PST

Nasjonal trusselvurdering

2026

Formålet med Nasjonal trusselvurdering

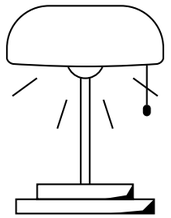
I Nasjonal trusselvurdering (NTV) gjør PST rede for den forventede trusselen fra statlige aktører og ekstremister samt trusselen mot myndighetspersoner i Norge det kommende året. Formålet er å skape en felles nasjonal forståelse av trusselen mot rikets sikkerhet.

NTV skal også sette andre samfunnsaktører i stand til å beskytte seg mot trusler, blant annet ved å gi beslutningsstøtte til virksomheter i deres forebyggende sikkerhetsarbeid. Den norske beredskapen er et felles ansvar, og både offentlige og private virksomheter har en rolle i det som til sammen utgjør landets totalberedskap.

I tillegg skal NTV bidra til økt årvåkenhet i samfunnet. Tips fra publikum er viktig i arbeidet med å avverge og forebygge trusler mot Norge. Har du informasjon som bekymrer deg, og som du tror PST bør vite om, oppfordrer vi deg derfor til å tipse oss. Terskelen for å ta kontakt er lav.

Tips oss

pst.no/tips-oss



Innhold

Forord	4
Bruk av NTV i risikovurderinger	6
Sannsynlighetsord om politisk motivert vold	7
PSTs terrortrusselskala	7
Trusselbildet for 2026 i korte trekk	8
Trusselen fra statlige aktører	**11**
De sentrale trusselaktørene	12
Fremhevede metoder	22
Politisk motivert vold	**31**
Trusselen fra ekstrem islamisme	32
Trusselen fra høyreekstremisme	38
Antistatlig ekstremisme	44
Trusselen mot myndighetspersoner i Norge	**47**
EOS-tjenestene PST, Etterretningstjenesten og NSM	50

Forord

Norge befinner seg i den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig.

Beate Gangås
Sjef PST

Foto
Politiets sikkerhetstjeneste

Norge befinner seg i den mest alvorlige sikkerhetspolitiske situasjonen siden andre verdenskrig. I Nasjonal sikkerhetsstrategi, som regjeringen la frem i mai 2025, fremheves tre hovedprioriteringer i møte med økt sikkerhetspolitisk alvor. Disse er raskt styrket forsvarsevne, et mer motstandsdyktig samfunn og styrket økonomisk sikkerhet. Strategien påpeker at prioriteringene krever innsats fra hele samfunnet.

PSTs oppdrag er å forstå, formidle og motvirke de mest alvorlige truslene mot rikets sikkerhet. I Nasjonal trusselvurdering beskriver vi de truslene vi mener vil gjøre seg mest gjeldende i 2026. Sammen med Etterretningstjenestens «Fokus» og Nasjonal sikkerhetsmyndighets «Risiko» bidrar vår nasjonale ugraderte trusselvurdering til å gi samfunnet og befolkningen et felles situasjonsbilde.

I en tid der fremmede stater gjennomfører etterretningsoperasjoner og tar i bruk sammensatte virkemidler i Norge for å undergrave vår motstandsdyktighet, er forebyggende sikkerhet, etterretning og situasjonsforståelse viktig. Vi bør alle være årvåkne og bevisste på at slike trusler kan forekomme i vår egen hverdag.

Terrortrusselbildet er mer uoversiktlig og komplekst enn før. Det underbygges av at statlige aktører ved hjelp av proxyaktører kan forsøke å gjennomføre terrorhandlinger i Norge. Dette gjør det mer krevende å avdekke potensielle terrorhandlinger. Den mest alvorlige terrortrusselen kommer fortsatt fra ekstreme islamister og høyreekstremister. Vi ser også at antistatlige holdninger bidrar til radikalisering. Graden av ideologisk tilhørighet varierer, og for noen kan voldsfasinasjon være veien inn til ekstremisme heller enn omvendt. Det digitale rom er fortsatt den viktigste arenaen for radikalisering, og nettet tilrettelegger for at det knyttes kontakter på tvers av landegrenser. Vi forventer at den negative utviklingen knyttet til mindreårige og unge som radikaliseres, vil vedvare.

En rekke aktører må stille opp og samhandle om vi skal lykkes med å forebygge ekstremisme og verne om demokratiet. Jeg vil takke alle som har samarbeidet med PST om å forebygge alvorlige trusler.

Det er svært viktig for PST at folk har tillit til oss og tar kontakt når de har en bekymring. I 2025 fikk PST sin høyeste plassering noensinne i en omdømmemåling av offentlige virksomheter. Vi ønsker å vise oss den tilliten verdig. Det er vårt ansvar å bringe klarhet i om det foreligger en reell trussel. PSTs ansatte tar dette ansvaret på stort alvor.

