
Postboks 564
NO-1327 Lysaker

+47 220 37 000
post@forskningsradet.no
forskningsradet.no
Org.nr. 970 141 669

All post og e-post som inngår i saksbehandlingen, bes adressert til Norges forskningsråd og ikke til enkelte personer.

(1) hva som er mulig innenfor dagens rammer,
(2) hva som er mulig innenfor en moderat økning i rammevilkår og
(3) hva et optimalt alternativ vil kreve av investeringer.»

Punkt 2.d inngår i oppdragets del 2 «konsekvenser og forutsetninger», som logisk sett følger etter del 1 «innretning og behov». Del 1 er premissgivende for del 2, men det er også slik at praktiske løsninger, med kostnader og usikkerheter, kan være premisser for vurderinger av innretning og behov. I denne leveransen besvares punkt 2.d isolert, uten at konsekvenser og forutsetninger eller innretning og behov er ferdig utredet. Et mer utfyllende svar vil komme i sluttleveransen 31. mai.

Spørsmålene om hva slags forskningssamarbeid og hva slags forskningsforvaltning som er det beste for Norge, og hva vi skal legge til rette for, er fortsatt ubesvart. Dette bidrar til usikkerhet i estimatene. Når vi allikevel mener at estimatene er verdifulle skyldes det at en betydelig del av utgiftene vil påløpe uavhengig av valg av løsning. Det å jobbe med en konkret løsning har gjort det nødvendig og mulig å vurdere en rekke forhold som har stor overføringsverdi til andre løsningsforslag.

Alternativ 1, innenfor dagens rammer

Rapporten viser til at dagens forvaltningssystem i Forskningsrådet kan brukes til finansiering av både åpen og skjermingsverdig, men ikke gradert, FoU. Tilsvarende kan FD og andre departementer finansiere åpne og skjermingsverdige bidrags- eller oppdrags-prosjekter til flere aktører enn i dag, uten at det nødvendigvis krever vesentlige investeringer. Det er med andre ord muligheter innenfor dagens rammer. Samtidig noterer vi at det er betydelige forskjeller mellom det sivile forskningssystemet og forsvarssektorens forskningssystem.

Mulighetene for økt gradert forskning er små i dette alternativet, siden det ikke er mange forskningsmiljøer som er rustet til det. En slik løsning vil derfor ikke bidra til mulighetene for å se på tvers av skillet gradert og ugradert.

Alternativ 2, innenfor en moderat økning i rammevilkår

Dette er alternativet som er vurdert i størst detalj, se vedlagte rapport. Alle tall som oppgis i dette brevet er forventet prosjektkostnad (P50) i 2024-priser inkl. mva. I rapporten er det også P85-estimater (med P50 og P85 mener man at sannsynligheten for at kostnadene vil ligger under eller lik estimatet er hhv 50% og 85%).

I rapporten identifiseres et sentralt eksempel på infrastruktur for forskningsforvaltning: en IT-løsning for søknadsoppfølging og prosjektoppfølging på nivå BEGRENSET. Dette er forenklet sagt en kopi av Forskningsrådets nye system for søknadsbehandling og prosjektoppfølging, implementert på Nasjonalt begrenset nett (NBN). Det er ikke gitt at denne IT-løsningen er det første som skal implementeres, men som estimat er denne IT-løsningen et relevant eksempel på hvilket nivå av kostnader vi må regne med for ny forvaltningsinfrastruktur på et moderat ambisjonsnivå.

Med dette utgangspunktet, estimeres en investeringskostnad på 18,75 MNOK i 2025 og en løpende årlig kostnad på 6,25 MNOK fra og med 2025 for den sentrale infrastrukturen for forskningsforvaltning. Det er en egen usikkerhet knyttet til dette estimatet: en samling av opplysninger som hver for seg er på nivå BEGRENSET kan som samling bli vurdert å være på et høyere graderingsnivå, noe som vil innebære en vesentlig økning i utgiftene. Denne usikkerheten er ikke lagt inn i estimatet. En slik samlet vurdering vil måtte bygge på en nærmere vurdering av hvilke data som lagres i systemet og av systemets mekanismer for tilgang til informasjon.

I rapporten vurderes også kostnadene et forskningsmiljø vil ha knyttet til etablering av digitale systemer og infrastruktur som støtter forvaltning *og* FoU-samarbeid mellom ulike aktører og/eller forskningsmiljøer på nivå BEGRENSET (det legges til grunn at det er samme infrastruktur for forvaltning og for samhandling / generell IT-støtte) samt de nødvendige investeringene i oppgradering av lokaler, adgangskontroll, mm. Dette er altså en form for stykkpris som må multipliseres med antall forskningsmiljøer hvor dette er aktuelt. Pr. forskningsmiljø er denne kostnaden vurdert til 5,75 MNOK i investeringer i 2025 og 3,125 MNOK i årlig drift fra og med 2025.

I tillegg antas det at det vil være behov for egne PCer for BEGRENSET, beregnet til 60.000 kr pr arbeidsplass. Den utgiften er ikke innarbeidet i de summene som presenteres i dette brevet.

Utover det foreligger det ingen estimater av kostnadene på BEGRENSET nivå knyttet til bruk av spesifikk forskningsinfrastruktur, enkelt sagt de verktøyene som brukes for å gjennomføre forskning. Disse kostnadene vil variere betydelig, avhengig av hva slags FoU og dermed verktøy det er snakk om. Om det er helt mekanisk utstyr kan tilleggskostnaden være null. Om det er snakk om infrastruktur for tungregning vil kostnaden være høy, men trolig felles for mange forskningsmiljøer. Om det er digitalt forskningsutstyr, f.eks. sensorer av et slag, er utfordringen at samme digitale utstyr skal kunne levere data på åpent nivå og på gradert nivå uten at det er fare for at graderte data lekker ut. Hva som må til i slike tilfeller vil være utstyrsspesifikt.

Med en antakelse om at det i første omgang er aktuelt å etablere en slik løsning i 10 forskningsmiljøer, estimeres en kostnad på 76,25 MNOK i 2025 og en løpende årlig driftskostnad på 37,5 MNOK for infrastruktur for gjennomføring av FoU. Med 20 forskningsmiljøer blir det 133,75 MNOK i investeringer og 68,75 MNOK i årlige driftsutgifter.

Alternativ 3, hva et mer ambisiøst alternativ vil kreve av investeringer

Det er vanskelig å definere hva som vil være et «optimalt» alternativ. I sluttleveransen kommer vi til å si noe om hvordan vi mener det bør legges til rette for å understøtte et nasjonalt forskningssystem for åpen, skjermingsverdig og gradert FoU.

I rapporten beskrives det «optimale» alternativet som et alternativ som minner om det moderate alternativet, men som i tillegg kan håndtere forskning på nivå HEMMELIG. Det antas at tilgangsstyringen på nivå HEMMELIG vil være så streng at det ikke er aktuelt å

konkurranseutsette midlene, men at de i stedet tildeles direkte. Det innebærer at behovet for en omfattende forvaltingsinfrastruktur reduseres.

Allikevel er kostnadene svært høye, grunnet de omfattende kravene til sikkerhet. For den sentrale infrastrukturen estimeres investeringskostnadene til 37,5 MNOK og de årlige driftskostnadene til 12,5 MNOK. Pr. forskningsmiljø er investeringskostnadene estimert til 19,5 MNOK og de årlige driftskostnadene til 9,375 MNOK. Det understrekes at det er spesielt høy usikkerhet når det gjelder estimatene for nivå HEMMELIG.

I rapporten legges ulikt graderingsnivå til grunn for skillet mellom et moderat og et mer ambisiøst alternativ. En annen inngang til et mer ambisiøst alternativ kunne være å legge til rette for flere former for forskningsforvaltning eller for forskjellige typer forskningssamarbeid. Slike vurderinger er ikke foretatt i denne leveransen.

Om usikkerhet

På flere områder bygger estimatene på kjente priser eller erfaringstall. Samtidig er det betydelige usikkerheter. De største usikkerhetene knytter seg til hva slags forskningsinfrastruktur som er aktuell og til hva slags forskningssamarbeid og forskningsforvaltning man ønsker å legge til rette for. Det er vurderinger det ikke har vært rom for i arbeidet så langt.

Når dette er sagt er det vår vurdering at estimatene som det redegjøres for i denne rapporten, er representative for hva slags kostnader man må regne med for å muliggjøre ugradert-gradert og sivilt-militært FoU-samarbeid i større skala enn i dag. Sluttleveransen fra oppdraget vil gi en samlet vurdering av disse spørsmålene.

Med vennlig hilsen

Mari Sundli Tveit
Adm. direktør
Norge forskningsråd

Lars Christian Aamodt
Direktør
Nasjonal sikkerhetsmyndighet

Kenneth Ruud
Adm. direktør
Forsvarets forskningsinstitutt

Mottakere:

- Forsvarsdepartementet
- Kunnskapsdepartementet
- Justis- og beredskapsdepartementet att. Annette Tjaberg (kopi)

Norges forskningsråd
Drammensveien 288
Postboks 564
NO-1327 Lysaker

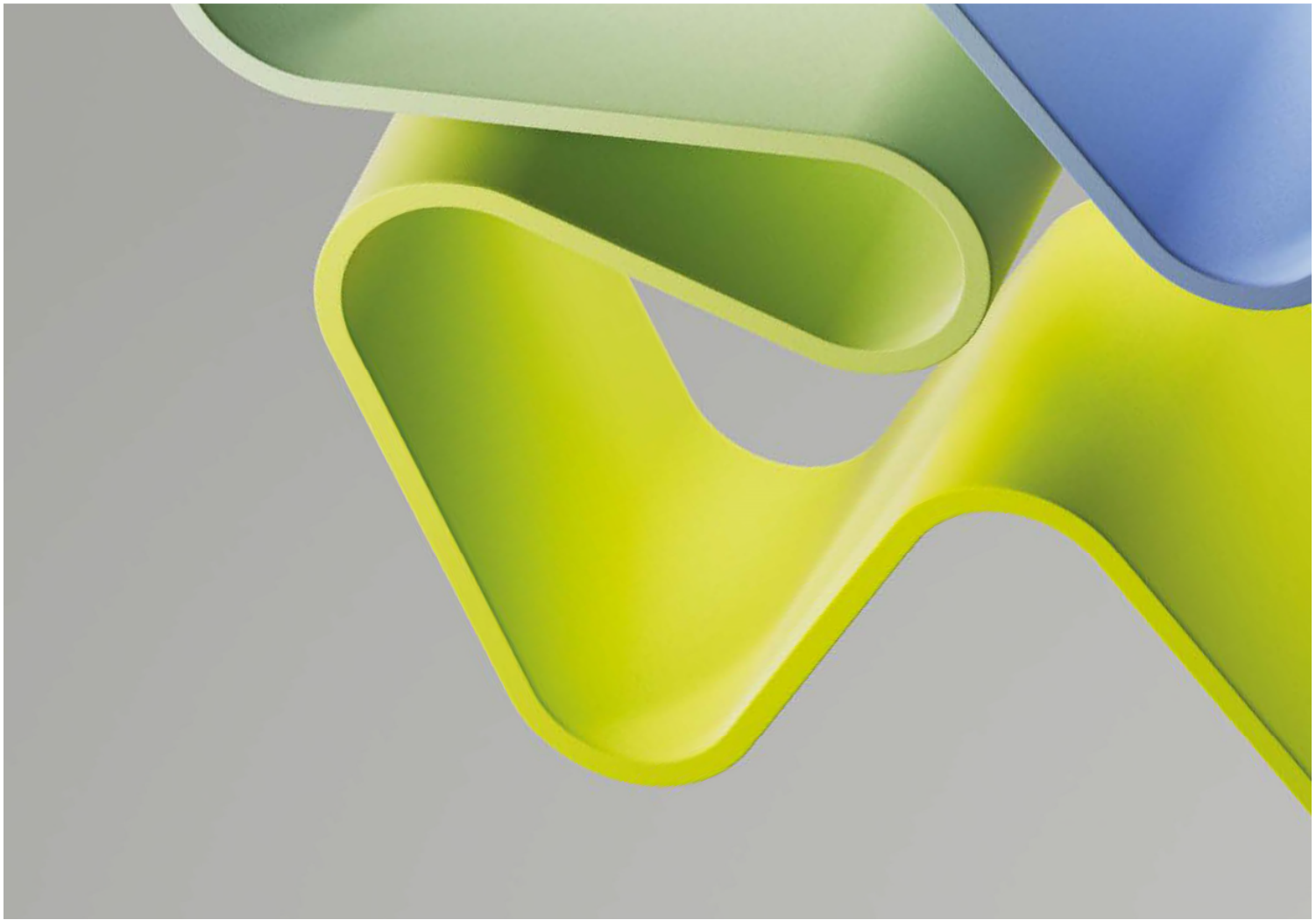
+47 220 37 000
post@forskningsradet.no
forskningsradet.no
Org.nr. 970 141 669

All post og e-post som inngår i saksbehandlingen, bes adressert til Norges forskningsråd og ikke til enkelte personer.

Forskningsrådet

Infrastruktur for et nasjonalt forskningssystem for åpen, skjermingsverdig og gradert FoU

Svar på del 2d i oppdrag til Forskningsrådet, Forsvarets forskningsinstitutt og Nasjonal sikkerhetsmyndighet i supplerende tildelingsbrev av 15.12.2023 fra Forsvarsdepartementet og Kunnskapsdepartementet



Innhold

Innledning 4

Oppdragsbeskrivelsen i oppdragsbrevet 4
Bakgrunn 4
Definisjoner av begreper benyttet i besvarelsen vår 4
Forståelse og avgrensning av oppdragets del 2d 5
Ytterligere avgrensninger og forutsetninger 6
Gradering 6

Investeringer i forvaltningsinfrastruktur 7

Forskningsforvaltning det må legges til rette for 7
Muligheter innenfor dagens rammer 7
Muligheter innenfor en moderat økning i rammevilkår 7
Et optimalt alternativ 12

Investeringer i forskningsinfrastruktur Hva slags forskningssamarbeid bør det legges til rette for? 15

Muligheter innenfor en moderat økning i rammevilkår 15
Et optimalt alternativ 16

Kort om forutsetninger for gradert FoU 17

Graderingsnivå 17
Godkjenning av IT-systemer 17
Fysisk sikkerhet 17
Personellsikkerhet 18
Organisatoriske forutsetninger for å håndtere gradert informasjon 18
Omfang av gradert informasjon 18

Innledning

Oppdragsbeskrivelsen i oppdragsbrevet

Rapporten besvarer konseptuelt oppdragets del 2d:

> Hvilke investeringer i infrastruktur er nødvendig for å understøtte et nasjonalt forskningssystem for åpen, skjermingsverdig og gradert FoU? Infrastruktur inkluderer forvaltningsinfrastruktur (for tildelinger, prosjektsøknader, oversikt osv.) og infrastruktur som støtter gjennomføringen av FoU. Løsningsalternativer må beskrives skalert utfra (1) hva som er mulig innenfor dagens rammer, (2) hva som er mulig innenfor en moderat økning i rammevilkår og (3) hva et optimalt alternativ vil kreve av investeringer.

Bakgrunn

Oppdragsbrevet gi følgende bakgrunn for oppdraget:

> Trussel- og risikobildet mot Norge og norske interesser blir stadig mer sammensatt og sektorovergripende. Dette øker den gjensidige avhengigheten mellom sivile og militære aktører, på tvers av sektorer og ansvarsområder nasjonalt, og på tvers av landegrenser og allierte samarbeidspartnere. Sikkerhet og beredskap vektlegges mer i alle sektorer. Kunnskap, kompetanse og teknologi blir stadig viktigere for internasjonal konkurranse, nasjonal sikkerhet og samfunnets motstandskraft. Flere enn tidligere vil bli involvert i sikkerhets- og beredskapsarbeid, og flere virksomheter vil komme i situasjoner der sikkerhet blir et sentralt hensyn i beslutningsprosesser. Det nasjonale forskningssystemet må kunne håndtere dette. I årene fremover vil det være behov for en mer strategisk tilnærming til kunnskapsutvikling, forskning og teknologiutvikling for å ivareta nasjonale sikkerhets- og forsvarspolitiske interesser. Både Forsvarskommisjonen og Totalberedskapskommisjonene peker på behovet for økt tverrsektorielt samarbeid og anbefaler at det etableres ytterligere mekanismer for å utvikle og ivareta relevant kunnskap på tvers av samfunnsområder, skjermingsbehov og gradering.
>
> Forsvars- og sikkerhetsrelatert FoU stiller større krav til infrastruktur, sikkerhetskompetanse og sikkerhetskultur enn annen FoU. Det norske forskningssystemet må videreutvikles og innrettes på en måte som gjør det i stand til å håndtere større grad av sensitivt, skjermingsverdig og sikkerhetsgradert forsknings- og teknologisamarbeid.

Definisjoner av begreper benyttet i besvarelsen vår

- *Forskningssystemet:* Ifølge siden «Forskningssystemet» på regjeringen.no omfatter forskningssystemet «aktørene som driver, påvirker og bruker forskning, og relasjonene mellom dem». En mer utdypende definisjon finnes på siden vi har lenket til ovenfor.

