

Til Justis og beredskapsdepartementet

Næringslivets innspill til nasjonal strategi mot voldelig ekstremisme og terror

Innledning.

Næringslivets Sikkerhetsråd (NSR) takker for invitasjonen til å gi innspill til ny nasjonal strategi mot voldelig ekstremisme og terror. NSR eies av NHO, Virke, Spekter, Finans Norge, Norges Rederiforbund og Den Norske Krigsforsikring for Skip. Innspillet er utarbeidet i dialog med eierne og et utvalg medlemsvirksomheter.

Grunntanken bak innspillet er at næringslivet er langt mer enn et mulig mål for voldelig ekstremisme og terror. Private virksomheter eier og drifter en betydelig del av samfunnets kritiske funksjoner, infrastruktur og verdikjeder. De er arbeidsplass for flertallet av norske arbeidstakere, og dermed en arena der bekymringstegn kan fanges opp tidlig. Næringslivet rår også over kapasiteter som myndighetene trenger når en hendelse inntreffer, fordi myndighetenes ressurser er begrenset. Politiet og andre sikkerhetsmyndigheter kan ikke være til stede overalt til enhver tid, og i den innledende fasen av en hendelse vil virksomhetenes egen evne til å varsle, beskytte og handle ofte være avgjørende.

Til tross for det har næringslivet ingen tydelig plass i det strategiske rammeverket. I Meld. St. 13 *Forebygging av ekstremisme*, nevnes næringslivet hovedsakelig som arena for arbeidsdeltakelse¹, og kontraterrorstrategiens næringslivstiltak har i stor grad stått som utredningsoppdrag siden 2022.²

En tydeligere rolle for næringslivet må gå begge veier. Strategien bør beskrive hva samfunnet kan forvente av virksomhetenes egen sikkerhets- og beredskapsevne, tilpasset de kritiske funksjoner de ivaretar. Den bør også beskrive hva virksomhetene kan forvente av myndighetene som for eksempel handlingsrettet trusselinformasjon, rettslig klarhet, tilstrekkelige virkemidler og støtte mot trusselaktører ingen virksomhet kan håndtere alene. NSR ber derfor om at strategien får et eget kapittel om næringslivets rolle, med tydelige forventninger begge veier.

Innspillet besvarer departementets fire spørsmål og munner ut i tre strategiske prioriteringer: å styrke samfunnets motstandskraft mot radikalisering og ekstremisme, å styrke beskyttelse og

¹ Meld. St. 13 (2024–2025) *Forebygging av ekstremisme*, kap. 4.2.3 og 5.1.6.

² Nasjonal kontraterrorstrategi (revidert 2022), innsatsområde 3 og 5, tiltak 13, 14, 17, 27, 28 og 31, s. 19–21.

motstandskraft til kritisk infrastruktur og samfunnskritiske funksjoner, og å etablere et mer forpliktende offentlig–privat samarbeid.

NSR vil også understreke betydningen av selve prosessen. Skal strategien etablere nye forventninger til næringslivet, bør den bygge på innsikt i de sårbarhetene og operative realitetene virksomhetene møter i praksis. NSR stiller seg gjerne til disposisjon i det videre arbeidet, for eksempel gjennom en referansegruppe for utforming og gjennomføring av strategien.

Spørsmål 1: Hva bør en ny strategi si om næringslivets rolle?

Strategien bør fastslå at næringslivet er en sentral og selvstendig aktør med egen rolle, ansvar og myndighet i fellesskapets arbeid mot radikaliserings, voldelig ekstremisme og terrorisme, og ikke bare en mottaker av råd eller et mulig mål. Dette gjelder særlig virksomheter som forvalter kritisk infrastruktur, kritiske forsyningskjeder, teknologi og samfunnsviktige tjenester. Strategien bør beskrive virksomhetenes roller i forebygging, beskyttelse, håndtering og gjenoppretting, tydeliggjøre hva myndighetene forventer, og hva næringslivet kan forvente tilbake.