PST beskriver et alvorlig trusselbilde. Vi ønsker å gi så konkret informasjon som vi kan, med de begrensningene vi har når det gjelder å dele graderte opplysninger. Åpenhet er viktig for PST. Truslene forsvinner ikke hvis vi ikke snakker om dem. Snarere kan de da utvikle seg uforstyrret.

Et felles situasjonsbilde gjør oss mer motstandsdyktige i en urolig tid.

Beate Gangås
Sjef PST

Bruk av NTV i risikovurderinger

Risiko kan vurderes på ulike måter. Vi legger til grunn at en risikovurdering i en virksomhet er en samlet vurdering av *verdiene* som skal beskyttes, aktuelle *trusler* og eksisterende *sårbarheter*.

Ved å kartlegge og vurdere verdiene sine systematisk får virksomheten et godt utgangspunkt for å vurdere hvilke trusler og sårbarheter som er relevante, og hvordan de kan påvirke verdiene. NTV beskriver et utvalg trusselaktører som kan være aktuelle. Den kan derfor brukes som grunnlag og beslutningsstøtte i trusselvurderingen. I tillegg må virksomheten ta høyde for andre trusler som kan påvirke den, som kriminalitet og andre typer uønskede hendelser.

Å vurdere sårbarheter innebærer å identifisere svakheter som kan gjøre virksomheten utsatt for påvirkning fra aktuelle trusler. I denne vurderingen er det også viktig å se på avhengigheter som befinner seg utenfor virksomheten, men som likevel inngår i verdikjeden. Det inkluderer underleverandører, for eksempel produsenter av adgangskort og leverandører av informasjonsbehandlings-programmer eller transporttjenester.

Den samlede vurderingen av faktorene verdier, trusler og sårbarheter gir grunnlag for å identifisere sannsynlighets- og konsekvensreduserende tiltak. Med slike tiltak kan virksomheten oppnå et forsvarlig sikkerhetsnivå.

Virksomheter med komplekse og sammensatte porteføljer bør gjennomføre strukturerte prosesser for å identifisere og beskrive aktuelle verdier, trusler og sårbarheter.

Hva menes med verdi, trussel og sårbarhet?

Verdi

Verdier kan strekke seg fra nasjonale sikkerhetsinteresser til virksomhetens egne interesser. Det kan for eksempel være liv og helse, natur, immaterielle verdier eller rett og slett virksomhetens funksjonsevne. Felles for alle verdier er at et tap eller midlertidig bortfall har negative konsekvenser for virksomheten eller for andre.

Trussel

En trussel er en tilsiktet handling som kan føre til en uønsket hendelse. For at noe skal kunne kalles en trussel, må aktøren som står bak, kunne påføre et tap av eller midlertidig bortfall av én eller flere verdier.

Sårbarhet

En sårbarhet er en manglende evne til å motstå en uønsket hendelse eller til å gjenoppta funksjon etter at en uønsket hendelse har oppstått. Sårbarheter er altså mangler som bidrar til at virkningen av en trussel blir unødvendig stor.

Sannsynlighetsord om politisk motivert vold

Innenfor fagfeltet politisk motivert vold – ekstremisme – bruker PST et sett med standardiserte sannsynlighetsord. Formålet med det er at vurderingene våre skal beskrive sannsynlighet på en mest mulig ensartet måte, for å redusere uklarhet og faren for misforståelser.

Standardisert uttrykk	Betydning
Meget sannsynlig	Det er meget god grunn til å forvente
Sannsynlig	Det er god grunn til å forvente
Mulig	Det er like sannsynlig som usannsynlig
Lite sannsynlig	Det er liten grunn til å forvente
Svært lite sannsynlig	Det er svært liten grunn til å forvente

PSTs terrortrusselskala

Terrortrusselskalaen gir et samlet bilde av hvordan PST vurderer terrortrusselsituasjonen i Norge. Mens sannsynlighetsordene beskriver hvor sannsynlige forsøk på terrorhandlinger er, angir skalaen hvor alvorlig situasjonen er.

Terrortrusselskalaen har fem nivåer. Når vi fastsetter eller endrer et nivå, bygger vi på en kvalitativ trusselvurdering. Vi vurderer hvordan relevante faktorer, aktører og hendelser påvirker situasjonen i Norge. I tillegg vurderer vi

- alvorlighetsgrad og skadepotensial ved en eventuell terrorhandling
- usikkerhet og omfang av mangler i etterretningen knyttet til aktuelle trusselaktører
- myndighetenes evne til å iverksette mottiltak før trusler eventuelt omsettes i handling

Med de fem terrortrusselnivåene forsøker vi å beskrive komplekse forhold på en enkel måte.