- *Forvaltningsinfrastruktur* (for tildelinger, prosjektsøknader, oversikt osv.): Systemer og digital infrastruktur som muliggjør konkurranseutsetting av offentlige tilskudd (bidrag) til forskning og utvikling (FoU).[1] Dette inkluderer systemer og infrastruktur for kommunikasjon mellom dem som søker om midler, og den som

[1] Merk at denne definisjonen ikke inkluderer oppdragsforskning slik den i dag foregår med for eksempel Forsvarsdepartementet, Forsvaret eller våpenindustrien som oppdragsgiver til en forskningsinstitusjon som FFI eller en annen leverandør av FoU-tjenester.

deler ut de offentlige tilskuddene etter at konkurransen er gjennomført, og for kommunikasjon mellom sistnevnte og nasjonale eller utenlandske eksperter som deltar i evalueringen av søknadene.[2]

- *Generisk IT-støtte for FoU:* Digitale systemer og infrastruktur som støtter FoU-samarbeid mellom ulike aktører eller institusjoner, som e-post, samhandlingsrom, fildeling og servere for deling av data. Vi mener her digital samhandling både mellom ulike forskningsinstitusjoner og mellom forskningsinstitusjoner og aktører i næringslivet eller offentlig sektor.

- *Forskningsinfrastruktur:* Vitenskapelig utstyr og utstyrsfasiliteter, elektronisk infrastruktur for tungregning, analyser og håndtering av store datamengder, i tillegg til vitenskapelige databaser og samlinger. Dette inkluderer altså IT-utstyr som er nødvendig for forskningen, utover samhandling mellom ulike aktører. Kort sagt er dette en samlebetegnelse for de verktøyene forskere bruker for å gjennomføre forskning.[3]

- *Skjermingsverdig FoU*: er ugradert. Vi har valgt å definere dette som at kunnskapen i forskningen er unntatt offentlighet og underlagt eksportkontrollregelverket.

Vi oppfatter de definerte begrepene ovenfor som generelle og gyldige for all FoU. Det spesielle her er at både forvaltningsinfrastrukturen, den generiske IT-støtten for FoU og bruken av forskningsinfrastruktur skal kunne håndtere gradert informasjon.

Forståelse og avgrensning av oppdragets del 2d

Vår forståelse av oppdraget er at det handler om hvordan øke kapasiteten på forsvarsrelatert forskning ved å inkludere forskningsinstitusjoner som i dag vanligvis ikke forholder seg til gradert informasjon. Oppdragets del 2d handler om prissetting av infrastruktur som er «nødvendig for å understøtte et nasjonalt forskningssystem for åpen, skjermingsverdig og gradert FoU». Det omfatter både forvaltningsinfrastruktur, generisk IT-støtte for FoU-samhandling og forskningsinfrastruktur – slik disse begrepene er definert ovenfor.

Vi har valgt følgende utgangspunkt for estimatene våre:

1. Dagens infrastruktur kan benyttes til (ugradert) skjermingsverdig forskning, og skjermingsverdighet vil ikke føre til ekstra kostnader til infrastruktur.

2. Kostnader for å kunne håndtere gradert informasjon i en forvaltningsinfrastruktur tilsvarer Forskningsrådets infrastruktur.

3. Da man ikke ennå har fått klargjort hva slags og hvor omfattende økt forskning som anbefales, har vi valgt å se på «stykkpris» for infrastruktur til et typisk forskningsmiljø. Stykkpris er estimert for hva det vil koste å inkludere én forskergruppe på ti ansatte i en forskningsinstitusjon som i dag ikke har systemer for å håndtere gradert informasjon, i et FoU-samarbeid med aktører som har systemer for å håndtere dette. Forskergruppens bruk av forskningsinfrastruktur vil normalt omfatte både IT-systemer og annet vitenskapelig utstyr, avhengig av aktuell FoU. Fordi omfanget av forskningsinfrastruktur varierer betydelig avhengig av FoU-en, har vi i kostnadsoverslagene bare omfattet IT-utstyr. IT-utstyr er dermed en minimumsinvestering.

Merk at punkt 3 i noen grad er generisk i den forstand at det skalerer med antallet aktører som inkluderes i FoU-samarbeidet. Samtidig må vi ta høyde for at ulike forskningsinfrastrukturer vil fordre ulike behov for investeringer for å kunne brukes i gradert forskning. Et viktig element tilknyttet dette er at (så å si) all moderne forskningsinfrastruktur produserer store datamengder som må kunne bearbeides og (deretter)

[2] Merk at definisjonen ikke er knyttet til hvilken aktør som forvalter midlene og utlysningene. Det behøver med andre ord ikke å være Norges forskningsråd.
[3] Denne definisjonen ligger tett opp til den Forskningsrådet bruker i sine utlysninger av midler til forskningsinfrastruktur, se siden «Eligible for funding 2023» på forskningsradet.no. Eneste forskjell fra Forskningsrådets definisjon er at sistnevnte inneholder adjektiver knyttet til størrelse på infrastrukturen («avansert vitenskapelig utstyr» og «store utstyrsfasiliteter»). Dette er fordi Forskningsrådets infrastrukturutlysninger er rettet mot større, nasjonale investeringer og norsk deltagelse i store, internasjonale infrastruktursamarbeid.

deles digitalt. I vår kontekst kan dette by på særskilte utfordringer siden forskningsinfrastrukturenes digitale systemer i hovedsak er designet for stor grad av åpenhet.[4]

Ytterligere avgrensninger og forutsetninger

- For investeringer ser vi kun på infrastruktur og ikke de menneskelige ressurser som kreves. For gradert arbeid på nivå BEGRENSET kreves autorisering, og på høyere nivå kreves både sikkerhetsklarering og autorisering. Videre kreves etablering av en sikkerhetsorganisasjon, opplæring av autoriserte i håndtering av gradert materiale og en endret sikkerhetskultur fra åpenhet og publisering til sikkerhetsmessig forsvarlig håndtering av informasjon og utstyr. Denne menneskelige innsatsen krever tid og et nytt «mindset». Å etablere gradert IT-infrastruktur vil kreve mer kapasitet og ny kompetanse av den lokale IT-enheten, og dette er inkludert i kostnadsestimatene for drift av systemer.
- Den generiske IT-støtten trenger ikke være direkte påkoplet forskningsinfrastrukturen som benyttes ved gjennomføringen av FoU-en.
- Forskningsrådet håndterer i dag kun bidragsforskning. Det er antatt at oppdragsforskning ikke gir mer kostnader for infrastruktur enn bidragsforskning.
- Kostnader til klarering av personell (som tilfaller klareringsmyndighetene) er ikke tatt med i regnestykket.
- Et eventuelt behov for nettverkskabler inn til forskningsmiljøet er ikke tatt med i estimatene. Dette gjelder først og fremst for nasjonalt hemmelig nett. Lengde og grunnforhold vil påvirke kostnaden såpass mye at det ikke er hensiktsmessig å gi et estimat.
- Alle kostnadene er basert på 2024-kroner.

Gradering

Informasjon skal sikkerhetsgraderes dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. Vi legger til grunn at det er to relevante sikkerhetsgraderinger for dette oppdraget: BEGRENSET (B) og HEMMELIG (H).

Disse to nivåene er valgt fordi infrastruktur for disse to nivå er mest utbredt. Av disse to er BEGRENSET det klart vanligste.

[4] Forskningsinstitusjoners forskningsinfrastruktur anvendes også i oppdragsforsking gjennomført av institutter og universiteter for næringslivet, der dataene og analysene ofte ikke skal deles med aktører som ikke tar del i oppdraget. Men selv om dataene og analysene anses som «bedriftsinterne», er de (normalt) ikke graderte og dermed ikke underlagt samme regelverk som det som gjelder for gradert informasjon.

Investeringer i forvaltningsinfrastruktur

Forskningsforvaltning det må legges til rette for

Det trengs infrastruktur der forvaltning med en ansvarlig aktør vurderer søknader med skjermingsverdig eller gradert innhold i egne utlysninger, ofte finansiert av Forsvarsdepartementet (FD), muligens med begrensing når det gjelder hvilke institusjoner som kan søke.

Besvarelsen av oppdragets del 1 (innretning og behov) vil gi føringer for besvarelsen av del 2 (konsekvenser og forutsetninger). Derfor gir vi et mer nyansert svar på del 2 i besvarelsen 31. mai 2024.

Muligheter innenfor dagens rammer

Forskningsrådet har en velfungerende forvaltningsinfrastruktur (for tildelinger, prosjektsøknader, oversikt osv.) som fungerer godt for åpen FoU. Alle forskningsinstitusjoner kan søke om midler gjennom denne løsningen. Dagens system kan brukes til åpen eller ugradert skjermingsverdig FoU. FD kan tilsvarende tildele åpne og ugradert skjermingsverdige oppdrag direkte til flere aktører enn i dag. Avhengig av hvor godt sikrede IT-systemer aktuelle FoU-virksomheter har, kan det være behov for investeringer i forbedret sikkerhet i eksisterende infrastruktur for skjermingsverdig FoU.

Det ligger i sakens natur at en betydelig andel av FoU innen forsvar og samfunnssikkerhet blir gradert. Vi kan likevel forestille oss at Forsvaret og andre aktører innenfor sikkerhet og beredskap i større grad enn i dag søker samarbeid med forskningsinstitutter og universiteter som vanligvis ikke håndterer gradert informasjon, da primært innenfor problemstillinger som isolert sett ikke er graderte. Vi ser også eksempler på samarbeid gradert-ugradert, i betydningen at ugraderte data fra akademia bearbeides gradert ved FFI .

Det er imidlertid fare for at denne typen samarbeid vil kunne gi begrenset utbytte dersom man ikke har mulighet til å jobbe gradert.

Det er mulig for FD å gi flere oppdrag på graderingsnivå BEGRENSET til virksomheter som i dag *har* graderte systemer. Disse virksomhetene kan da få lokale kostnader dekket gjennom indirekte kostnader. En utfordring er at man slik ikke vil ha en koordinert eller samlet oversikt over gradert og ugradert FoU.

Innenfor dagens rammer kan økt aktivitet og samarbeid skje ved lån av og tilgang til andres forskningsinfrastruktur. I et slikt tilfelle er det mest aktuelt at sivile institusjoner uten graderte systemer får tilgang til andres graderte forskningsinfrastruktur. Eksempelvis ved at et universitetsinstitutt får tilgang til FFI.

En slik tilgang vil kreve sikkerhetsklarering og autorisering av aktuelt personell fra universitetsinstituttet. Videre krever det at FFI har ledig kapasitet i sin forskningsinfrastruktur. Per i dag har FFI ikke ledig kapasitet, verken ved laboratorier eller kontorer, slik at dette dessverre ikke er gjennomførbart. Vi kjenner ikke til andre graderte forskningsinstitusjoner som kan stille forskningsinfrastruktur til rådighet for nye forskningsmiljøer. For å få til mer gradert forskning, er det derfor nødvendig med økte rammevilkår.

Gradert informasjon krever investeringer i håndtering av informasjonen i en forvaltningsinfrastruktur, i generisk IT-støtte og i forskningsinfrastruktur. Forskningsrådet, FFI og andre FoU-virksomheter har ikke satt av midler til å finansiere nye graderte løsninger.

Muligheter innenfor en moderat økning i rammevilkår

Forsvarssektoren har to systemer som behandler skjermingsverdig og gradert informasjon opp til BEGRENSET: FIS Basis B og FIS Basis H. Disse kommuniserer kun med etatene innenfor forsvarssektoren. Nasjonalt begrenset nett (NBN) kan kommunisere med andre relevante fagmiljøer som har behov for å

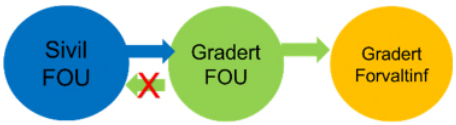
håndtere skjermingsverdig og gradert informasjon. FIS Basis B og NBN kan kommunisere med hverandre. I dag er NBN allerede etablert i noen virksomheter i forsvarsindustrien og enheter under Kunnskapsdepartementet, som Forskningsrådet. FD IT har en etablert leveransemodell av NBN som inkluderer godkjenning av installasjonen. Vi mener derfor at «gjenbruk» av NBN vil være kostnads- og tidseffektivt til bruk for forvaltningsinfrastruktur og generisk IT-støtte for FoU.

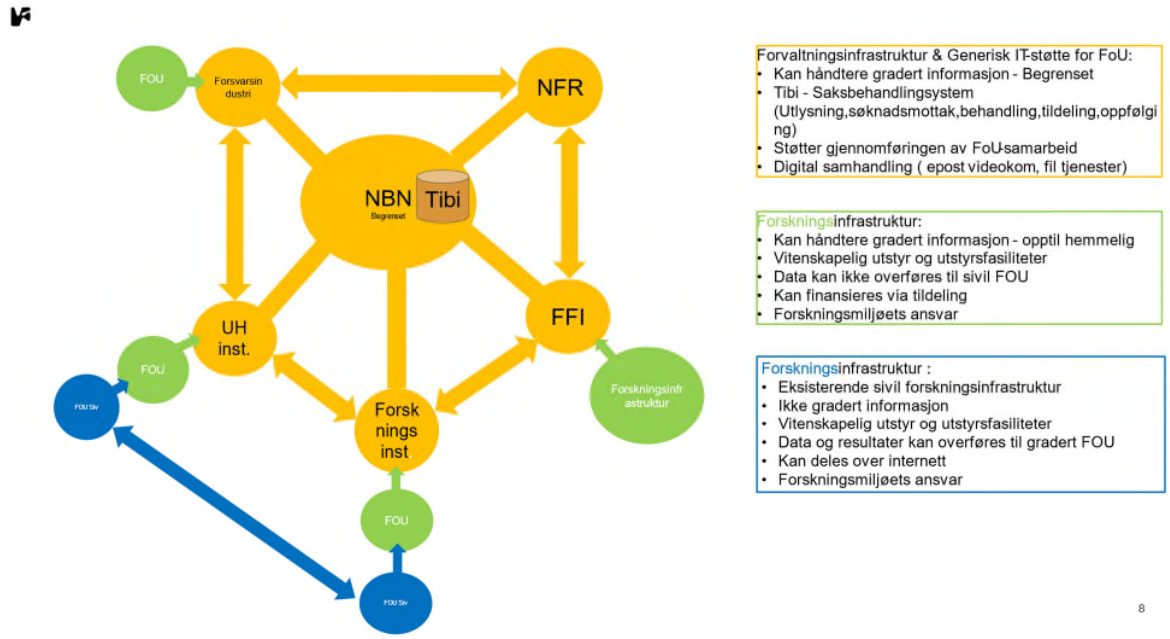
Videre foreslår vi å etablere en modifisert og forenklet utgave av Forskningsrådets forvaltningssystem (Tibi) på NBN. Forvaltningssystemet Tibi har de siste årene blitt forbedret i en ny utgave, der det har blitt lagt vekt på ny teknologi og effektivisering, samtidig som det ivaretar 30 års erfaring på tilskuddsforvaltning og prosessene rundt dette. Vi mener derfor at «gjenbruk» av Tibi vil være kostnads- og tidseffektivt til bruk som forvaltningssystem.

Arbeidsgruppen har holdt møter med driftsansvarlige for NBN, altså FD IT, og de stiller seg positive til den løsningen som er foreslått.

Import av data til NBN skjer i dag kun per e-post. Det kan bli behov å investere i en ny løsning for å håndtere større datamengder. En slik investering er ikke kostnadsestimert.

Vi mener også at man kan utnytte dagens sivile forskningsinfrastruktur ved å importere data fra disse miljøene inn i den graderte forskningsinfrastrukturen. Dataflyt kan imidlertid ikke gå andre veien, fra graderte til ugraderte systemer. Informasjonsflyten blir da som dette:





En utfordring med å samle informasjon om alle FoU-prosjekter på ett sted, i Tibi, er at summen av mange rapporter og mye informasjon gradert BEGRENSET vil kunne få en høyere gradering. Ekstra kostnader knyttet til å håndtere dette er ikke tatt med i de videre estimatene.

Forvaltningsinfrastruktur og generisk IT-støtte for FoU – sentral kostnad

Forvaltningsinfrastruktur kan også brukes til generisk IT-støtte.

Kostnadsestimatet er beregnet ut ifra erfaringstall fra investering og drift av dagens forvaltningssystem ved Norges forskningsråd.

Tabell 1. Investering i forvaltningsinfrastruktur til NBN (utlysning, søknadsmottak, behandling, tildeling av midler og oppfølging)

Kalkyle	Tillegg	Kostnad	Mva.	Kostnad inkl. mva.	Kommentar
Etablering av forvaltningssystem på NBN:		10 000 000	2 500 000	12 500 000	Tilpasning av forvaltnings-systemet
Tilpasning av ugraderte lokaler til BEGRENSET		2 500 000	625 000	3 125 000	Se behov for fysisk sikkerhet
Sum investeringer:		12 500 000	3 125 000	15 625 000	
Forventet tillegg	20 %	2 500 000	625 000	3 125 000	
Forventet prosjektkostnad (P50)		**15 000 000**	**3 750 000**	**18 750 000**	
Usikkerhetsavsetning	40 %	6 000 000	1 500 000	7 500 000	
Kostnadsramme (P85)		**21 000 000**	**5 250 000**	**26 250 000**	

Investering i sentral forvaltningsinfrastruktur er estimert til 15 mill. kroner ekskl. mva. De største risikoene knyttet til å estimere kostnader er endring i markedspriser, omfang av tiltak på bygg, kompleksitet i utvikling av forvaltningssystem på NBN og tilgang på klarerte ressurser for å implementere, drifte og bruke NBN.

Tabell 2. Drift av forvaltningsinfrastruktur og generisk IT-støtte til NBN

Kalkyle	***Kostnad***	***Mva.***	***Kostnad inkl. mva.***	***Kommentar***
Årlige lisenskostnader	1 000 000	250 000	1 250 000	
Forvaltning av system	3 000 000	750 000	3 750 000	IT-ressurser
Årlige driftskostnader	1 000 000	250 000	1 250 000	
Sum drift:	**5 000 000**	**1 250 000**	**6 250 000**	

Årlige driftskostnader er estimert til 5 mill. kroner ekskl. mva. Den største usikkerheten knytter seg til forvaltning av systemet. I starten kan det ta lengre tid og koste mer enn estimert å få forvaltningsinfrastrukturen til å fungere etter formålet.

