

## Notat

---

Til: Alle fakulteter, avdelinger, rektor, viserektor, DOI

---

Kopi til:

---

Fra: Seksjon for sikkerhet og beredskap

---

Sikkerhetsorganisasjonen ved NTNU har utarbeidet dette notatet, med tilhørende presentasjon, for å beskrive trusselbildet for 2026 slik det fremkommer i de nasjonale trusselvurderingene. Notatet sammenfatter de mest relevante utviklingstrekkene og vurderer hva disse betyr for forskningssektoren generelt og for NTNU spesielt.

## Sikkerhetstjenestenes risiko- og trusselbilde for 2026 - relevans for forskningssektoren og NTNU

[PST](#), [NSM](#) og [E-tjenesten](#) har nå publisert sine årlige, åpne trusselvurderinger. Trusselvurderingene skal sette organisasjoner og mennesker i stand til å forstå hvordan man er utsatt for de mest alvorlige truslene som truer Norge, men også hvordan vi kan beskytte oss mot disse truslene. Dette notatet oppsummerer de mest sentrale punktene relevant for forskningssektoren og er ment som støtte til NTNUs ledere og deres arbeid med å ivareta sikkerhet.

Trusselbildet mot forskningssektoren og NTNU for 2026 følger det som sikkerhetstjenestene har advart om gjennom flere år. Det er ingen endringer i trusselbildet utover at årets trusselvurderinger fremhever forskningssektoren enda mer konkret enn tidligere. Det krever at NTNU forbereder seg på å jobbe med forskning og utdanning under mer krevende forhold i årene som kommer.

### Forskningssamarbeid

Russland, Kina og Iran er de landene som utfordrer forskningssektoren mest – hver på sin måte.

- Russland forsøker å utnytte forskningsmiljøer for å få innsikt i norsk sikkerhetspolitikk og kritisk infrastruktur, særlig med søkelys på Nordområdene.
- Kina utnytter forsknings- og utviklingssamarbeid til fordel for å bygge egen militære kapasitet, samt posisjonere seg i Nordområdene gjennom forskningssamarbeid.
- Både Russland og Iran vil forsøke å omgå sanksjoner for å få tilgang på teknologi.
- Iran vil true alle som kritiserer iranske myndigheter.

---

**Postadresse**  
Postboks 8900  
7491 TRONDHEIM

**Org.nr. 974 767 880**  
E-post:  
postmottak@ntnu.no  
<http://www.ntnu.no>

**Besøksadresse**

**Telefon**  
+47 73 59 50 00

**Saksbehandler**  
Vidar Synstad

Tlf: +47

Bruk av sivil teknologi i militære våpenprogram er i dag et globalt fenomen. Dette gjelder også kjemiske og biologiske våpen. Forskningsmiljøer i autoritære regimer vil ikke nødvendigvis være åpne om at sivil forskning skal brukes til militære formål. Forskere -både norske og utenlandske – kan dermed være delaktig i dette uten å vite det. Det kan skje gjennom å utnytte gjesteforskningsordninger eller tilganger til spesialiserte laboratorier utover det som er avtalt.

NTNU bør...

- Bevisstgjøre og sette forskere og ledere i stand til å inngå samarbeid på en ansvarlig måte
- Hegne om akademisk frihet.
- Spre kunnskap internt om regelverk for eksportkontroll og sanksjoner.
- Balansere hensynet til norsk politikk for internasjonalt forskningssamarbeid med sikkerhetshensyn - så åpen institusjon som mulig, og så sikker som nødvendig.
- Ta vare på medarbeidere og studenter fra land som er nevnt i trusselvurderingene, og sørge for at de er inkludert i et godt arbeids- og studiemiljø.

### Digitale trusler

Russland, Kina, Iran og Nord-Korea er de mest fremtredende landene som gjennomfører digitale etterretningsoperasjoner mot Norge. Dette gjør de både for å innhente informasjon de ellers ikke har tilgang til, men også for å forberede og gjennomføre digitale sabotasjeaksjoner i den hensikt å skape kaos i det norske samfunnet. Likevel er det fremdeles organiserte kriminelle som utgjør den største trusselen mot NTNU sin digitale infrastruktur.

NTNU bør...

- Etterleve retningslinjene i styringssystemet for informasjonssikkerhet og personvern.
- Ha fokus på digital grunnmur og fornyelse av IKT-infrastruktur.
- Gi opplæring og bevisstgjøre studenter og ansatte på hvor og hvordan de lagrer og behandler data på en forsvarlig måte.
- Gjøre risiko- og sårbarhetsvurderinger av nye systemer før de tas i bruk.

### Rekruttering av personer

Utenlandske etterretningstjenester jobber kontinuerlig for å rekruttere personer med tilgang til sensitiv informasjon eller tilgang til beslutningsprosesser. Alle som har tilgang til noe som etterretningstjenestene ønsker seg er utsatt, uavhengig av nasjonalitet. Dette gjelder derfor også nordmenn.

Russland og Kina vil forsøke å rekruttere personer for å få informasjon om dissidenter og regimekritikere.

Ansatte og studenter med knytninger til autoritære regimer kan være ekstra sårbare for rekrutteringsforsøk.

NTNU bør...

- Gjøre ansatte og studenter bevisste på hva de har tilgang til og sette de i stand til å vurdere hvem de samarbeider med og med hvilke betingelser.
- Vurdere sikkerhetshensyn i ansettelsesprosesser.

- Ledere må utvikle inkluderende arbeidsmiljø. Ansatte fra land pekt på i trusselvurderinger skal på lik linje med øvrige ansatte ha et arbeidsmiljø preget av tillit og inkludering.

### **Terrorisme**

Trusselbildet for terror er komplekst og uforutsigbart, og at én eller flere personer kan gjennomføre terrorhandlinger mot Norge i 2026. Psykisk ustabilitet og radikaliserings blant unge på nett er den største risikoen for terrorhandlinger.

Det er ingenting i årets trusselvurderinger som fremhever universitetene som særskilte mål for terrorhandlinger. Likevel har NTNU store ansamlinger av mennesker på campus hver eneste dag. Dette kan være en sårbar situasjon.

NTNU bør...

- Legge til rette for at man skal kunne ytre seg på campus.
- Øve jevnlig på håndtering av krisehendelser.
- Gi ansatte kompetanse og bevissthet på hvordan de skal ivareta egen sikkerhet i situasjoner de opplever trusler og vold.

### **Sikkerhetskultur**

NSM fremhever i sin risikorapport at sikkerhet er et lederansvar og må omfatte alle fagområder. En god sikkerhetskultur skapes gjennom å ivareta ansatte og gi de nødvendig kunnskap om hvordan de skal gjøre jobben sin på en forsvarlig måte.

NTNU bør...

- Styrke kunnskapen og bevisstheten blant ledere for deres ansvar for å ivareta sikkerhet i daglig virke.
- Studenter og ansatte må settes i stand til å ha et bevisst forhold til hvordan de kan gjennomføre sine daglige gjøremål på en forsvarlig måte.
- Ledere må normalisere arbeidet med sikkerhet gjennom å sette sikkerhet på agendaen i arbeidshverdagen.