1. Virksomheten som mål og eier av sårbarheter. Aktører innen handel, kjøpesentre, utesteder, arrangementer, transport og eiendom forvalter mange av de åpne byrommene der lavteknologiske angrep mot folkemengder er mest sannsynlig.

Virksomheter med kritiske funksjoner, symbolverdi eller tilknytning til Israel, USA eller støtten til Ukraina er i tillegg til voldelig ekstremisme og terrorisme, også aktuelle mål for statlig styrt sabotasje. Det samme gjelder virksomheter som kan bli mål på grunn av hva de produserer, som forsvarsindustri, energi, mineralutvinning og produksjon av kritiske innsatsfaktorer. Strategien bør slå fast at virksomhetene har ansvar for å gjennomføre risikobaserte egenbeskyttelsestiltak innenfor sine rettslige, økonomiske og operative rammer. Samtidig må den anerkjenne at næringslivet ikke alene kan beskytte seg mot avanserte statlige eller statlig støttede trusselaktører. Myndighetene må derfor bidra med lovgivning, handlingsrettet trussel- og sikringsinformasjon og nødvendig støtte og bistand ved de mest alvorlige truslene.

2. Virksomheten som førstelinje. Arbeidsgivere, vektere, banker og betalingsforetak, utleievirksomheter og logistikkelskaper, forhandlere av kjemikalier og droner, telekom og digitale plattformer ser bekymringstegn og forberedelseshandlinger som myndighetene ikke ser. Strategien bør gjøre det enklere og rettslig trygt å melde fra, og samtidig trekke en tydelig grense. Næringslivet skal være årvåkent, ikke overvåke. Ansattes personvern og ytringsfrihet respekteres, men kan ikke være en unnskyldning for ikke å handle på tydelige og definerte indikatorer. Ansattes personvern og ytringsfrihet skal respekteres, samtidig som virksomhetene må kunne handle på tydelige og definerte indikatorer.

3. Arbeidslivet som forebyggende arena. Det å ha jobb å gå til, og en inntekt å leve av, er viktige beskyttelsesfaktorer mot mange typer utenforskap.³ Arbeid gir tilhørighet, struktur og et alternativ til ekstreme fellesskap. Strategien bør derfor løfte arbeidsgivere som partnere i inkludering og i exit- og reintegreringsarbeid, med støtte og veiledning når de ansetter personer med slik bakgrunn.

4. Næringslivet som ressurs i håndtering og gjenoppretting. Private aktører rår over vakthold, logistikk, helsetjenester, kommunikasjonsinfrastruktur og eiendom som politiet og kommunene trenger under og etter et angrep. Dette er det samme mulighetsrommet som Nasjonal sikkerhetsstrategi peker på for totalforsvaret. Strategien bør følge opp kontraterrorstrategiens tiltak 31 med konkrete avtaler, ikke flere utredninger.⁴

³ Meld. St. 13 (2024–2025), kap. 5.1.7, s. 37, som bygger på NOU 2024: 3 Felles innsats mot ekstremisme.

⁴ Nasjonal sikkerhetsstrategi (2025), s. 18; Nasjonal kontraterrorstrategi (revidert 2022), tiltak 31, s. 21.

Strategien bør også omtale virksomhetenes egen evne til å varsle, beskytte og handle i den innledende fasen av en hendelse, før offentlige ressurser er på plass.

Et gjennomgående prinsipp: Dagens trusselbilde gjør næringslivet til en integrert del av Norges samlede sikkerhet og beredskap. Rollene bør forankres i samme strukturer som brukes i totalforsvaret, slik at offentlige og private aktører sammen styrker samfunnets motstandskraft, beskytter kritisk infrastruktur og opprettholder viktige samfunnsfunksjoner i fred, krise, væpnet konflikt og krig. Virksomhetene bør møte én samlet sikkerhetsforventning fra staten, ikke parallelle regimer for terror, sabotasje, krise og krig.