Forvaltningsinfrastruktur og generisk IT-støtte for FoU – lokal kostnad hos FoU

Kostnadene for å etablere NBN ved nye forskningsmiljøer er basert på priser innhentet fra FD IT og erfaringstall fra implementering av NBN hos Forskningsrådet i 2022.

Tabell 3. Investering per nytt forskningsmiljø

Kalkyle	Tillegg	Kostnad	Mva.	Kostnad inkl. mva.	Kommentar
Etablering av NBN per forskningsmiljø		500 000	125 000	625 000	Inkl. utstyr, klient, printer osv.
Ressurser for å implementere NBN		1 200 000	300 000	1 500 000	2 ressurser i 3 måneder
Tilpasning av ugraderte lokaler til BEGRENSET		2 100 000	525 000	2 625 000	Se behov for fysisk sikkerhet
Sum investeringer:		3 800 000	950 000	4 750 000	
Forventet tillegg	21 %	800 000	200 000	1 000 000	
Forventet prosjektkostnad (P50)		**4 600 000**	**1 150 000**	**5 750 000**	
Usikkerhetsavsetning	43 %	2 000 000	500 000	2 500 000	
Kostnadsramme (P85)		**6 600 000**	**1 650 000**	**8 250 000**	

Erfaringstall fra forsvarssektoren tilsier et behov for å investere i ugraderte arealer på mellom 8 000 og 12 000 kroner per kvadratmeter for å ivareta kravene opp til BEGRENSET. Eksempelvis vil 10 arbeidsplasser med 21 kvadratmeter per arbeidsplass (forsvarssjefens normtall) og en gjennomsnittlig kvadratmeterpris på 10 000 kr gi en estimert kostnad på 2,1 mill. kroner ekskl. mva. Investeringen kan gjøres betydelig rimeligere hvis forskningsinstitusjonen eier eller leier hele bygget eller kontorplassene kan plasseres i en kjeller eller i etasjer uten innsyn. Da kan det være tilstrekkelig å investere i dørlåser inn til de graderte lokalene og noen mindre tilpasninger. Estimert kostnad på en slik løsning er på 400 000 kroner ekskl. mva.

Investering i forvaltningsinfrastruktur er estimert til en forventet prosjektkostnad på 4,6 mill. kroner ekskl. mva. per nytt forskningsmiljø.

Tabell 4. Drift av forvaltningssystemet og generisk IT-støtte

Kalkyle	***Kostnad***	***Mva.***	***Kostnad inkl. mva.***	***Kommentar***
Årlige lisenskostnader	500 000	125 000	625 000	
Forvaltning av system	1 500 000	375 000	1 875 000	IT-ressurs til å drifte løsningen
Årlige driftskostnader	500 000	125 000	625 000	
Sum drift:	**2 500 000**	**625 000**	**3 125 000**	

Årlige driftskostnader er estimert til 2,5 mill. kroner ekskl. mva. per nytt forskningsmiljø. Da er det tatt høyde for behov for både økt kompetanse og økt kapasitet hos IT-enheten.

Oppsummert: investeringer i forvaltningsinfrastruktur og generisk IT-støtte

Tabell 5. Årlige kostnader sentralt og lokalt de neste 4 årene ved 10 nye forskningsmiljøer

Kalkyle	***Kostnad***	***Mva.***	***År 1***	***År 2***	***År 3***	***År 4***
Investeringer sentralt	15 000 000	3 750 000	18 750 000			
Investeringer lokalt	46 000 000	11 500 000	57 500 000			
Drift sentralt	5 000 000	1 250 000	6 250 000	6 250 000	6 250 000	6 250 000
Drift lokalt	25 000 000	6 250 000	31 250 000	31 250 000	31 250 000	31 250 000
Sum drift:	**91 000 000**	**22 750 000**	**113 750 000**	**37 500 000**	**37 500 000**	**37 500 000**

Samlet investeringsbehov sentralt og lokalt for 10 nye forskningsmiljøer er estimert til 61 mill. kroner ekskl. mva. og 76 mill. kroner inkl. mva. Årlige driftskostnader er estimert til 30 mill. kroner ekskl. mva. og 37,5 mill. kroner inkl. mva.

Tabell 6. Årlige kostnader sentralt og lokalt de neste 4 årene ved 20 nye forskningsmiljøer

Kalkyle	***Kostnad***	***Mva.***	***År 1***	***År 2***	***År 3***	***År 4***
Investeringer sentralt	15 000 000	3 750 000	18 750 000			
Investeringer lokalt	92 000 000	23 000 000	115 000 000			
Drift sentralt	5 000 000	1 250 000	6 250 000	6 250 000	6 250 000	6 250 000
Drift lokalt	50 000 000	12 500 000	62 500 000	62 500 000	62 500 000	62 500 000
Sum drift:	**162 000 000**	**40 500 000**	**202 500 000**	**68 750 000**	**68 750 000**	**68 750 000**

Samlet investeringsbehov sentralt og lokalt for 20 nye forskningsmiljøer er estimert til 107 mill. kroner ekskl. mva. og 134 mill. kroner inkl. mva. Årlige driftskostnader er estimert til 55 mill. kroner ekskl. mva. og 68,75 mill. kroner inkl. mva.

Anbefalt løsning er i første fase å gjøre NBN tilgjengelig til et antall nye forskningsmiljøer. Som eksempel vil investeringskostnaden sentralt og lokalt for 10 nye forskningsmiljøer være estimert til 76 mill. kroner inkl. mva. og en årlig driftskostnad på 37,5 mill. kroner inkl. mva.

Et optimalt alternativ

Hva som er innholdet i det beste, «optimale» alternativet for å møte økt kunnskapsbehov, er egentlig ikke vurdert innenfor fristen for denne rapporten. Det vil vi komme tilbake til i oppdaterte vurderinger til 31. mai 2024. Fordi denne første delleveransen handler om nødvendige investeringer med tilhørende kostnader, har vi sett på hva som kan være både kostnadsdrivende og nyttig.

I tillegg til investeringene som er beskrevet under moderat økning i rammevilkår, inkluderer et optimalt alternativ muligheter for å kunne håndtere informasjon på graderingsnivået HEMMELIG. Alternativet kan også omfatte flere aktører på BEGRENSET, men her er HEMMELIG valgt fordi forskning innen forsvar ofte trenger ytterligere beskyttelse, og fordi infrastruktur på HEMMELIG er kostnadsdrivende.

Nærmere drøfting av ulike alternativer overlates til neste levering i mai.

På graderingsnivået HEMMELIG vil det være streng tilgangsstyring for hvem som kan få informasjon om forskningen, og derfor legger vi til grunn at FoU-midler ikke settes ut på konkurranse, men tildeles direkte. Det innebærer at vi ikke trenger en omfattende forvaltningsinfrastruktur, men har behov for samhandling mellom oppdragsgivere og aktuelle FoU-virksomheter.

Bruk av nasjonalt hemmelig nett (NHN) ligger til grunn for dette alternativet. Teknologien for NHN er under utvikling og er ikke ferdig rullet ut per i dag.

Forvaltningsinfrastruktur og generisk IT-støtte for FoU – sentral kostnad

Kostnadsestimatet er usikkert og tar utgangspunkt i erfaringstall fra investering og drift av dagens forvaltningssystem ved Norges forskningsråd.

Tabell 7. Investering i forvaltningsinfrastruktur og generisk IT-støtte, NHN

Kalkyle	Tillegg	Kostnad	Mva.	Kostnad inkl. mva.	Kommentar
Etablering av forvaltningssystem på NHN:		10 000 000	2 500 000	12 500 000	Tilpasning av forvaltnings-systemet
Tilpasning av ugraderte lokaler til HEMMELIG		15 000 000	3 750 000	18 750 000	Se behov for fysisk sikkerhet
Sum investeringer:		25 000 000	6 250 000	31 250 000	
Forventet tillegg	20 %	5 000 000	1 250 000	6 250 000	
Forventet prosjektkostnad (P50)		**30 000 000**	**7 500 000**	**37 500 000**	
Usikkerhetsavsetning	60 %	18 000 000	4 500 000	22 500 000	
Kostnadsramme (P85)		**48 000 000**	**12 000 000**	**60 000 000**	

Investeringskostnaden til forvaltningsinfrastruktur er estimert til 30 mill. kroner ekskl. mva. De største risikoene knytter seg til estimering av kostnader knyttet til omfanget av tiltak på bygg og annen infrastruktur, endring i markedspriser og tilgang på klarerte ressurser for å implementere, drifte og bruke NHN. Det er høy usikkerhet knyttet til investeringskostnaden, og usikkerhetsavsetningen settes derfor til 60 %.

Tabell 8. Drift av forvaltningsinfrastruktur og generisk IT-støtte, NHN

Kalkyle	*Kostnad*	*Mva.*	*Kostnad inkl. mva.*	*Kommentar*
Årlige lisenskostnader	1 000 000	250 000	1 250 000	
Forvaltning av system	4 000 000	1 000 000	5 000 000	IT-ressurser
Årlige driftskostnader	5 000 000	1 250 000	6 250 000	Inkl. behov for økt sikkerhet
Sum drift:	**10 000 000**	**2 500 000**	**12 500 000**	

Årlige driftskostnader er estimert til 10 mill. kroner ekskl. mva. Det er tatt høyde for behov for både økt kompetanse og økt kapasitet hos IT-enheten. Den største usikkerheten knytter seg til når NHN er ferdig testet og klar for utrulling.

Forvaltningsinfrastruktur og generisk IT-støtte for FoU – lokal kostnad

Kostnadene for å etablere NHN på nye forskningsmiljøer er basert på estimat innhentet fra FD IT.

Tabell 9. Investering per nytt forskningsmiljø

Kalkyle	**Tillegg**	**Kostnad**	**Mva.**	**Kostnad inkl. mva.**	**Kommentar**
Etablering av NHN per forskningsmiljø		1 000 000	250 000	1 250 000	Inkl. utstyr, klient, VC, printer osv.
Ressurser for å implementere NHN		3 600 000	900 000	4 500 000	2 ressurser i 8 måneder
Tilpasning av ugraderte lokaler til HEMMELIG		8 400 000	2 100 000	10 500 000	Fysisk sikkerhet
Sum investeringer:		13 000 000	3 250 000	16 250 000	
Forventet tillegg	20 %	2 600 000	650 000	3 250 000	
Forventet prosjektkostnad (P50)		**15 600 000**	**3 900 000**	**19 500 000**	
Usikkerhetsavsetning	60 %	9 400 000	2 350 000	11 750 000	
Kostnadsramme (P85)		**25 000 000**	**6 250 000**	**31 250 000**	

Investeringskostnaden er estimert til 15,6 mill. kroner per nytt forskningsmiljø. Det er høy usikkerhet knyttet til investeringskostnaden, og usikkerhetsavsetningen er derfor satt til 60 %. NHN er ikke rullet ut per i dag, og vi har derfor ingen erfaringstall for hva dette kan komme til å koste.

Erfaringstall fra forsvarssektoren tilsier et behov for å investere i eksisterende arealer for mellom 30 000 og 50 000 kroner per kvadratmeter for å ivareta kravene opp til HEMMELIG. 10 arbeidsplasser med 21 kvadratmeter per arbeidsplass og en gjennomsnittlig kvadratmeterpris på 40 000 kroner gir en estimert kostnad på 8,4 mill. kroner ekskl. mva.

Investeringen kan gjøres noe lavere (20–30 %) hvis forskningsinstitusjonen har en god perimetersikring eller døgnkontinuerlig vaktordning.

Tabell 10. Drift av forvaltningssystemet og generisk IT-støtte

Kalkyle	***Kostnad***	***Mva.***	***Kostnad inkl. mva.***	***Kommentar***
Årlige lisenskostnader	500 000	125 000	625 000	
Forvaltning av system	2 000 000	500 000	2 500 000	IT-ressurs til å drifte løsningen
Årlige driftskostnader	5 000 000	1 250 000	6 250 000	Inkl. behov for økt sikkerhet
Sum drift:	**7 500 000**	**1 875 000**	**9 375 000**	

Årlige driftskostnader er estimert til 7,5 mill. kroner ekskl. mva. per nytt forskningsmiljø.

Oppsummert: investeringer i forvaltningsinfrastruktur og generisk IT-støtte

Tabell 11. Årlige kostnader sentralt og lokalt de neste 4 årene ved 10 nye forskningsmiljøer

Kalkyle	***Kostnad***	***Mva.***	***År 1***	***År 2***	***År 3***	***År 4***
Investeringer sentralt	30 000 000	7 500 000	37 500 000			
Investeringer lokalt	156 000 000	39 000 000	195 000 000			
Drift sentralt	10 000 000	2 500 000	12 500 000	12 500 000	12 500 000	12 500 000
Drift lokalt	75 000 000	18 750 000	93 750 000	93 750 000	93 750 000	93 750 000
Sum drift:	**271 000 000**	**67 750 000**	**338 750 000**	**106 250 000**	**106 250 000**	**106 250 000**

Anbefalt løsning er i første fase å tilgjengeliggjøre NHN til 10 nye forskningsmiljøer. Dette vil ha en estimert investeringskostnad sentralt og lokalt på 233 mill. kroner inkl. mva. og en årlig driftskostnad på 106 mill. kroner inkl. mva.

Investeringer i forskningsinfrastruktur

Hva slags forskningssamarbeid bør det legges til rette for?

Som beskrevet over vil NBN-plattformen som forvaltningsinfrastruktur også kunne benyttes til FoU-samhandling («generisk IT-støtte».)

Praktisk kan økt forskningssamarbeid skje ved

a) utveksling, deling og samling av data eller forskningsresultater, og analyser;
b) lån av og tilgang til forskningsinfrastruktur;
c) spesielle samarbeidslinjer med felles forskningsinfrastruktur. Det kan tenkes situasjoner der NBN ikke er et kraftig nok samhandlingsverktøy, grunnet behov for eksempelvis datautvekslinger mellom to forskningsvirksomheter hvor datamengden er for omfattende for NBN. Da kan det være aktuelt med enkelte spesielle samarbeidslinjer med felles forskningsinfrastruktur.

Den samme IT-infrastrukturen som vi foreslår å etablere for forvaltningsinfrastruktur, kan altså også benyttes som generisk IT-støtte for FoU i felles forskningsprosjekter. For forskningsanalyser og generering av forskningsresultater forutsetter vi imidlertid at dette må gjøres på egne IT-enheter fordi FoU gjerne innebærer programvare og applikasjoner av en art som ikke kan tillates på for eksempel NBN eller FIS Basis B. Til dette legger vi til grunn at det benyttes enkeltstående pc-er. Hvilket labutstyr og fasiliteter som trengs, avhenger av og varierer betydelig med type FoU. Dette har vi per nå definert ut av omfanget for denne rapporten og må se på senere.

På graderingsnivå HEMMELIG er forskningssamarbeid prinsipielt likt med BEGRENSET, men med færre aktører og mer tilgangsstyring.

Muligheter innenfor en moderat økning i rammevilkår

For en moderat økning har vi lagt til grunn bruk av forskningsinfrastruktur gradert BEGRENSET i et utvalgt antall forskningsmiljøer. Kostnadsestimatet er for ett nytt forskningsmiljø.

Etablering av IT-utstyr (PC, skjermer, mus og kabler) for forskning på nivå BEGRENSET er estimert til 50 000 kroner per kontorplass. Vi legger til grunn et forskningsmiljø med 10 ansatte, altså 500 000 kroner for et forskningsmiljø. Hvor mange slike forskningsmiljøer det er behov for, er ikke vurdert.

Mer avansert enkeltstående IT-utstyr i FoU for å bearbeide store datamengder koster fra 100 000 kroner og oppover.

Etablering av et nytt laboratorium varierer betydelig i kostnad, og de siste laboratoriene på FFI har en kvadratmeterpris på mellom 70 000 og 250 000 kroner ekskl. mva. per kvadratmeter. Inkludert i dette beløpet er mellom 15 og 25 prosent til inventar og spesialinstrumenter. Et nytt laboratorium til gradert nivå BEGRENSET estimeres til 125 000 kroner per kvadratmeter. For 200 kvadratmeter blir kostnaden derfor 25 mill. kroner ekskl. mva.

Oppsummert vil investeringer i forskningsinfrastruktur minimum bestå i IT-utstyr til 600 000 kroner for et forskningsmiljø. Mer kostnadsdrivende er imidlertid lokaler og laboratorieutstyr, som her ikke er estimert fordi det avhenger av hvilken FoU som er aktuell.

Et optimalt alternativ

For en moderat økning har vi lagt til grunn bruk av infrastruktur gradert HEMMELIG på et utvalgt antall forskningsmiljøer. Dette i tillegg til investering på moderat nivå. Konstandsestimatet er for ett forskningsmiljø.

Etablering av IT-utstyr (PC, skjermer, mus og kabler) for forskning på nivå HEMMELIG er estimert til 60 000 kroner per kontorplass. Med 10 ansatte utgjør dette 600 000 kroner for et forskningsmiljø. Vi har ikke relevante oppdaterte erfaringstall for avanserte enkeltstående IT-utstyr til HEMMELIG. Vi anbefaler å legge til grunn en snittpris på 150 000 kroner ekskl. mva.

Etablering av et nytt laboratorium varierer betydelig i kostnad, og de siste laboratoriene på FFI har en kvadratmeterpris på mellom 70 000 og 250 000 kroner ekskl. mva. per kvadratmeter. Inkludert i dette beløpet er mellom 15 og 25 prosent til inventar og instrumenter. Med en snittpris på 250 000 kroner per kvadratmeter og et nytt laboratorium på 200 kvadratmeter er kostnaden estimert til 50 mill. kroner ekskl. mva.

Utrulling av NHN bør kun gjøres til de forskningsinstitusjonene som forventes å kunne bidra med høy nytteverdi.

Oppsummert vil investeringer i forskningsinfrastruktur minimum bestå i IT-utstyr til 750 000 kroner for et forskningsmiljø. Betydelig mer kostnadsdrivende er imidlertid lokaler og laboratorieutstyr, som ikke er estimert her fordi det avhenger av hvilken FoU som er aktuell.

Kort om forutsetninger for gradert FoU

Graderingsnivå

Informasjon skal sikkerhetsgraderes dersom det kan skade nasjonale sikkerhetsinteresser[5] om den blir kjent for uvedkommende.

- BEGRENSET – dersom det i noen grad kan få skadefølger
- KONFIDENSIELT – dersom det kan få skadefølger
- HEMMELIG – dersom det kan få alvorlige skadefølger
- STRENGT HEMMELIG - dersom det kan få svært alvorlige skadefølger

Dette står i sikkerhetsloven § 5-3.

Definisjonene legger opp til en stor grad av tolkning og er derfor fulgt opp av en rekke bestemmelser, veiledninger og råd.

Bruk av graderte IT-systemer krever at IT-systemene godkjennes av NSM, at lokalene hvor disse benyttes, er godkjent, og at personell er sikkerhetsklarert av myndighetene og/eller autorisert lokalt. Dette er nærmere beskrevet nedenfor.

Godkjenning av IT-systemer

NSMs veiledere på området gir detaljerte føringer på hva som må gjennomføres for å godkjenne informasjonssystemer.

En av svakhetene med de fleste veiledningene er at de forutsetter at virksomheten er underlagt sikkerhetsloven eller på en annen måte er kjent med håndtering av gradert informasjon eller graderte systemer.

Det er ingen vesentlig forskjell når det gjelder IT-arkitektur for forskjellige graderingsnivåer, men det kan være forskjellige prosesser, og det er forskjell på krav til tekniske sikkerhetstiltak.

Fysisk sikkerhet

Fysisk sikkerhet omfatter følgende:

- inndeling av fysiske soner i kontrollert, beskyttet og sperret område
- krav til sikring av de ulike områdene
- krav til oppbevaring for gradert informasjon
- krav til dører og låser
- krav til vakthold og elektroniske sikringstiltak

[5] Sikkerhetsloven § 1-5 definerer nasjonale sikkerhetsinteresser som: landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til

a) de øverste statsorganers virksomhet, sikkerhet og handlefrihet
b) forsvar, sikkerhet og beredskap
c) forholdet til andre stater og internasjonale organisasjoner
d) økonomisk stabilitet og handlefrihet
e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

Det er vesentlige forskjeller på krav til BEGRENSET og til KONFIDENSIELT og høyere, og det er her de store kostnadene ofte vil være.

Personellsikkerhet

Sikkerhetsklarering er en avgjørelse tatt av klareringsmyndigheten om en persons antatte sikkerhetsmessige skikkethet for behandling av sikkerhetsgradert informasjon. Personer skal sikkerhetsklareres dersom de skal ha tilgang til informasjon gradert KONFIDENSIELT eller høyere.

Autorisasjon er godkjennelse fra virksomheten for å få tilgang til sikkerhetsgradert informasjon og adgang til skjermingsverdige objekter og infrastruktur. Der autorisasjon er et krav, skal sikkerhetsklarering være gjennomført før autorisasjon kan gis.

Organisatoriske forutsetninger for å håndtere gradert informasjon

Virksomhetsikkerhetsforskriften inneholder krav til virksomheter som omfattes av sikkerhetsloven. Dette er forutsetninger som må være på plass før virksomheten behandler gradert informasjon.

Kort oppsummert skal virksomheten gjøre følgende:

- legge frem informasjon om virksomheten og forretningsområder
- etablere styringssystem med forankring i organisasjonen, policy og roller
- etablere ressurser, kompetanse, bevisstgjøring, kommunikasjon og dokumentasjon
- avklare føringer for og etablere evne til risikovurdering og risikohåndtering på virksomhetsnivå
- etablere evne til å evaluere og kontinuerlig forbedre styringssystemet

Det er opp til virksomheten selv å fastsette hvordan den oppnår et forsvarlig sikkerhetsnivå gjennom organiseringen av det forebyggende sikkerhetsarbeidet.

Merk at dette kan føre til kostander og bør også inn i et kostnadsestimat.

Omfang av gradert informasjon

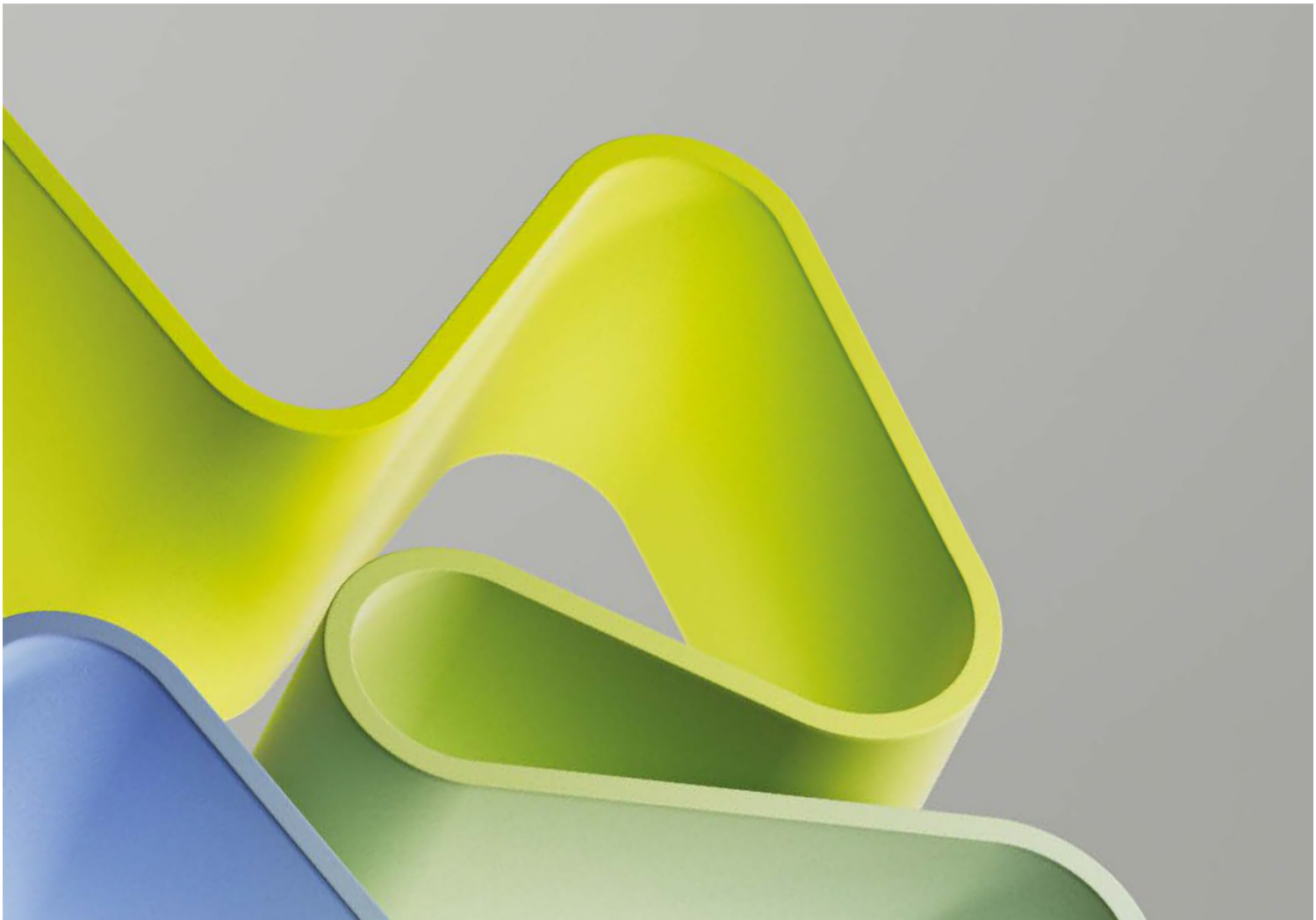
Verdivurdering og risikohåndtering kan konkludere med ekstra tiltak utover informasjonens graderingsnivå. En av de vanligste problemstillingene er omfanget av gradert informasjon. Dette gjelder generelt og er understreket i eksempelvis NATO Security Policy, som sier:

> When a large amount of NATO Classified information is collated together, the original security classification markings shall be retained, and that information shall be assessed for the impact its collective loss or compromise would have upon the organization. If this overall impact is assessed as being higher than the impact of the actual individual NATO security classification then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.

Norges forskningsråd
Besøksadresse: Drammensveien 288
Postboks 564
1327 Lysaker

Telefon: 22 03 70 00
Telefaks: 22 03 70 01

post@forskningsradet.no
www.forskningsradet.no



Vedlegg E: Økonomiske og administrative konsekvenser

Notatet vurderer økonomiske og administrative konsekvenser av ulike løsninger.

Beregningene i dette vedlegget er basert på relevante erfaringstall og har betydelige usikkerheter ved seg, men vil likevel gi en god pekepinn på hva overgangen fra åpen til skjermet til gradert FoU-aktivitet, -støtte og -forvaltning vil koste. Som tommelfingerregel kan vi si at man må beregne et påslag fra ugradert digital infrastruktur på minst 20 % for skjermingsnivå BEGRENSET, minst 40 % for skjermingsnivå KONFIDENSIELT og minst 60 % på skjermingsnivå HEMMELIG for digital infrastruktur.

Påslag for ulike oppgraderinger	Påslag % sats
Påslag for graderte nye kontorlokaler opp til B:	20 %
Påslag rehabilitering av kontorlokaler opp til B:	20 %
Påslag for gradert kontorlokaler opp til K:	40 %
Påslag rehabilitering av kontorlokaler opp til K:	40 %
Påslag for graderte nye kontorlokaler opp til H:	60 %
Påslag rehabilitering av kontorlokaler opp til H:	60 %

Tabell 1: Tillegg per kvadratmeter for kontorlokalers håndtering av nasjonalt begrenset nett hentet fra Forsvarsbyggs tidligfasekalkyler

Vi har ikke beregnet kostnader til faglig arbeid, fasilitering og bidrag fra relevante aktører (som NSM i forbindelse med rådgivning, autorisasjon, klarering, kontroll etc).

Vi har ikke beregnet kostnader for vitenskapelige årsverk.

1. Økonomiske og administrative konsekvenser av hvert anbefalte tiltak

Tiltak 1: Økt bruk av sivile forskningsmiljøer innenfor forsvar, sikkerhet og beredskap.[1] Et viktig element i dette er å etablere en systematikk for å identifisere flerbruksmuligheter (dual-use) og skjermet forskning.[2] I tillegg må antall forskningsutførende aktører som kan utføre gradert forskning øke noe.

For gradert arbeid på nivå BEGRENSET kreves autorisering, og på nivå KONFIDENSIELT eller høyere kreves både sikkerhetsklarering og autorisering.

[1] Med *sivile* forskningsmiljøer og det *sivile* forskningssystemet mener vi her de delene av forskningssystemet som normalt ikke arbeider med militære og/eller graderte problemstillinger.

[2] *Dual use can be defined as research conducted for legitimate purposes that generates knowledge, information, technologies, and/or products which could be utilized for both benevolent and harmful purposes.* På norsk kalles dette ofte for flerbruks*teknologi.* Men siden vi her tenker bredere enn "bare" teknologi, har vi valgt å oversette *dual use* med flerbruks*muligheter,* som for øvrig ligger tettere opp mot den engelske termen. Men også begrepet flerbruksteknologi er brukt i teksten der vi mener dette er mest dekkende.

Videre krever alt gradert arbeid etablering av en sikkerhetsorganisasjon, opplæring av autorisert personell i håndtering av gradert materiale og en endret sikkerhetskultur fra åpenhet og publisering til sikkerhetsmessig forsvarlig håndtering av informasjon, systemer og utstyr.

Denne menneskelige innsatsen krever tid og et nytt «mindset». Å etablere gradert IT-infrastruktur vil kreve mer kapasitet og ny kompetanse av den lokale IT-enheten ved institusjonene, og dette er inkludert i kostnadsestimatene for drift av systemer.

Kostnadene er basert på fiber hvor påkoblingspunkt ligger maks 100 meter fra nytt forskningsmiljø.

Ressurser:

- Sikkerhetsleder-/rådgiver
- IT-ressurs

Kostnader for etablering av nasjonalt begrenset nett (NBN) ved nye forskningsmiljøer er basert på priser innhentet fra Forsvarsdepartementets IT-avdeling og erfaringstall fra implementering av NBN hos Forskningsrådet i 2022.

Årlige driftskostnader er estimert til 4,25 mill. kroner per nyetablering av gradert forskning i tilknytning til eksisterende forskningsmiljøer.

Kalkyle	*Kostnad*	*Mva.*	*Kostnad inkl. mva.*	*Kommentar*
Årlige lisenskostnader	500 000	125 000	625 000	NBN - prisliste pr 2024
Årlige driftskostnader	500 000	125 000	625 000	
Sikkerhetsleder-/rådgiver[3]	1 500 000		1 500 000	1 årsverk[4]
IT-ressurs	1 500 000		1 500 000	1 årsverk til forvaltning av løsningen
Sum administrasjon og drift:	**4 000 000**	**250 000**	**4 250 000**	

Tabell 2: Drift av forvaltningssystemet og generisk IT-støtte

Forventet prosjektkostnad (P50) til investering i forvaltningsinfrastruktur er estimert til 5,75 mill. kroner per nyetablering i tilknytning til eksisterende forskningsmiljøer.

Kalkyle	*Tillegg*	*Kostnad*	*Mva.*	*Kostnad inkl. mva.*	*Kommentar*

[3] *Ikke medtatt i innspill 16. februar 2024 - Infrastruktur for et nasjonalt forskningssystem for åpen, skjermingsverdig og gradert FoU.*

[4] *Estimerte kostnader pr årsverk inkluderer lønn, sosiale kostnader (arbeidsgiveravgift og pensjon) og driftskostnader.*

Etablering av NBN per forskningsmiljø		500 000	125 000	625 000	Inkl. utstyr,
Ressurser for å implementere NBN		1 200 000	300 000	1 500 000	2 ressurser i 3 måneder
Tilpasning av ugraderte lokaler til BEGRENSET		2 100 000	525 000	2 625 000	Se behov for fysisk sikkerhet
Sum investeringer:		3 800 000	950 000	4 750 000	
Forventet tillegg	21 %	800 000	200 000	1 000 000	
Forventet prosjektkostnad (P50)		**4 600 000**	**1 150 000**	**5 750 000**	
Usikkerhetsavsetning	43 %	2 000 000	500 000	2 500 000	
Kostnadsramme (P85)		**6 600 000**	**1 650 000**	**8 250 000**	

Tabell 3: Investeringskostnader per nytt forskningsmiljø

Tiltak 2: Opprettelse av en ny portefølje i Forskningsrådet for å styrke forskning relevant for forsvar, sikkerhet og beredskap.

I beregningene under har vi ikke vurdert hvor stor porteføljen må være i form av midler til utlysninger (inntekter), men vil understreke at en forutsetning for at målene beskrevet i oppdraget skal oppnås er at finansieringen er tilstrekkelig og forutsigbar over tid.

Administrative roller som kreves for forvaltningsinfrastruktur og FoU på begrenset (NBN).

- Sikkerhetsleder
- Informasjonssystemsikkerhetsansvarlig
- Personellsikkerhetsansvarlig
- IT-ressurser
- Søknadsbehandlere
- Fag eksperter
- Porteføljestyre

Kostnadsestimatet er beregnet ut ifra erfaringstall fra investering og drift av dagens forvaltningssystem ved Forskningsrådet. Samlet er det estimert et behov for ca. 6 årsverk til å drifte løsningen og ca. 6 årsverk til behandling av de graderte søknadene.

Årlige administrasjon og driftskostnader er estimert til ca. 21,5 mill. kroner. pr år. Den største usikkerheten knytter seg til forvaltning av systemet. I starten kan det ta lengre tid og koste mer enn estimert for å få forvaltningsinfrastrukturen til å fungere etter formålet. Rekruttering av personell til forvaltning av løsningen og saksbehandling av søknadene kan ta lengre tid enn det som er norm for etablerte porteføljer med standard mandat.

Kalkyle	***Kostnad***	***Mva.***	***Kostnad inkl. mva.***	***Kommentar***
Årlige lisenskostnader	1 200 000	300 000	1 500 000	NBN - prisliste pr 2024
Sikkerhetsleder	1 500 000		1 500 000	1 årsverk

IT-sikkerhet	1 500 000		7 500 000	5 årsverk til forvaltning av løsningen
Søknadsbehandlere	1 500 000		7 500 000	5 årsverk til behandling av graderte søknader
Fageksperter og porteføljestyre (inkludert reiser og honorar)	100 000		3 500 000	25 ressurser til behandling av graderte søknader + porteføljestyre
Sum administrasjon og drift:			**21 500 000**	

Tabell 4. Drift av forvaltningsinfrastruktur, generisk IT-støtte til NBN, søknadsbehandlere, porteføljestyret og fageksperter

Forvaltningsinfrastruktur

Forventet prosjektkostnad (P50) til investering i sentral forvaltningsinfrastruktur er estimert til 18,75 mill. kroner. De største risikoene knyttet til å estimere investeringskostnadene er endring i markedspriser, omfang av tiltak på bygg, kompleksitet i utvikling av forvaltningssystem på NBN og tilgang på klarerte ressurser for å implementere, drifte og bruke NBN.