Spørsmål 2: Hvilke trusler, sårbarheter og utviklingstrekk bør det tas særlig hensyn til:

PST peker på et mer sammensatt trusselbilde, der radikalisering i økende grad skjer digitalt, voldsfascinasjon og ideologi blandes, og skillet mellom terror, statlig sikkerhetstruende virksomhet og organisert kriminalitet blir mindre tydelig. For virksomhetene kan angrepsmåter og enkelte sårbarheter være sammenfallende, men aktør, motivasjon og oppdragsgiver har stor betydning for hvilket trusselnivå virksomheten må kunne motstå, mulige konsekvenser og hvilken støtte som kreves fra myndighetene. Strategien bør derfor omfatte digital radikalisering, Strategien bør derfor omfatte digital radikalisering, sammensatte trusler der statlige aktører, kriminelle nettverk og ekstremister i økende grad flyter sammen, kritisk infrastruktur som mål, innsiderisiko og hvordan polarisering og desinformasjon kan svekke tillit og øke samfunnets sårbarhet.⁵

1. Konvergens, stedfortredere og et bredt angrepsspekter. Nasjonal sikkerhetsstrategi beskriver hvordan statlige aktører finansierer radikalisererte miljøer og kriminelle nettverk og bruker dem til å utføre handlinger på sine vegne. PST vurderte i april 2026 det som *sannsynlig* at iranske tjenester vil bruke stedfortredere til angrep i Norge, og Russland bruker stedfortredere til sabotasje mot infrastruktur og logistikk. Trusselen kan også rettes direkte mot enkeltpersoner, blant annet ledere og nøkkelpersonell i europeisk forsvarsindustri, personer som støtter Ukraina, og russiske dissidenter. Det rapporterte attentatkomplottet mot Rheinmetall-sjef Armin Papperger i 2024 og nyere advarsler fra europeiske sikkerhets- og etterretningstjenester viser at kartlegging, trusler og planlagte voldshandlinger mot personer inngår i det bredere russiske virkemiddelapparatet, og er trolig mer aktuelt enn tidligere.⁶ En sabotasjehandling kan samtidig være en terrorhandling dersom formålet er å skape alvorlig frykt eller påvirke myndigheter eller samfunn. Strategien bør derfor favne relevante angrepsformer som kidnapping, drap, attentat, kapring, bombeangrep, skyting, brannstiftelse og sabotasje, og avklare hvordan statlig initierte eller støttede terrorhandlinger omfattes. Dette rammer virksomheter direkte, og krever at terror- og sabotasjevern ses i sammenheng, uten at forskjeller mellom aktører, intensjon og nødvendig myndighetsrespons viskes ut.

2. Virksomheter som blir mål på grunn av hva de gjør. Forsvarsindustri som understøtter Ukrainas forsvar, energiprodusenter både fornybare og fossile, virksomheter som utvinner og foredler mineraler og produsenter av kritiske innsatsfaktorer med sivil og militær bruk, kan bli mål på grunn av det de produserer. Trusselen kan komme fra statlige aktører gjennom stedfortredere, og fra ideologisk motiverte miljøer. Virkemidlene er ofte de samme; trusler om vold, skadeverk, brannstiftelse og sabotasje. Tilsvarende virksomheter har vært utsatt for dette i flere europeiske land de siste årene. Truslene kan også rettes mot ansatte og deres familier, blant annet gjennom kartlegging og offentliggjøring av personopplysninger. Nasjonal sikkerhetsstrategi omtaler disse virksomhetene som del av den økonomiske sikkerheten, men de har ingen plass i rammeverket mot

⁵ PST, Nasjonal trusselvurdering 2026, kap. 2, s. 31

⁶ Financial Times, October 11, 2026, «Russia steps up bid to kill European defence chiefs, spy agencies warn».

voldelig ekstremisme og terror. Strategien bør se dette i sammenheng. Den bør samtidig slå fast at lovlig protest og sivil ulydighet mot slik virksomhet ikke er ekstremisme; grensen går ved vold, trusler om vold og sabotasje.