Kalkyle	Tillegg	Kostnad	Mva.	Kostnad inkl. mva.	Kommentar
Etablering av forvaltningssystem på NBN:		10 000 000	2 500 000	12 500 000	Tilpasning av forvaltnings - systemet
Tilpasning av ugraderte lokaler til BEGRENSET		2 500 000	625 000	3 125 000	Se behov for fysisk sikkerhet
Sum investeringer:		12 500 000	3 125 000	15 625 000	
Forventet tillegg	20 %	2 500 000	625 000	3 125 000	
Forventet prosjektkostnad (P50)		**15 000 000**	**3 750 000**	**18 750 000**	
Usikkerhetsavsetning	40 %	6 000 000	1 500 000	7 500 000	
Kostnadsramme (P85)		**21 000 000**	**5 250 000**	**26 250 000**	

Tabell 5. Investering i forvaltningsinfrastruktur til NBN (utlysning, søknadsmottak, behandling, tildeling av midler og oppfølging)

Tiltak 3: **Etablering av en arena for kunnskapssamarbeid innenfor forsvar, sikkerhet og beredskap.**

Kalkyler i tabellene over gjelder også for dette tiltaket. I tillegg beregner vi her kostnader og administrative behov hvis arenaen skal kunne håndtere informasjon og FoU på skjermingsnivå HEMMELIG. Vi forutsetter tilgang til nasjonalt hemmelig nett (NHN).

Estimerte kostnader ved å etablere og drifte helt nye og frittstående graderte arealer opp til HEMMELIG hvor forskningsmiljøene etter behov kan gjennomføre gradert forskning.

Ressurser:

- Sikkerhetsleder-/rådgiver
- Informasjonssikkerhetsansvarlig
- Personellsikkerhetsansvarlig
- Information Manager
- Vakt og resepsjon
- IT-ressurser

Investeringer i egnede lokaler med infrastruktur kan gjøres igjennom leie eller ved å investere i nye kontorer og laboratorier.

Følgende forutsetninger er lagt til grunn for kalkylen;

- Forsvarssjefens normtall på 21 kvadratmeter (m2) per kontorplass.
- 63 700,- kroner pr m2 for ugraderte arealer.
- + 60 prosent for investering i bygg og teknisk infrastruktur opp til HEMMELIG.
- 40 medarbeidere = 840 kvadratmeter.
- Etablering av et laboratorium på 800 kvadratmeter opp til nivå HEMMELIG.
- Årlige leiekostnader er estimert til 3 000,- inkl. mva. pr år.
- Årlige driftskostnader er estimert til 30 % av leiekostnaden.

Årlige driftskostnader er estimert til ca. 26 mill. kroner for nye arealer for gradert forskning. Kostnadene ved å etablere en ny arena i en organisasjon som allerede er godkjent for håndtering av gradert informasjon vil ha betydelig lavere kostnader (blant annet til vakt og sikring). Risikoen knytter seg blant annet til å få tak i riktig kompetanse til rett tid og lokaler som er egnet til å bygges om til ønsket graderingsnivå.

Kalkyle	*Kostnad*	*Mva.*	*Kostnad inkl. mva.*	*Kommentar*
Leie av kontorarealer (plass til 40 personer – 21 m^2 * 40 = 840 m^2)	2 400 pr m^2	600 pr m^2	2 520 000	
Leie av laboratorium arealer (800 m^2)	2 400 pr m^2	600 pr m^2	2 400 000	
Årlige lisenskostnader	1 000 000	250 000	1 250 000	NHN - prisliste pr 2024
Årlige driftskostnader	1 000 000	250 000	1 250 000	
Sikkerhetsleder-/rådgiver/ personellsikkerhetsansvarlig/ Information Manager	1 500 000		4 500 000	3 årsverk
Vakt og resepsjon	1 200 000		9 600 000	8 årsverk
IT-ressurser og informasjonssikkerhetsansvarlig	1 500 000		4 500 000	3 årsverk til forvaltning av løsningen
Sum administrasjon og drift:			**26 020 000**	

Tabell 6. Leie av arealer, sikker drift av forvaltningssystemet og vakt/resepsjon

Forventet prosjektkostnad (P50) til investering i forvaltningsinfrastruktur i leide lokaler for etablert av en ny forskingsarena er estimert til 87 mill. kroner. Etablering av et helt nytt gradert bygg opp til HEMMELIG vil ta 2 til 3 år og koste ca. 63 700 kr pr m2 * 1,6 * 1.640 * 1,2 (forventet tillegg) = ca. 200 mill. kroner. Investeringene kan gjøres rimeligere hvis forsknings-institusjonen eier eller leier hele bygget og/eller kontorplassene kan plasseres i etasjer uten innsyn og med tilstrekkelig sikkerhetsmessige avstander. Det er betydelig geografiske forskjeller i leiepriser og kostnader ved etablering av slike lokaler. Risikoen knytter seg blant annet til markedspriser, endring i prosjekterte løsninger og størrelsen per ny gradert arena.

Kalkyle	*Tillegg*	*Kostnad*	*Mva.*	*Kostnad inkl. mva.*	*Kommentar*
Etablering av NHN per forskningsmiljø		3 000 000	750 000	3 750 000	Inkl. utstyr, klient, printer osv.
Ressurser for å implementere NHN		4 800 000	1 200 000	6 000 000	4 ressurser i 8 måneder
Tilpasning av ugraderte lokaler til HEMMELIG (1.640 m^2 * 38.220,-)		50 200 000	12 550 000	62 750 000	Se behov for fysisk sikkerhet
Sum investeringer:		58 000 000	14 500 000	72 500 000	
Forventet tillegg	20 %	11 600 000	2 900 000	14 500 000	
Forventet prosjektkostnad (P50)		**69 600 000**	**17 400 000**	**87 000 000**	
Usikkerhetsavsetning	60 %	41 800 000	10 400 000	52 200 000	
Kostnadsramme (P85)		**111 400 000**	**27 800 000**	**139 200 000**	

Tabell 7: Investering ny arena i leide lokaler opp til HEMMELIG

Tiltak 4: Styrket tverrdepartemental koordinering av FoU for forsvar, sikkerhet og beredskap.

Ikke beregnet økonomiske og administrative konsekvenser for dette tiltaket.

Vedlegg F: Risiko

Notatet vurderer risiko knyttet til ulike løsninger.

1. Metodikk

Metoden følger trinnene i risikovurdering basert på NS 5814 – «krav til risikovurderinger», og består av følgende trinn:

- Initiering, herunder innsamling av kunnskapsgrunnlag
- Identifikasjon av farer/ risikoer
- Analyse av risiko, herunder vurdering av sannsynlighet, og vurdering av konsekvens opp mot de 4 forvaltningsverdiene, samt hvordan risiko eventuelt endres fra risikonivået i dagens forskningssystem
- Evaluering av risiko, herunder bruk av ALARP-prinsippet for vurdering av hvorvidt risiko kan reduseres
- Dokumentasjon (dette notatet)

Dagens forskningssystem er ikke uten risiko. For å skape et godt beslutningsgrunnlag er det derfor mest relevant å se på *endring av risiko* som følge av de foreslåtte *endringene av forskningssystemet*. Noen forhold kan få et lavere risikonivå, hvilket er like viktig å få frem som de forhold som får høyere risikonivå. Et høyere risikonivå vil kreve en vurdering av om konsekvensreduksjon kan gjøres ved risikoreduserende tiltak, endring i modell etc.

Risiko defineres som konsekvenser av fremtidige aktiviteter og tilhørende usikkerhet. Det er usikkerhet knyttet til hvilke hendelser som kan inntreffe, og hvor ofte, og hva konsekvensen vil være. Usikkerhet beskrives i denne sammenheng med sannsynligheter.

Konsekvenser vurderes opp mot de 4 forvaltningsverdiene; demokrati, rettsikkerhet, faglig integritet og effektivitet (jf. oppdragsbrevet).

Beslutningskriterium

Beslutningskriteriet i denne analysen er hvorvidt en endring i forskningssystemet vil medføre høyere eller lavere risiko. Risiko som blir lavere vil kunne aksepteres uten videre (siden den aksepteres i dag), mens risiko som blir høyere som følge av et endret forskningssystem må reduseres så mye som praktisk og økonomisk mulig (ALARP-prinsippet: As low as reasonably practicable).

Forutsetninger

For denne risikovurderingen er følgende forutsetninger gjort:

Det foreligger ikke risikoakseptkriterier, og en beslutning knyttet til hvorvidt risiko er akseptabel eller ikke er avhengig av om eventuelle risikoreduserende tiltak som er samfunnsøkonomisk lønnsomme gjennomføres eller ikke. Risikoen er ikke akseptabel dersom det finnes gode risikoreduserende tiltak som ikke blir gjennomført.

2. Identifikasjon av risiko

Følgende risikoer knyttet til endringer i forskningssystemet er identifisert:

#	**Fare/ risiko**
1.	Forskning som i henhold til lovkrav burde være skjermet forblir åpen
2.	Overgradering, forskning får for høy skjermingsgrad/gradering
3.	Nytt porteføljestyre i Forskningsrådet fører til svekket prioriteringseffektivitet
4.	Knapphet på fagpersoner med relevant kunnskap om sikkerhet knyttet til skjermingsverdig informasjon.
5.	Utenlandske aktører mister tillit til at norske aktører klarer å håndtere gradert informasjon, vil ikke samarbeide.
6.	Forskere bruker mer tid på søknadsskriving på bekostning av tid til forskning, nå også innen gradert forskning.
7.	Interne målkonflikter i regelverk (UH-loven og Sikkerhetsloven, ulike definisjoner i ulike regelverk) fører til ikke-enhetlig gjennomføring av verdivurderinger.
8.	Tap av gradert informasjon

3. Analyse av risiko

I dette kapittelet analyseres de enkelte risikoer som er identifisert og listet i kapittel 2.

Forskning som i henhold til lovkrav burde være skjermet forblir åpen

Årsaker til at hendelse:

- Lav kompetanse om verdivurdering. Det må antas at dette i dag er en ukjent aktivitet i de fleste sivile forskningsinstitusjoner.
- Manglende fokus på problemstillingen knyttet til vurdering av skade på nasjonale sikkerhetsinteresser da dette ikke er/har vært relevant for de fleste sivile forskningsinstitusjoner.
- Bevisst unndragelse av verdivurderingsaktivitet og bruk av faktisk kunnskap for å unngå at forskning blir gradert.

Sannsynlighet for hendelsen gitt dagens forskningssystem:

- Sannsynlighet for at forskning som i henhold til lovkrav burde være skjermet forblir åpen er **høy** i dag. Kompetansen om verdivurdering og bevisstheten omkring nasjonale sikkerhetsinteresser er lav. Vi kan ikke se bort fra bevisst unndragelse, da det vil legge sterke begrensninger på de enkelte forskningsmiljøers muligheter til å få finansiering og samarbeid med andre.

Sannsynlighet for hendelsen med et endret forskningssystem:

- Med økt kunnskap og økt fokus på nasjonale sikkerhetsinteresser vil sannsynligheten for en utilsiktet unndragelse av forskning samlet bli noe redusert, til **middels**.

Konsekvenser av hendelse med dagens forskningssystem:

- Demokrati: Hendelsen anses å ha middels konsekvens for demokratiske prosesser da manglende skjerming kan skade offentlige interesser, og gjøre demokratiske prosesser mer sårbare for uønsket påvirkning.
- Rettsikkerhet: Hendelsen anses å ha høy konsekvens for innbyggerens rettsikkerhet, da manglende skjerming nettopp kan skade offentlige interesser, en bedrift, en institusjon eller en enkeltperson om forskningen/informasjonen blir kjent.

- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha lav konsekvens for effektivitet, med noe lavere kostnadseffektivitet grunnet skjerming, men høyere formålseffektivitet da det er en hensikt med skjermingen.

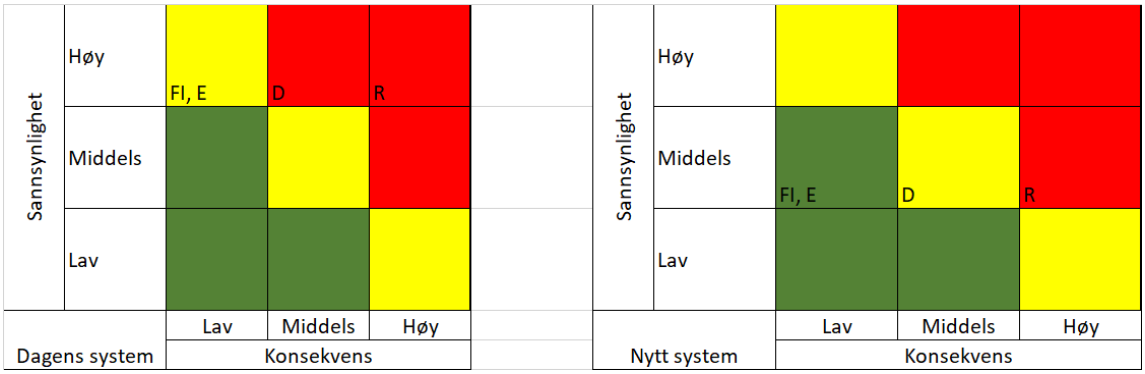
Konsekvenser av hendelse med foreslått forskningssystem:

- Demokrati: Hendelsen gitt det foreslåtte forskningssystemet anses å ha uendret konsekvens for demokratiske prosesser sammenlignet med dagens forskningssystem.
- Rettsikkerhet: Hendelsen gitt det foreslåtte forskningssystemet anses å ha uendret konsekvens for rettssikkerhet sammenlignet med dagens forskningssystem.
- Faglig integritet: Hendelsen gitt det foreslåtte forskningssystemet anses å ha uendret konsekvens for faglig integritet sammenlignet med dagens forskningssystem.
- Effektivitet: Hendelsen gitt det foreslåtte forskningssystemet anses å ha uendret konsekvens for effektivitet sammenlignet med dagens forskningssystem.

Behov for nye barrierer/risikoreduserende tiltak:

At alle utlysninger fra Forskningsrådets nye portefølje medfører en plikt for søker til å etablere prosesser rundt verdivurdering som en forutsetning for å få tildelt midler.

Endring av risiko som følge av foreslått forskningssystem: Med lavere sannsynlighet og uendret konsekvens vil risikoen knyttet til hendelsen være noe lavere med nytt forskningssystem.



Overgradering, forskning får for høy skjerming/ gradering

Årsaker til at hendelse:

- Ansatte har liten erfaring med og bevissthet rundt nyanser i verdivurdering, og overvurderer behovet for å føle seg trygge..
- I et nytt forskningssystem vil verdivurderingsaktiviteter være nye for enkelte virksomheter.

Sannsynlighet for hendelsen gitt dagens forskningssystem:

- Sannsynlighet for at forskning overgraderes er lav i dag. Gradert forskning skjer ved noen få institusjoner med omfattende erfaring med verdivurderinger.

Sannsynlighet for hendelsen med et endret forskningssystem:

- Flere aktører som skal håndtere gradert forskning og en fase med flere aktører med liten erfaring, vil øke sannsynligheten for at overgradering skjer.

Konsekvenser av hendelse med dagens forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha lav konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha middels konsekvens for effektivitet, med noe lav kostnadseffektivitet grunnet unødig skjerming, og lav formålseffektivitet med skjermingen.

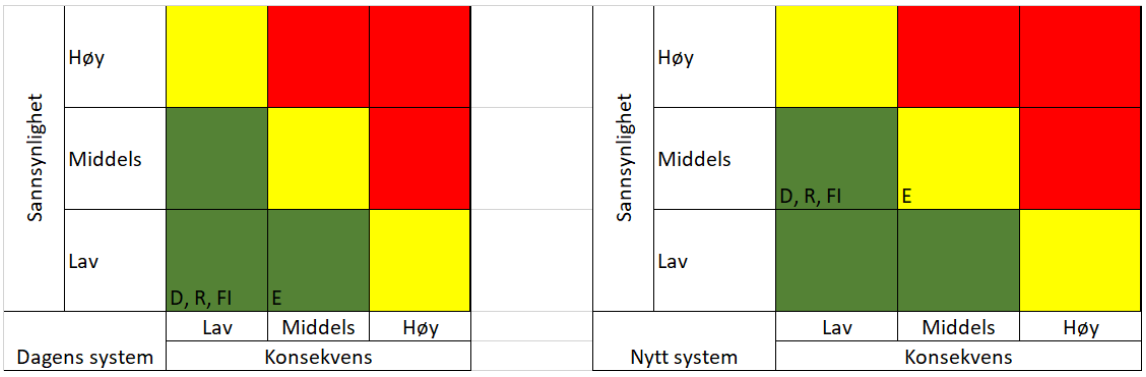
Konsekvenser av hendelse med foreslått forskningssystem:

- Demokrati: Hendelsen gitt det foreslåtte forskningssystemet anses å ha uendret konsekvens for demokratiske prosesser sammenlignet med dagens forskningssystem.
- Rettsikkerhet: Hendelsen gitt det foreslåtte forskningssystemet anses å ha uendret konsekvens for rettssikkerhet sammenlignet med dagens forskningssystem.
- Faglig integritet: Hendelsen gitt det foreslåtte forskningssystemet anses å ha uendret konsekvens for faglig integritet sammenlignet med dagens forskningssystem.
- Effektivitet: Hendelsen gitt det foreslåtte forskningssystemet anses å ha uendret konsekvens for effektivitet sammenlignet med dagens forskningssystem.

Behov for nye barrierer/ risikoreduserende tiltak:

- Det må etableres en sikkerhetskultur som bygger på god kompetanse, tilstrekkelig forståelse og etterlevelse i alle virksomheter som håndterer skjermingsverdig informasjon.
- Alle utlysninger fra Forskningsrådets nye portefølje medfører en plikt for søker til å etablere prosesser rundt verdivurdering som en forutsetning for å få tildelt midler.

Endring av risiko som følge av foreslått forskningssystem: Med høyere sannsynlighet og for det meste uendret konsekvens vil risikoen knyttet til hendelsen være **noe høyere** med nytt forskningssystem.



Nytt porteføljestyre i Forskningsrådet fører til svekket prioriteringseffektivitet

Årsaker til at hendelse:

- Dersom det i nytt forskningssystem utnevnes medlemmer av porteføljestyre med feil bakgrunn, som ikke kjenner de konkrete behovene innenfor forsvar og sikkerhet, og heller ikke har forståelse for prosesser knyttet til skjermingsverdig informasjon, vil det

medføre svekket prioriteringseffektivitet, da det vil kunne fattes uhensiktsmessige beslutninger i porteføljestyret.

Sannsynlighet for hendelsen gitt dagens forskningssystem:

- Det er ikke et eget porteføljestyre i dag.

Sannsynlighet for hendelsen med et endret forskningssystem:

- Da medlemmer ikke er utpekt er det uvisst hvor sannsynlig dette er. Inntil medlemmer er utpekt vurderes sannsynligheten til lav.

Konsekvenser av hendelse med dagens forskningssystem:

- Ikke aktuelt, da det ikke er egen portefølje i dag.

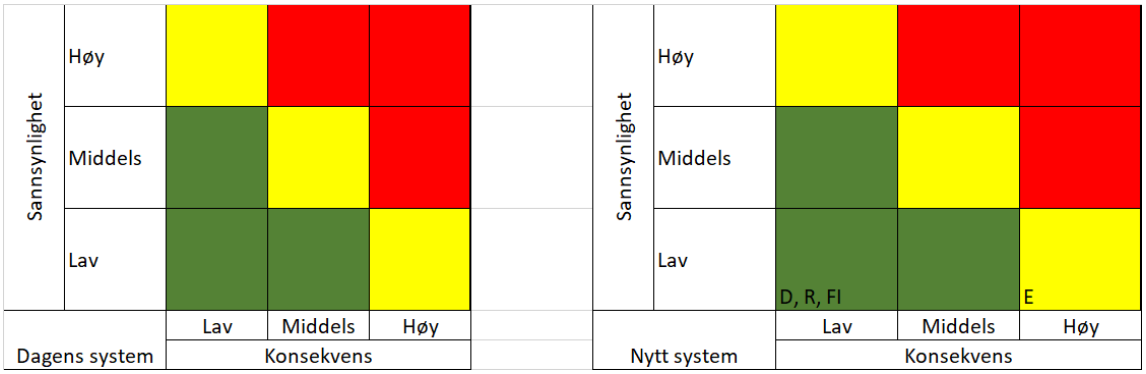
Konsekvenser av hendelse med foreslått forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha lav konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Prioriteringseffektivitet er et element i forvaltningsverdien effektivitet. Hendelsen anses å ha høy konsekvens for effektivitet, da tildeling av midler til feil satsning/ teknologi/ aktør vil være alvorlig.

Behov for nye barrierer/ risikoreduserende tiltak:

- Tydeliggjøre krav til medlemmer i porteføljestyret før dette utnevnes

Endring av risiko som følge av foreslått forskningssystem: Med økt sannsynlighet vil risikoen knyttet til hendelsen være **noe høyere** med nytt forskningssystem.



Knapphet på fagpersoner med relevant kunnskap om sikkerhet knyttet til skjermingsverdig informasjon.

Årsaker til at hendelse:

- Samfunnets utvikling medfører økt fokus på, og utfordringer knyttet til, sikkerhet.
- Det er allerede i dag en viss knapphet av personer med sterk kompetanse på relevante sikkerhetsområder, og det er vanskelig å rekruttere personer med ønsket kompetanse.

Sannsynlighet for hendelsen gitt dagens forskningssystem:

- Med dagens forskningssystem vurderes sannsynligheten til middels.

Sannsynlighet for hendelsen med et endret forskningssystem:

- Med økende sikkerhetsutfordringer i samfunnet, samt at antall virksomheter som har behov for denne kompetansen øker, øker sannsynligheten med det foreslåtte forsyningssystemet til høy.

Konsekvenser av hendelse med dagens forskningssystem:

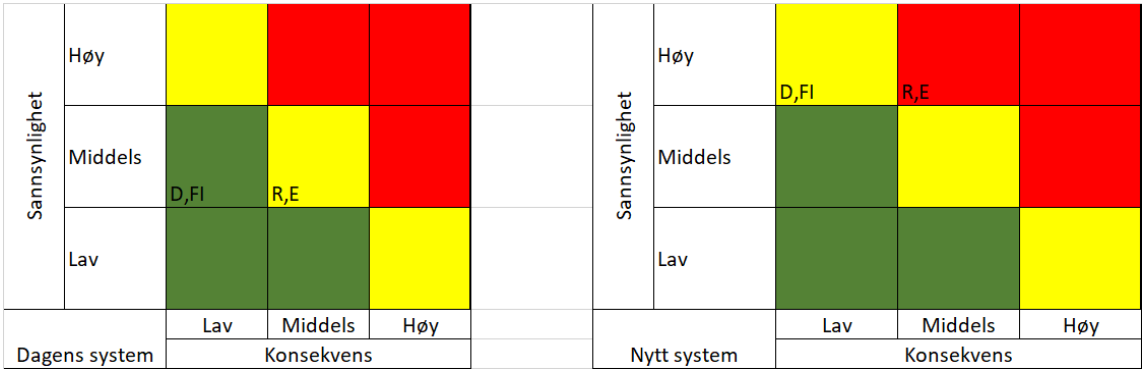
- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: endelsen anses å ha middels konsekvens for innbyggerens rettsikkerhet Manglende etterlevelse av lover, forskrifter og bestemmelser på grunn av lav kapasitet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha middels konsekvens for effektivitet (lav formålseffektivitet).

Konsekvenser av hendelse med foreslått forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha lav konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha middels konsekvens for effektivitet (lav formålseffektivitet).

Behov for nye barrierer/ risikoreduserende tiltak:

Endring av risiko som følge av foreslått forskningssystem: Med økt sannsynlighet vil risikoen knyttet til hendelsen være **noe høyere** med nytt forskningssystem.



3 Utenlandske aktører mister tillit til at norske aktører klarer å håndtere gradert informasjon, vil ikke samarbeide.

Årsaker til at hendelse:

- Dersom det blir mange aktører som håndterer skjermingsverdig forskning, og hvor håndtering av gradert forskning synes å ha varierende godhet og lite pålitelig fra en

utenlandsk aktørs ståsted, er det en fare for at de utenlandske aktørene vil foretrekke å samarbeide med andre land der håndteringen av gradert forskning har høyere pålitelighet.

Sannsynlighet for hendelsen gitt dagens forskningssystem:

- Med dagens forskningssystem vurderes sannsynligheten til lav.

Sannsynlighet for hendelsen med et endret forskningssystem:

- Med et økt antall virksomheter som skal drive skjermingsverdig forskning, og disse ikke har erfaring med dette fra før, øker sannsynligheten for hendelsen til middels inntil de nye virksomhetene har fått god kompetanse og pålitelige prosesser og infrastruktur på området, og viser at de håndterer skjermingsverdig forskning i henhold til reglene over tid.

Konsekvenser av hendelse med dagens forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha lav konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha høy konsekvens for effektivitet da vi vil miste tilgang til andre lands forskning, og derfor må utføre mer selv for å oppnå de samme resultater.

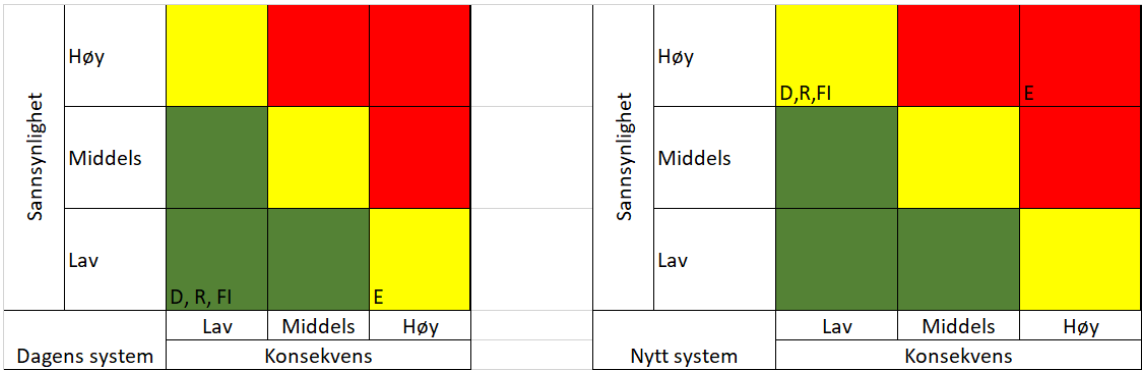
Konsekvenser av hendelse med foreslått forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha lav konsekvens for innbyggerens rettsikkerhet
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha høy konsekvens for effektivitet da vi vil miste tilgang til andre lands forskning, og derfor må utføre mer selv for å oppnå de samme resultater.

Behov for nye barrierer/ risikoreduserende tiltak:

- Etablering av en sterk sikkerhetskultur
- At nye virksomheter ikke får håndtere gradert informasjon uten at alle tekniske, organisatoriske og operasjonelle krav er kontrollert.

Endring av risiko som følge av foreslått forskningssystem: Med økt sannsynlighet vil risikoen knyttet til hendelsen være **noe høyere** med nytt forskningssystem.



Forskere brukere mer tid på søknadsskriving på bekostning av tid til forskning, nå også innen gradert forskning.

Årsaker til at hendelse:

- Dersom gradert forskning blir konkurranseutsatt gjennom utlysninger fra Forsknings-rådet, vil det være økt konkurranse om oppdragene, og det må nødvendigvis medføre en ny søknadsprosess. Noen må skrive søknadene, og det vil kreve tid og innsats fra forskere.

Sannsynlighet for hendelsen gitt dagens forskningssystem:

- I dag benyttes det betydelig tid til å forankre prosjekter med oppdragsgivere før inngåelse av avtale, men dette kan ikke regnes som «søknadsskriving». Med dagens forskningssystem vurderes sannsynligheten for økt tidsbruk til søknadsskriving på bekostning av forskning til lav.

Sannsynlighet for hendelsen med et endret forskningssystem:

- Med konkurranse om utlysningene sannsynligheten øke i et nytt forskningssystem. Forskere som fra før arbeider med gradert forskning må bruke mer av sin tid enn de gjør i dag for å konkurrere om oppdrag, og mindre på selve forskningen, og sannsynligheten øker til høy.

Konsekvenser av hendelse med dagens forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha lav konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha middels konsekvens for effektivitet da det i dag nyttes liten tid på søknadsarbeid.

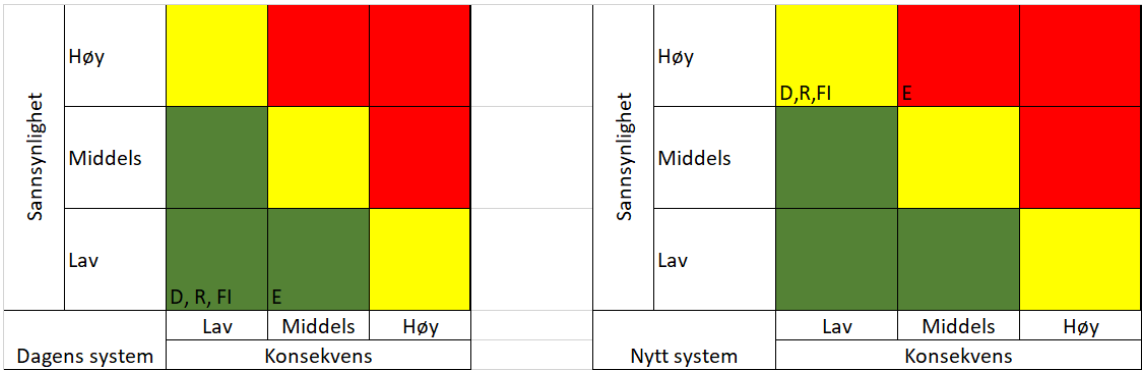
Konsekvenser av hendelse med foreslått forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha lav konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.

- Effektivitet: Hendelsen anses å ha middels konsekvens for effektivitet da vi vil medføre betydelig økt timeantall på søknadsskriving, samtidig som konkurranse kan skjerpe aktørene ytterligere.

Behov for nye barrierer/ risikoreduserende tiltak:

Endring av risiko som følge av foreslått forskningssystem: Med økt sannsynlighet vil risikoen knyttet til hendelsen være **noe høyere** med nytt forskningssystem.



Interne målkonflikter i regelverk (UH-loven og Sikkerhetsloven), ulike definisjoner i ulike regelverk) fører til ikke-enhetlig gjennomføring av verdivurderinger.

Årsaker til at hendelse:

- UH-loven pålegger forskere å publisere/ offentliggjøre forskning, og både metoder, beregningsmetoder, og resultater skal være åpne *("bidra til å spre og formidle resultater fra forskning og faglig og kunstnerisk utviklingsarbeid" (§ 1-3 c))*.
- Sikkerhetsloven pålegger virksomheten å sikkerhetsgradere informasjon etter gitte kriterier, nettopp for å unngå at informasjon (dette kan være om selve forskningsaktivitetene, beregningsmetoder og resultater med mer) blir tilgjengelig for uvedkommende.
- Dette arbeidet (modelloppdraget) har gjort oss oppmerksomme på at det nyttes ulike definisjoner på like og nesten like uttrykk i de ulike lover og regelverk. Dette gjør at man snakker forbi hverandre inntil man forstår at man bruker de samme begreper ulikt.

Sannsynlighet for hendelsen gitt dagens forskningssystem:

- Det er i dag en god forståelse i de virksomheter som har gradert forskning om betydningen av skjerming, og mindre fokus på åpen publisering.
- Det er allerede i dag en noe uensartet språkbruk innenfor ulike fagområder og etater innenfor sikkerhetsområdet og gradert forskning. Etablert språkpraksis henger noe etter forskningsfronten.
- Sannsynlighet i dag vurderes som middels.

Sannsynlighet for hendelsen med et endret forskningssystem:

- Flere sivile virksomheter som går i gang med gradert forskning vil øke sannsynligheten for en ikke-enhetlig gjennomføring av ulike aktiviteter som verdivurdering. Sannsynlighet vurderes til høy.

Konsekvenser av hendelse med dagens forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha middels konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha lav konsekvens for effektivitet.

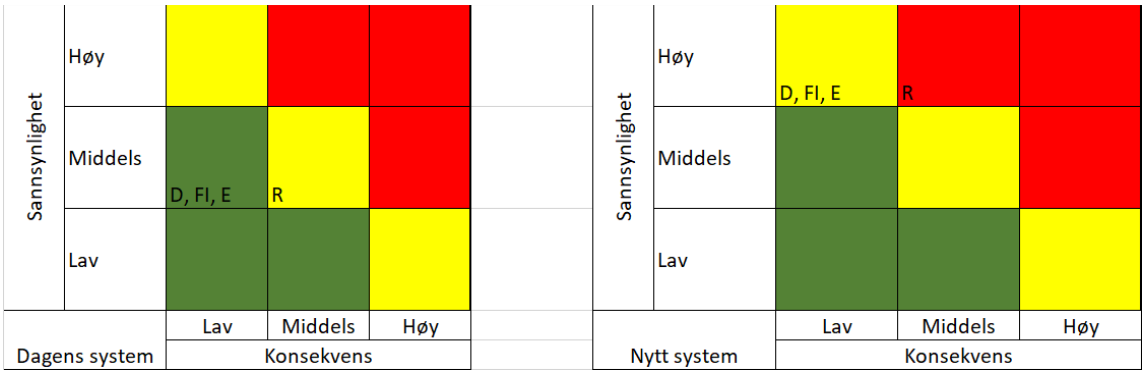
Konsekvenser av hendelse med foreslått forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha middels konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha lav konsekvens for effektivitet.

Behov for nye barrierer/ risikoreduserende tiltak:

- At alle åpne utlysninger fra Forskningsrådet medfører en plikt for søker til å etablere prosesser rundt verdivurdering som en forutsetning for å få tildelt midler.
- Etablering av en sterk sikkerhetskultur
- At nye virksomheter ikke får håndtere gradert informasjon uten at alle tekniske, organisatoriske og operasjonelle krav er kontrollert.

Endring av risiko som følge av foreslått forskningssystem: Med økt sannsynlighet vil risikoen knyttet til hendelsen være **noe høyere** med nytt forskningssystem.



Tap av gradert informasjon.

Årsaker til at hendelse:

- Utilsiktet menneskelig feil, ved at mangel på kunnskap om krav gjør at gradert informasjon ligger åpent tilgjengelig for uvedkommende.
- Utilsiktet feil ved at graderte dokumenter og pc'er hensettes på reise etc.
- Mangel på sikkerhetskultur, der man er kjent med krav, men ikke er så nøye med at krav etterleves.
- Tilsiktet hendelse der forsker som har fått tilgang til gradert informasjon formidler dette til fremmed stat etc.