3. Unge utsatt for raske, digitale radikaliseringsløp. Mindreårige var involvert i nesten halvparten av gjennomførte og avvergede høyreekstreme angrep i Vesten i 2025, og radikaliseringen skjer i digitale nettverk, på spillplattformer og i krypterte kanaler. Radikaliseringen går raskt, og er vanskelig å oppdage.⁷ Det flytter forebyggingen ut av de tradisjonelle sporene, og øker betydningen av aktører som ser det myndighetene ikke ser.

4. Åpne byrom og folkemengder. Lavteknologiske angrep med kniv, kjøretøy eller skytevåpen mot sivile i offentlige rom er den mest sannsynlige angrepsformen. Ansvar for sikring av offentlige områder mellom stat, kommune og private eiere er fortsatt uavklart, fire år etter at kontraterrorstrategien (tiltak 27) ba om en avklaring.⁸

5. Innsiderisiko. Personer med legitim tilgang til kritiske funksjoner, sensitiv informasjon, systemer eller fysiske anlegg kan bli radikalisert, påvirket, presset eller rekruttert. Dette er en reell sårbarhet, særlig fordi virksomheter utenfor sikkerhetsloven har begrensede rettslige virkemidler for personellkontroll og ofte er usikre på hva de har adgang til å gjøre. Strategien bør derfor se forebygging av radikalisering og personellsikkerhet i sammenheng og gi virksomhetene tydelig veiledning om tidlig varsling og håndtering.

6. Ny teknologi som senker terskelen. Droner, kunstig intelligens i planlegging og propaganda, 3D-printede våpen og digitale angrep mot fysiske systemer gjør angrep billigere og vanskeligere å avdekke forberedelsene til. Næringslivet er både produsent, forhandler og mål for denne teknologien. Droner brukes i økende grad til kartlegging, overvåkning og påvirkning, og som plattform for sabotasje og andre fysiske angrep. Det rapporterte droneangrepet mot Leipzig/Halle lufthavn i 2026 illustrerer hvordan droner kan brukes mot kritisk infrastruktur og strategiske logistikkfunksjoner.⁹ Strategien bør derfor omfatte forebygging, deteksjon, varsling og håndtering av uønsket droneaktivitet som en integrert del av beskyttelsen av kritisk infrastruktur og samfunnskritiske funksjoner. Teknologikutviklingen går samtidig raskere enn lov- og regelverksutviklingen, noe som kan skape uklarhet om ansvar, forebyggende tiltak, informasjonsdeling og myndighetenes adgang til å gripe inn. Strategien bør derfor legge opp til regelmessig vurdering og raskere tilpasning av relevante rettslige og regulatoriske virkemidler.

7. Terrorfinansiering i nye kanaler. Penger sendes via digitale betalingstjenester, kryptovaluta og utenlandske aktører som ikke er rapporteringspliktige i Norge. De rapporteringspliktige får for lite tilbakemelding og typologier fra myndighetene til å treffe godt.¹⁰

8. Polarisering, desinformasjon og påvirkning. Polarisering, utenforskap, desinformasjon og påvirkningsoperasjoner kan bidra til radikalisering, og svekke tilliten som er en sentral styrke i det norske samfunnet. Strategien bør derfor koble forebygging av voldelig ekstremisme tettere til arbeidet med demokratisk motstandskraft, kildekritikk og beskyttelse mot påvirkning.

En tverrgående sårbarhet: Små og mellomstore virksomheter har sjelden tilstrekkelig sikkerhetskompetanse i egen organisasjon. De får ikke tilgang til gradert trusselinformasjon med mindre de er underlagt sikkerhetsloven. Manglende kompetanse og mange oppgaver som skal løses samtidig, leder ofte til at disse virksomhetene ikke rapporterer mistenkelige eller ubehagelige hendelser til myndighetene. Samtidig kan virksomhetene inngå i verdikjeden til virksomheter som

⁷ PST, Nasjonal trusselvurdering 2026, s. 9 og 39.

⁸ PST, Nasjonal trusselvurdering 2026, s. 37; Nasjonal kontraterrorstrategi (revidert 2022), tiltak 27, s. 21.

⁹ Financial Times, September 1, 2026, "Germany blames Russia for Leipzig drone attack".

¹⁰ PST, Nasjonal trusselvurdering 2026, s. 35; Meld. St. 13 (2024–2025), boks 4.3.

fyller en eller flere kritiske nasjonale funksjoner eller behov. Strategien bør ta utgangspunkt i der sårbarheten er størst, og ikke hos de store virksomhetene som allerede har egne sikkerhetsorganisasjoner og et strukturert sikkerhetsarbeid.

Spørsmål 3: Hvordan kan samarbeidet videreutvikles?

Samarbeidet må bli mer systematisk og proaktivt, og mindre hendelsesstyrt. Det bør gå fra enveis trusselformidling til et forpliktende, toveis partnerskap med etablerte strukturer, klare kontaktpunkter, tydelige varslingskanaler og rettslig trygghet for informasjonsdeling. Strategien bør legge til rette for rask og forutsigbar deling av sikkerhetsrelevant informasjon ved endringer i trusselbildet, felles øvelser og faste arenaer for erfaringsutveksling. For virksomheter med samfunnskritiske funksjoner er det særlig viktig at PST, politiet, NSM og infrastruktureierne raskt kan etablere en felles situasjonsforståelse.

Etabler en fast strategisk arena. Strategien bør etablere et nasjonalt samarbeidsforum for næringsliv og kontraterror, ledet av JD med PST, Politidirektoratet, NSM, DSB og det nye nasjonale senteret mot radikaliserings og voldelig ekstremisme, og med næringslivets hovedorganisasjoner som medlemmer. NSR kan være næringslivets kontaktpunkt. Forumet kan kobles til næringslivets observatørrolle i Sentralt totalforsvarsforum, slik at terror, sabotasje og krise håndteres i samme struktur. NSR er kjent med at STFes rolle og oppgaver er under revisjon av DSB og Forsvaret, og kan bli endret.

Gjør trusselinformasjonen handlingsrettet og bransjetilpasset. De åpne trusselvurderingene fra PST, E-tjenesten og NSM er gode, men forteller sjelden en kjøpesenterdirektør eller en logistikksjef hva de bør gjøre. Kontraterrorstrategiens tiltak 12–14 og 17 bør følges opp med en fast rådgivningsfunksjon for sikring mot terror, én tydelig adresse for virksomhetene, og bransjevise trusselbriefinger.¹¹

Reduser graderingsbarrieren. Flere nøkkelpersoner i virksomheter med kritiske funksjoner bør sikkerhetsklareres, slik at myndighetene kan dele gradert informasjon når det trengs, ikke først etter en hendelse.

Gjør det rettslig trygt å dele begge veier. Veilederen om taushetsplikt og informasjonsdeling som Meld. St. 13 beskriver, bør også omfatte private aktører. Hva kan en arbeidsgiver melde, til hvem, og hvordan skal ansattes personvern ivaretas? Den nasjonale funksjonen for trusselformidling og tiltaksrådgivning¹² og det nasjonale senteret mot radikaliserings og voldelig ekstremisme bør ha et uttrykkelig mandat til å veilede arbeidsgivere ved bekymring.¹³

Styrk det lokale samarbeidet. Politiråd og andre former for lokalt samarbeid bør systematisk inkludere næringslivet der det er relevant, og lokale kontraterrorøvelser bør ha private aktører med som hovedregel, ikke unntak (tiltak 28).¹⁴

Formaliser private ressurser i håndtering. Utredningen etter tiltak 31 bør ferdigstilles og følges opp med rammeavtaler og forhåndsplanlagte bidrag fra vaktsselskaper, eiendomsforvaltere, transport og helse.¹⁵

Mål effekten. Samarbeidet bør evalueres jevnlig med enkle indikatorer – for eksempel andel virksomheter som kjenner trusselbildet for sin bransje, antall bekymringsmeldinger fra arbeidsgivere og deltakelse i øvelser.