Sannsynlighet for hendelsen gitt dagens forskningssystem:

- Det er i dag et fåtall virksomheter som bedriver gradert forskning, og disse har etablert infrastruktur, og har i hovedsak en god forståelse for viktigheten av å etterleve gjeldende regelverk.
- Det er lav sannsynlighet, men kan ikke utelukkes at tilsiktede hendelser kan skje også i dag.

Sannsynlighet for hendelsen med et endret forskningssystem:

- Flere sivile virksomheter som går i gang med gradert forskning vil øke sannsynligheten for at gradert informasjon kommer på avveie. Sannsynlighet vil forhåpentligvis fortsatt være lav, men settes her som middels for å få frem en økning i sannsynlighet.

Konsekvenser av hendelse med dagens forskningssystem:

- Demokrati: Hendelsen anses å ha konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha middels konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha lav konsekvens for effektivitet.

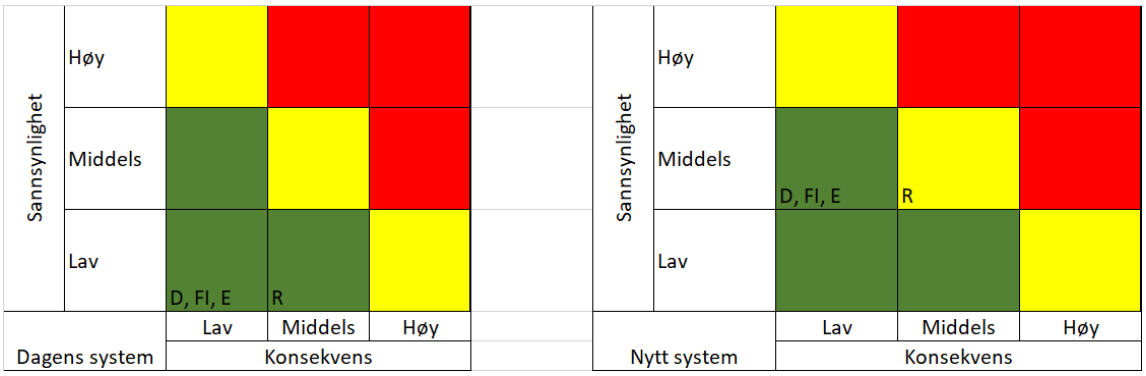
Konsekvenser av hendelse med foreslått forskningssystem:

- Demokrati: Hendelsen anses å ha lav konsekvens for demokratiske prosesser.
- Rettsikkerhet: Hendelsen anses å ha middels konsekvens for innbyggerens rettsikkerhet.
- Faglig integritet: Hendelsen anses å ha lav konsekvens for embetsverkets faglige uavhengighet og objektivitet.
- Effektivitet: Hendelsen anses å ha lav konsekvens for effektivitet.

Behov for nye barrierer/ risikoreduserende tiltak:

- At alle åpne utlysninger fra Forskningsrådet medfører en plikt for søker til å etablere prosesser rundt verdivurdering som en forutsetning for å få tildelt midler.
- Etablering av en sterk sikkerhetskultur.
- At nye virksomheter ikke får håndtere gradert informasjon uten at alle tekniske, organisatoriske og operasjonelle krav er kontrollert.

Endring av risiko som følge av foreslått forskningssystem: Med økt sannsynlighet vil risikoen knyttet til hendelsen være **noe høyere** med nytt forskningssystem.



Risikobilde – endring av risiko

Fra analysen ser vi at følgende risikoer får et lavere risikonivå:

#	Risiko	Nivå før	Nivå etter	Endring
1.	Forskning som i henhold til lovkrav burde være skjermingsverdig forblir åpen	Høy-middels	Middels	Lavere

Fra analysen ser vi at følgende risikoer får et høyere risikonivå:

#	Risiko	Nivå før	Nivå etter	Endring
2.	Overgradering, forskning får for høy skjerming/ gradering	Lav	Lav-middels	Høyere
3.	Nytt porteføljestyre i Forskningsrådet fører til svekket prioriteringseffektivitet	Ingen	Lav-middels	Høyere
4.	Knapphet på fagpersoner med relevant kunnskap om sikkerhet knyttet til skjermingsverdig informasjon	Lav-middels	Middels-høy	Høyere
5.	Utenlandske aktører mister tillit til at norske aktører klarer å håndtere gradert informasjon, vil ikke samarbeide.	Lav-middels	Middels-høy	Høyere
6.	Forskere brukere mer tid på søknadsskriving på bekostning av tid til forskning, nå også innen gradert forskning	Lav	Middels-høy	Høyere
7.	Interne målkonflikter i regelverk (UH-loven og Sikkerhetsloven), ulike definisjoner i ulike regelverk) fører til ikke-enhetlig gjennomføring av verdivurderinger.	Lav-middels	Middels-høy	Høyere
8.	Tap av gradert informasjon.	Lav	Lav-middels	Høyere

Vedlegg G: Kompetansebehov

Notatet beskriver hvilke kompetansebehov må dekkes for at
a) et felles nasjonalt forskningssystem skal kunne fungere i praksis, og
b) at enkelte nye leverandører skal kunne bidra innenfor sensitivt, skjermingsverdig og gradert forsknings- og teknologisamarbeid?

1. Innledning

For å ivareta et forsvarlig sikkerhetsnivå i de fire tiltakene må tiltakene støttes av riktige og tilstrekkelige ressurser knyttet til sikkerhetsstyring og forebyggende sikkerhet. Dette oppnås når aktørene har oversikt over hvilke verdier som skal beskyttes og hvordan, derfor vil det være nødvendig med god sikkerhetskultur og sikkerhetssystem knyttet til tiltakene som foreslås.

Overordnet er det viktig at åpenhet ikke går på bekostning av prinsippene for integritet eller konfidensialitet i henhold til sikkerhetsloven. Det er viktig at involverte parter i forskningen har de riktige forutsetningene til å drive skjermet og gradert forskning og håndtering av skjermet og gradert informasjon. For å kunne oppnå dette må de ha tilstrekkelig kompetanse til å se hvilken verdi forskningen deres har opp mot forsvar, sikkerhet og beredskap. Deretter må forskerne ha tilstrekkelig kjennskap til sikkerhetsloven til å vite hvordan de kan oppnå et forsvarlig sikkerhetsnivå og hvilke krav i sikkerhetsloven som skal oppnås. Derfor vil de anbefalte tiltakene være avhengig av en administrativ funksjon som har god kjennskap til sikkerhetsloven og kan bistå med råd om sikkerhet - en *sikkerhetsorganisasjon*. Denne sikkerhetsorganisasjonen må ha tilstrekkelig med ressurser til å kunne forsvarlig håndtere det risiko- og trusselbildet et felles forskningssystem kan være utsatt for.

Sikkerhetsorganisasjonen bør ha som sekundæroppdrag å kartlegge fremtidige behov for kompetanse og ressurser knyttet til de anbefalte tiltakene. Dette fordi de vil ha konkret erfaring og best forutsetning til å vite hvilke behov og ikke minst hvilke utfordringer, et helhetlig forskningssystem møter. Det anbefales følgende alternativer til løsning:

Det bør opprettes sikkerhetsorganisasjoner i alle virksomheter som enten skal utføre skjermet eller gradert FoU eller som skal forvalte det helhetlige systemet. Sikkerhetsorganisasjonene anbefales å ha en risikobasert sikkerhetsstyring som tilnærming.

En sikkerhetsorganisasjon bør som et minimum inneholde følgende roller: sikkerhetsleder, sikkerhetsrådgiver, informasjonssystemsikkerhetsansvarlig, personellsikkerhetsansvarlig og informasjonsforvalter. Målet er å kartlegge, identifisere og implementere de nødvendige sikkerhetstiltak knyttet til risiko- og trusselbildet aktørene kan være utsatt for.

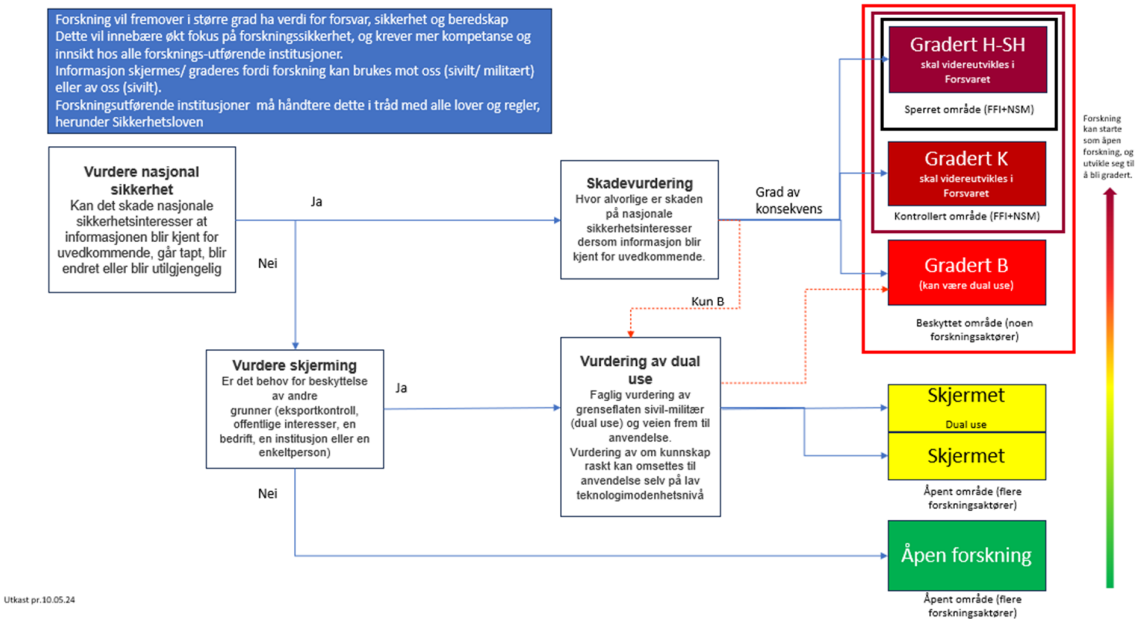
- *Sikkerhetsleder*: bør inneha kompetanse til å etablere og opprettholder primær intensjonen til en slik enhet, ha myndighet og ansvar for å iverksette nødvendige tiltak for å ivareta et forsvarlig sikkerhetsnivå. Denne organisasjonen/enheten skal ivareta den daglige sikkerhetsledelsen og samtidig ivareta verdivurdering og skadevurdering knyttet til forskningsarbeidet. Denne enheten blir rådgivende funksjon for ivaretagelse av forsvarlig sikkerhetsnivå i nytt helhetlig forskningssystem. I samsvar med sikkerhetsrådgiver skal sikkerhetsleder ha ansvar for å stille krav og håndtere verdier, samt ha kompetanse innenfor sikkerhetsloven, arbeidstakeroppfinnelse, patentloven, designloven, varemerkeloven, åndsverkloven, forretningshemmelighetsloven, lov om forsvarsviktig oppfinnelser.

- *Sikkerhetsrådgiver*: Rollen bør ha tilstrekkelig kompetanse til å analysere trussel- og risikobildet mot aktivitet i forskningssystemet og iverksette tilstrekkelige sikkerhetstiltak. Sikkerhetsrådgiver må ha kompetanse innenfor industrisikkerhet, for å ivareta riktig håndtering av skjermet og gradert informasjon knyttet til sivile forskningsmiljøer og verdikjeder. Sikkerhetsrådgiver må jobbe aktivt med forebyggende sikkerhet og fysisk sikring, avdekke sårbarheter og håndtere uønskede hendelser knyttet til verdiene det helhetlige forskningssystemet forvalter.
- *Informasjonssystemsikkerhetsansvarlig*: Jobber aktivt med forebyggende sikkerhet, avdekker sårbarheter og håndterer uønskede hendelser knyttet til verdier i informasjonssystemene brukt i det helhetlige forskningssystemet. Har primæransvaret for godkjenning og håndtering/oppbevaring av informasjonssystemer.
- *Personellsikkerhetsansvarlig*: Jobber aktivt med forebyggende sikkerhet, avdekker sårbarheter og håndterer uønskede hendelser knyttet til innsiderisiko og personellsikkerhet. Har hovedansvaret for klarering og autorisasjon.
- *Informasjonsforvalter:* Denne ressursen bør primært ha ansvar for tilgangsstyring knyttet til skjermet og gradert informasjon og forskning. Har kontroll over at riktig informasjon blir tilgjengelig til riktig tid for de ulike tiltakene. Sørger for å koordinere på tvers og at konkrete oppdrag eller krav blir fulgt opp til riktig tid. I tillegg har informasjonsforvalter ansvar for forvaltning av gradert informasjon i henhold til kravene i sikkerhetsloven.

2. Overordnet kompetansebehov knyttet til de fire tiltakene

Tiltak 1: Økt bruk av sivile forskningsmiljøer innenfor forsvar, sikkerhet og beredskap. *Et viktig element i dette er å etablere en systematikk for å identifisere flerbruksmuligheter (dual-use) og skjermet forskning.*

Sikkerhetsloven stiller strenge krav til håndtering av skjermet og gradert informasjon. Momenter som må tas hensyn til er: tilstrekkelig kompetanse og erfaring innenfor følgende fagområder verdivurdering, skadevurdering, industrisikkerhet, personellsikkerhet, informasjonssikkerhet og informasjonssystemsikkerhet.



Figur 1: Prosessen knyttet til vurdering av skjermingsverdig informasjon/ forskning og «dual use»

Det må stilles strenge krav til forskningens integritet fra start, og det kan være hensiktsmessig å gjennomføre en verdivurderingsprosess som første steg i en dual use- eller skjermet forskning for å kunne identifisere beskyttelsesbehovet. Beskyttelsesbehovet som identifiseres vil fastsette rammen og kravene til videre arbeid.

Tiltak 2: Opprettelse av en ny porteføljе i Forskningsrådet for å styrke kunnskapsbygging relevant for forsvar, sikkerhet og beredskap.

Sikkerhetsloven krever at det innføres riktige ressurser og kompetanse knyttet til organisatoriske, infrastrukturelle, teknologiske og menneskelige tiltak dersom forskningen eller informasjon knyttet til forskningen har et skjermingsbehov. Derfor vil det være nødvendig med en sikkerhetsorganisasjon.

***Tiltak 3* Etablering av en arena for kunnskapssamarbeid innenfor forsvar, sikkerhet og beredskap.**

Arenaen må møte kravene i sikkerhetsloven knyttet til det graderingsnivået som er identifisert. Arenaen må være tilrettelagt for håndtering og oppbevaring av både skjermet og gradert arbeid.

3. Overordnet kompetansebehov knyttet til livsløpet for gradert eller skjermet forskning

Fase 0 – Etablering av et forskningsprosjekt med sannsynlighet for skjermingsverdige komponenter

Det vil være nødvendig med en verdivurdering, hvor den enkelte forsker i samråd med en sikkerhetsfaglig rådgiver lager en verdivurdering. Prosessen innebærer en analyse av

forskningens verdi opp mot områdene forsvar/sikkerhet/beredskap og kartlegger hvilke lover/regelverk som er gjeldende og relevante for forskningen.

Dersom den enkelte forsker, institusjon eller forvaltningsorgan skal gjøre dette uten bruk av sikkerhetsressurser identifisert i en sikkerhetsorganisasjon, så må de selv ha tilstrekkelig med kompetanse i verdi- og risikovurderinger. I tillegg må de ha god nok kjennskap til sikkerhetsloven og andre regelverk til å kunne skrive en vurdering som gir verdi for videre identifisering av beskyttelsesbehovet.

Det vil være hensiktsmessig å legge ansvaret hos en sikkerhetsorganisasjon enten i forskningsinstitusjonene eller hos forvaltning for å bistå med veiledning og opplæring av verdieiere. På denne måten vil man sørge for en helhetlig og lik tilnærming. Disse ressursene vil i tillegg kunne bidra med å skape en god sikkerhetskultur, hvor den enkelte forsker får riktige forutsetninger til å kunne vurdere verdiene opp mot sikkerhetsloven og annet regelverk.

I tillegg til å ha spesialiserte fagressurser som bidrar til å skape god sikkerhetskultur, så kan man stille krav i ulike prosesser tilknyttet for eksempel finansiering. Verdivurdering bør være et krav som må dokumenteres før innvilget søknad og kanskje et krav underveis i arbeidet. Dette tiltaket vil mest sannsynlig være mest realistisk og gjennomførbart i statlig finansierte prosesser, men for privatfinansiert forskning så må det forutsette at institusjonene eller forskere har insentiver nok til å pålegge et slik tiltak/krav.

Fase 1 – Oppstart

Når verdivurderingen er utarbeidet og beskyttelsesbehovet er identifisert, så vil det være nødvendig å implementere de riktige tiltakene knyttet til beskyttelsesbehovet. Dette kan være organisatoriske, teknologiske, menneskelige og fysiske tiltak. Faktiske skjermingstiltak er helt avhengige av resultatet av en verdivurdering.

Fase 2 - Anskaffelser, innkjøp eller samarbeid med andre parter

Avhengig av resultatet av verdivurderingen og identifiserte tiltak, så kan enkelte ha behov for å samarbeide med private instanser. Enten i form av innkjøp av varer med vedlikehold eller utviklingssamarbeid/forskningssamarbeid.

Det vil kreve kompetanse innenfor industrisikkerhet, hvor en må kunne bistå med utarbeidelse av sikkerhetsavtaler ved utveksling av gradert informasjon. Hensikten med slike avtaler er å beskrive partenes ansvar og rolle, samt krav i sikkerhetsloven knyttet til oppbevaring eller behandling av gradert informasjon innenfor identifisert samarbeidsform mellom partene.

Dette krever en bred kompetanse innenfor industrisikkerhetsfaget, men også kjennskap til både organisatoriske, teknologiske, fysiske og menneskelige krav i sikkerhetsloven og annet regelverk.