¹¹ Nasjonal kontraterrorstrategi (revidert 2022), tiltak 12–14 og 17, s. 19.

¹² Nasjonal kontraterrorstrategi (revidert 2022), tiltak 14, s. 19

¹³ Meld. St. 13 (2024–2025), kap. 1.3 (s. 9), 4.2.1 og 4.2.2.

¹⁴ Meld. St. 13 (2024–2025), kap. 4.2.3; Nasjonal kontraterrorstrategi (revidert 2022), tiltak 28, s. 21.

¹⁵ Nasjonal kontraterrorstrategi (revidert 2022), tiltak 31, s. 21.

Spørsmål 4: Hva er de tre viktigste strategiske prioriteringene for å styrke næringslivets bidrag til forebygging og beredskap mot voldelig ekstremisme og terrorisme

De tre viktigste prioriteringene bør være å styrke samfunnets motstandskraft mot radikaliserings og ekstremisme, styrke beskyttelsen og motstandskraften til kritisk infrastruktur og samfunnskritiske funksjoner, og etablere et mer forpliktende offentlig–privat samarbeid. Prioriteringene henger sammen: Tidlig forebygging reduserer risiko, robuste virksomheter begrenser konsekvenser og opprettholder viktige funksjoner, og et forpliktende samarbeid gir aktørene nødvendig informasjon, støtte og felles situasjonsforståelse.

Prioritering 1 – Styrk samfunnets motstandskraft mot radikaliserings og ekstremisme. Strategien bør øke kunnskap, bevissthet og evne til tidlig identifisering av bekymringsutvikling i både offentlige og private virksomheter. Arbeidsgivere bør få tydelig veiledning om inkluderende arbeidsmiljøer, sikkerhetskultur, tidlig varsling og grensen mellom nødvendig årvåkenhet og overvåking.

Prioritering 2 – Styrk beskyttelsen og motstandskraften til kritisk infrastruktur og samfunnskritiske funksjoner. Næringslivet kan ikke alene beskytte seg mot de mest alvorlige trusselaktørene, herunder statlige aktører og deres stedfortredere. Strategien bør styrke virksomhetenes evne til å forebygge og håndtere angrep, redusere sårbarheter, begrense konsekvenser og raskt gjenopprette kritiske og samfunnsviktige funksjoner. Dette forutsetter nødvendig støtte og bistand fra myndighetene, sektorvise trusselvurderinger, handlingsrettede råd og samordnede øvelser. Strategien bør samtidig avklare hvilke forventninger samfunnet skal ha til virksomhetenes egen sikkerhets- og beredskapsevne, tilpasset kritikalitet, og gi virksomhetene de virkemidlene som trengs for å innfri dem. Sammen med næringslivet bør det også utredes om en forholdsmessig beskyttelsesplikt for større publikumsarenaer etter britisk modell er hensiktsmessig i Norge.

Prioritering 3 – Etabler et mer forpliktende offentlig–privat samarbeid. Det bør etableres faste og robuste mekanismer for informasjonsdeling, felles situasjonsforståelse, øving og koordinering mellom myndighetene og næringslivet – både i det løpende forebyggende arbeidet og ved alvorlige hendelser. Virksomhetene bør møte én samlet sikkerhetsforventning fra staten – ikke parallelle regimer for terror, sabotasje, krise og krig. Samarbeidet bør omfatte en fast strategisk arena, én tydelig adresse for råd om sikring, bransjetilpasset trusselinformasjon, nødvendige ordninger for sikkerhetsklarering og rettslig trygghet for informasjonsdeling. Strukturene bør bygge på totalforsvarets arenaer, ikke utvikles ved siden av dem. Næringslivets rolle og de gjensidige forventningene bør beskrives i et eget kapittel i strategien.

Oslo, 15. oktober 2026

Odin Johannessen
Direktør
Næringslivets sikkerhetsråd