Fase 3 – Drift, endring, utvidelse og videreutvikling

Kontinuerlig oppfølging av verdiene er viktig, for å kunne avdekke endringer i beskyttelsesbehovet. Hovedsakelig skal endringer, utvidelser og videreutvikling av forskningen bli rapportert av verdieiere til en sikkerhetsorganisasjon, som deretter vil kunne bistå med rådgivning og veiledning i videre håndtering og beskyttelse. Dette ansvaret ligger hos verdieier fordi de har det daglige sikkerhetsmessige ansvaret for at verdien håndteres i henhold til kravene og tiltakene identifisert i verdivurderingen. Derfor bør det vektlegges å ha en sikkerhetsorganisasjon som har kompetanse og erfaring til å skape god sikkerhetskultur og forståelse for hvilke krav som må følges opp.

Fase 4 - Terminering og avhending

Sikkerhetsloven stiller krav til terminering og avhending av gradert materiale. Dette er kompetanse som skal ligge hos en sikkerhetsorganisasjon, og sikkerhetsressursene må kunne håndtere terminering eller avhending opp mot krav som stilles til det graderingsnivået identifisert for materialet.

Kravene for terminering og avhending kan i enkelte tilfeller, som for eksempel innenfor informasjonssystemsikkerhet, bli kompliserte. Det vil derfor være behov for ressurser i form av en sikkerhetsorganisasjon som har kompetanse i videre håndtering og terminering av slikt materiale.

Vedlegg H: Bakgrunnsnotat om Forskningssystemet

Notatet beskriver hvem som i sivil sammenheng er aktørene og brukerne i forskningssystemet, og hvordan relasjonene mellom dem påvirkes av finansiering gjennom Forskningsrådet. Det pekes også på noen elementer i dagens system som kan videreutvikles med tanke på forskning relevant for sikkerhet og beredskap. Notatet beskriver også hvordan forskningssystemet innenfor forsvarssektoren fungerer i dag, både hvem som er aktørene og hvordan de samhandler.

1. Innledning

Forskningssystemet defineres ofte som "aktørene som driver, påvirker og bruker forskning, og relasjonene mellom dem".[1] Dette notatet beskriver kortfattet hvem som i sivil sammenheng er aktørene og brukerne, og hvordan relasjonene mellom dem påvirkes av finansiering gjennom Forskningsrådet. I beskrivelsen har også vi pekt på noen elementer i dagens system som kan videreutvikles med tanke på forskning relevant for sikkerhet og beredskap. I tillegg beskriver notatet hvordan forskningssystemet innenfor forsvarssektoren fungerer i dag, både hvem som er aktørene og hvordan de samhandler.

2. De forskningsutførende aktørene i det sivile systemet

De forskningsutførende aktørene kan deles i to hovedgrupper: i) de som har uavhengig forskning og utvikling (FoU) som et hovedformål og ii) de som utfører og/eller bruker FoU, men som ikke har FoU som hovedformål. Mens sistnevnte gruppe kan deles i offentlig og privat sektor, deles førstnevnte ofte i universitets- og høyskolesektoren (UH-sektoren) inkludert universitetssykehusene, og instituttsektoren. Det er betydelig samarbeid mellom gruppene i) og ii), dels i form av offentlig delfinansiert *faktisk samarbeid,*[2] eller ved at aktører i sistnevnte gruppe kjøper *FoU-oppdrag* fra førstnevnte gruppe.

Størstedelen av norsk FoU foregår i næringslivet (drøyt 25.000 FoU-årsverk i 2022), etterfulgt av UH-sektoren og instituttsektoren (henholdsvis ca. 18.000 og ca. 10.000 FoU-årsverk).[3] Private aktører forvalter også store deler av norsk, kritisk infrastruktur. Det er derfor viktig ikke å undervurdere deres FoU-kompetanse og mulige rolle i forbindelse med nasjonal sikkerhet og beredskap.

UH- og instituttsektoren består av en rik flora av institusjoner med ulike samfunnsoppdrag og kjerneoppgaver, ulik grad av autonomi, ulike kilder til forskningsfinansiering og ulike økonomiske rammevilkår. Diversiteten er en styrke, med tanke på forskjellene i de ulike samfunnsaktørenes arbeidsmodus og kunnskapsbehov (men kan også by på utfordringer i det

[1] Se (f.eks.) Forskningsrådets Årsrapport for 2022, side 59.
[2] Statsstøtteregelverkets begrep *faktisk samarbeid* er definert slik på Forskningsrådets nettside om Samarbeidspartnere og leverandører: "Samarbeid mellom minst to uavhengige parter for å utveksle kunnskap eller teknologi eller for å nå et felles mål på grunnlag av arbeidsdeling, der partene i fellesskap definerer omfanget av samarbeidsprosjektet, bidrar til dets gjennomføring og deler risikoer og resultater. En eller flere parter kan bære alle kostnadene knyttet til prosjektet og dermed frita andre parter for finansiell risiko. Oppdragsforskning og yting av forskningstjenester anses ikke som en form for samarbeid."
[3] Kilde: SSB tabell 13511.

daglige samarbeidet). Forskningsrådet opererer med en liste over til enhver tid *godkjente forskningsinstitusjoner* der institusjonene må oppfylle spesifikke krav, blant disse at uavhengig forskning skal være et hovedmål.[4]

UH-sektoren er kjennetegnet av stor grad av autonomi, og tett kobling mellom forskning og undervisning. Sammenlignet med mange andre land finansierer statlige grunnbevilgningen en relativt høy andel av norske universiteters FoU-kostnader. Dette muliggjør en bred, nasjonal kunnskapsbase, og utvikling av helt nye forskningsfelt, også felt som kan ha betydning for norsk sikkerhet og beredskap. En helt sentral del av UH-sektorens rolle er at den utdanner kandidater som bruker sin kompetanse i alle deler av samfunnet, inkludert forsvarssektorens forskningssystem. I UH-sektoren finnes mange sterke forskningsmiljøer innenfor fagfelt med relevans for nasjonal sikkerhet og beredskap.

Instituttsektoren, slik denne er avgrenset i regjeringens Strategi for helhetlig instituttpolitikk,[5] innehar ca. 1/3 av det samlede antallet FoU-årsverk i institutt- og UH-sektoren sett under ett. Cirka 2/3 av instituttsektorens FoU-årsverk finner vi i uavhengige institusjoner omfattet av Retningslinjer for statlig grunnbevilgning.[6] Disse er kjennetegnet av at en svært høy andel (ca. 90 %, gruppen sett under ett) av driftsinntektene er konkurranseutsatt og kommer fra næringsliv, offentlig forvaltning, Forskningsrådet og EU. Dette sikrer behovet for nært samarbeid med oppdragsgivere i privat og offentlig sektor.

De øvrige instituttene omfattet av regjeringens strategi er statlig eide og kjennetegnet av tett samhandling med eierdepartement og deres underliggende organer, som disse instituttene også mottar mesteparten av sine FoU-inntekter fra (ca. 70 % av FoU-inntektene, gruppen sett under ett). Disse instituttene mottar årlig tildelingsbrev fra sitt eierdepartement. Dette legger rammene for deres rådgiving til myndighetene og den FoU som støtter om under disse. Her ligger også departementenes mulighet til dirkete styring av instituttenes arbeid innenfor sikkerhet og beredskap.

Instituttsektoren har primært fast ansatte forskere. Dette bidrar til at sektoren kan opprettholde og tilby relevant kapasitet permanent over tid.

3. Forskningsrådets rolle

Kunnskapsdepartementet skriver følgende:[7] "[…] Norge har ett forskningsråd med ansvar for alle fagområder innenfor så vel grunnleggende forskning som innovasjonsrettet forskning. Om lag en fjerdedel av offentlige FoU-midler kanaliseres gjennom Forskningsrådet.[8] Alle departementene finansierer forskning gjennom Forskningsrådet. […] Forskningsrådet har i hovedsak tre viktige roller i det norske forskningssystemet. For det første er rådet myndighetenes sentrale forskningspolitiske rådgiver. For det andre er Forskningsrådet det viktigste organet for å realisere regjeringens overordnede forskningspolitikk. Til sist fungerer

[4] Godkjente forskningsorganisasjoner (forskningsradet.no).
[5] Strategi for helhetlig instituttpolitikk - regjeringen.no, februar 2020.
[6] Retningslinjer for statlig grunnbevilgning til forskningsinstitutter og forskningskonsern - regjeringen.no.
[7] Sitatet er hentet fra regjeringens nettside om organisering og finansiering av forskning i Norge.
[8] I 2022 forvaltet Forskningsrådet tilskudd til FoU på til sammen ca. 11,6 mrd. kroner.

også rådet som en møteplass hvor samfunnet og dets aktører involveres i utforming og gjennomføring av forskningspolitikken."

Forskningsrådet tilskudd til FoU, vanligvis kalt *bidrag* eller *bidragsfinansiering*,[9] foregår ved at midlene konkurranseutsettes gjennom utlysninger. Hovedbegrunnelsen for slik konkurranse-utsetting er at det øker kvaliteten på forskningen sammenlignet med om de samme offentlige midlene ble tildelt direkte, men behovet å insentivere samarbeidsrelasjoner mellom aktørene er også sentral del av begrunnelsen. Søknadene vurderes på grunnlag av vitenskapelig kvalitet, hvorvidt de imøtekommer eventuelle tematiske føringer og/eller eventuelle krav til samarbeid mellom ulike aktører. Midler tildeles til de beste søknadene, dog oppad begrenset til den gitte utlysningens øvre økonomiske ramme. Den vitenskapelige vurderingen foretas i hovedsak av innleide utenlandske forskere, men også norske eksperter bidrar, særlig i utlysninger rettet mot eller relevant for næringsliv eller offentlig sektor.

Praktiske talt alle Forskningsrådets utlysninger retter seg mot én av hovedaktørgruppene nevnt ovenfor, nemlig godkjente forskningsorganisasjoner, næringslivet eller offentlig sektor. Overordnet mål for utlysinger rettet mot førstnevnte gruppe (utover økt kvalitet pga. konkurranseutsettingen) er forskningsbasert kunnskap til nytte for myndighetene og samfunnet ellers, og det forventes at forskningsresultatene offentliggjøres. Overordnet mål for utlysninger rettet mot privat eller offentlig sektor er videreutvikling av sektorene gjennom økt bruk av FoU og FoU-samarbeid, særlig med godkjente forskningsorganisasjoner.

En betydelig del av næringslivets oppdragsforskning er finansiert som et spleiselag der Forskningsrådet bidrar med offentlig støtte. Mekanismen er at en bedrift, ofte på vegne av flere bedrifter, søker om et bidrag til et FoU-prosjekt som bedriften(e) finansierer størstedelen av.[10] Deretter kjøper bedriften(e) oppdragsforskning fra en (eller flere) forskningsinstitusjon(er).[11] Slike spleiselag utgjør en av de største inntektskildene til flere av de uavhengige instituttene, og kommer i tillegg til deres oppdragsportefølje fullfinansiert av oppdragsgivere, uten offentlig støtte.

Et kjennetegn ved offentlig/privat-finansiert oppdragsforskning som beskrevet ovenfor, er at forskningsinstitusjonene ofte spiller en betydelig rolle under initieringen av FoU-prosjektet. Forskningsinstituttene anser dette som en naturlig del av sin akkvisisjon, og bedriftene får drahjelp til utformingen av søknaden til Forskningsrådet. Lignende samspill kan utvikles innenfor FoU rettet mot sikkerhet og beredskap, i alle fall innenfor ugraderte problemstillinger.

Oppdragsforskning gir ofte forskningsinstitusjonens forskere innsyn i forhold oppdragsgiver ikke ønsker delt med andre, f.eks. av konkurransehensyn, og forskningsinstituttene har en veletablert praksis for denne typen hemmelighold. Selv om slikt hemmelighold normalt ikke er omfattet av Sikkerhetsloven, kan det gi grunnlag for oppdrag relatert til sikkerhet og beredskap, i alle fall innenfor ugraderte problemstillinger.

[9] Dette i motsetning til oppdrag; kjøp av FoU-oppdrag inngår ikke i Forskningsrådets tilskuddsforvaltning.
[10] Statsstøtteregelverket setter grenser for hvor stor den offentlige støtteintensiteten gjennom Forskningsrådet kan være.
[11] SSBs veileder for instituttenes innmelding av nøkkeltall for egen virksomhet definerer *nasjonale oppdragsinntekter* som "vederlag for leveranse av anvendt forskning som er definert av norsk oppdragsgiver" (hele definisjonen er noe mer spesifikk).

Oppdragsforskning skjer oftest i en forskergruppe som jevnlig videreutvikler sin kompetanse gjennom en miks av bidragsfinansiering fra offentlige kilder (primært Forskningsrådet og EU) og oppdrag fra flere (ofte konkurrerende) oppdragsgivere. Utover at dette selvsagt stiller særskilte krav til uavhengighet og integritet i oppdragsforskningen, representerer det også et ansvar for Forskningsrådet: Innenfor fag og tema der det er naturlig å tilby tjenester i et oppdragsmarked, vil det ofte være behov for at Forskningsrådet også finansierer oppbygging/videreutvikling av relevant kompetanse. Særlig gjelder dette innenfor nye forskningsfelt. Men det er også relevant der man ønsker å etablere nye kontaktflater mellom oppdragsgivere og forskningsinstitusjoner som tradisjonelt ikke har arbeidet sammen. Økt samarbeid og oppdragsforskning innenfor sikkerhet og beredskap er eksempler på det siste.

4. Forsvarssektorens forskningssystem

Forsvarssektoren har etablert et eget forsknings- og innovasjonssystem. Det er bransje-spesialisert for å møte de behov for kunnskap, kompetanse og innovasjon som sektoren har, og det er innrettet med et sikkerhetssystem som ivaretar beskyttelse av nasjonale og alliertes verdier. Kompetanse og problemstillinger er i stor grad gradert, og arbeidet er koblet mot internasjonalt gradert statlig samarbeid gjennom et nettverk av bilaterale og allierte samarbeider. Forskning, utvikling og innovasjon skal understøtte ambisjonene for forsvars-evnen som settes i sektorens langtidsplan og retningen som pekes ut i sektorens strategi for forskning og utvikling.[12, 13] Sektorens innovasjonsmodell er det såkalte trekantsamarbeidet,[14] og denne har gitt suksess og en sterk vekst for norsk forsvarsindustri. Sektorens forskning og utvikling er en driver i denne modellen. Nasjonal forsvarsindustriell strategi,[15] sektorens arbeid med en ny innovasjonsstrategi og støtteordninger for forsvarsindustrien understøtter utviklingen.

Forsvarssektorens forskningsforum (F3) er det formelle styringsorganet for beslutninger om oppstart, endring og avslutning av oppdragsforskningen i sektoren. Her samles beslutnings-takere, utførere og interessenter. F3 ledes av Forsvarsdepartementet.

Sektoren har et eget forskningsinstitutt (Forsvarets forskningsinstitutt, FFI) som er navet i forskning, utvikling og innovasjon, og en egen høyskole (Forsvarets høgskole) som sørger for forskningsbasert undervisning for Forsvarets behov, samt driver sikkerhetspolitisk forskning, særlig ved Institutt for forsvarsstudier. Også Forsvarsbygg og Nasjonal sikkerhetsmyndighet utfører egen forskning samt kjøper inn oppdragsforskning fra andre.

FFI er et sivilt forskningsinstitutt direkte underlagt Forsvarsdepartementet. Det er et statlig forvaltningsorgan med særskilte fullmakter og et eget styre.[16] FFI har som formål "å gi den politiske og militære ledelsen rettidige, forskningsbaserte og uavhengige råd til utvikling av forsvarspolitikk, forsvarsplanlegging og forvaltning av sektoren".[17] FFIs direktør er rådgiver til forsvarsminister og forsvarssjef om teknologiske og militærtekniske spørsmål. FFI er en

[12] Langtidsplanlegging i forsvarssektoren - regjeringen.no
[13] FoU-strategi for forsvarssektoren (regjeringen.no)
[14] Trekantsamarbeidet (ffi.no)
[15] Forsvarsindustri - regjeringen.no
[16] Styret Forsvarets forskningsinstitutt - regjeringen.no
[17] Vedtekter for Forsvarets forskningsinstitutt (FFI).PDF

prosjektorganisasjon der alle de vitenskapelige ansatte fører sine timer i prosjekter. Alle prosjekter har en prosjektavtale, som blant annet beskriver prosjektets leveransemål, og et prosjektråd. Over 80 % av omsetningen er oppdragsfinansiert og er i stor grad oppdrag fra sektoren. Prosjektene prioriteres i forhold til relevans for forsvarsevnen og resultatene vurderes mot oppnådd effekt. Det er et tett samspill med brukerne av resultatene for å sikre effekt.

Forsvarssektorens forskning og utvikling samspiller med nasjonale kompetansemiljøer og næringsliv hovedsakelig gjennom oppdragsprosjektene. Nasjonale aktører inviteres inn og samarbeider med sektorens miljøer når de utfyller hverandre. Oftest skjer dette i form av ugradert eller lavere gradert arbeid der sikkerhetskravene er lavere. Etatene kan også velge aktører utenfor sektoren til å utføre arbeidet. FFI skal utnytte kunnskapen nasjonalt til å videreutvikle og underbygge sektorens kunnskapsbehov. Dette skjer oftest gjennom samarbeid om kunnskapsbygging. Samarbeid om doktorgrader, studentoppgaver, utveksling gjennom II-er-stillinger og deltakelse i felles prosjekter er typiske samarbeidsformer. Dette er samarbeids-former som kan utvides i et fremtidig forskningssystem.