Nivå	Begrep og forklaring
5	**Kritisk** PSTs vurdering er at et terrorangrep er nært forestående, eller at et terrorangrep har blitt gjennomført og flere angrep kan inntreffe.
4	**Høy** PSTs vurdering er at én eller flere personer har konkrete og realistiske planer og tar konkrete skritt for å gjennomføre terrorangrep, og/eller at flere forhold forsterker terrortrusselen.
3	**Moderat** PSTs vurdering er at én eller flere personer har en intensjon om å gjennomføre terrorangrep, men uten å ha tatt konkrete skritt eller å ha realistiske planer, og/eller uten at noen forhold forsterker terrortrusselen.
2	**Lav** PSTs vurdering er at få personer ønsker å gjennomføre terrorangrep, og/eller at få forhold forsterker terrortrusselen.
1	**Ingen** PSTs vurdering er at ingen personer ønsker å gjennomføre terrorangrep, og at det ikke foreligger forhold som bidrar til en terrortrussel.

Trusselbildet for 2026 i korte trekk

Trusselen fra statlige aktører

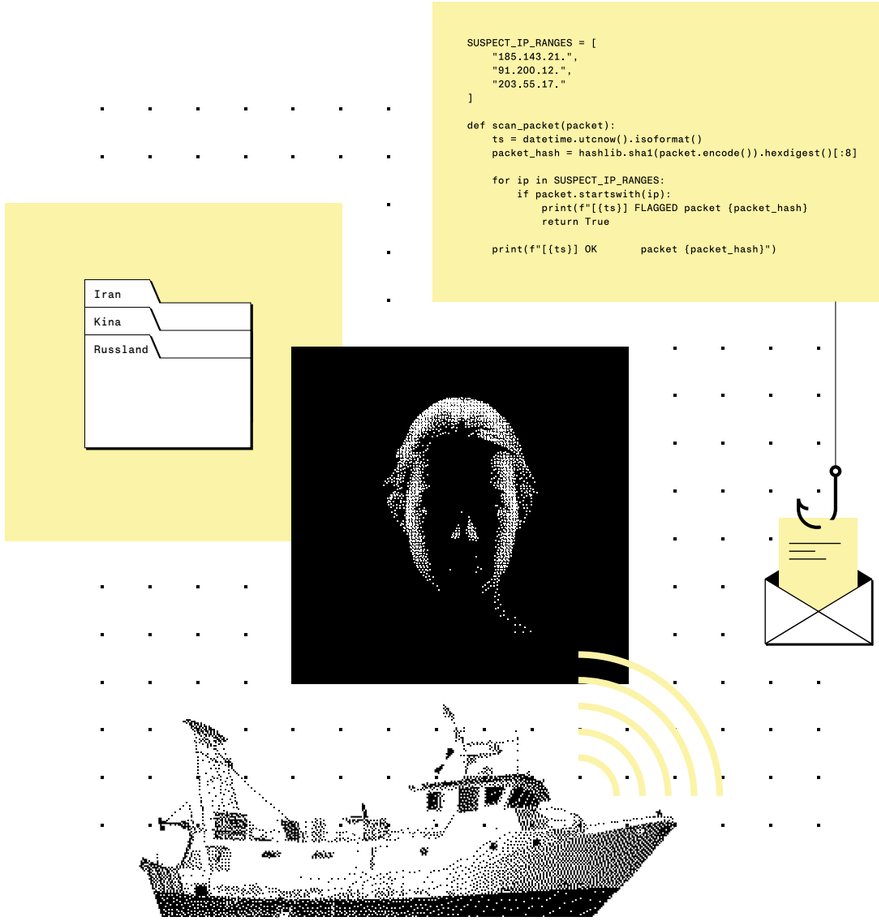
- De overordnede interessene og aktivitetene til statlige aktører i Norge vil vedvare i 2026.
- Den spente sikkerhetspolitiske situasjonen i Europa gjør at russisk etterretning har flere forhold av interesse knyttet til Norge og andre NATO-land. Med flere militære mål på norsk jord og mer alliert tilstedeværelse og øvingsaktivitet forventer vi mer aktivitet fra de russiske etterretningstjenestene.
- Russisk etterretning kan se seg tjent med å utføre sabotasjeaksjoner mot mål i Norge i 2026.
- I 2026 forventer vi en økning i russiske cyberoperasjoner, påvirkningsoperasjoner og rekrutteringsforsøk via digitale kanaler.
- Kinesiske sikkerhets- og etterretningstjenester har økt evne til å gjennomføre etterretningsoperasjoner i Norge, både cyberoperasjoner og innhenting av informasjon via menneskelige kilder.
- I 2026 vil kinesiske etterretningsaktører innhente informasjon, kartlegge norsk digital infrastruktur og true grupper og enkeltpersoner i befolkningen til å avstå fra kritikk av det kinesiske kommunistpartiet.
- Den største etterretningstrusselen fra Kina er i cyberdomenet.
- Vi forventer at iranske etterretnings- og sikkerhetstjenester vil gjennomføre etterretnings- og påvirkningsoperasjoner i Norge i 2026.
- Det iranske regimet kan også forsøke å angripe vestlige mål gjennom hærverk, målrettede attentater, terrorhandlinger eller destruktive cyberoperasjoner.
- For å gjennomføre operasjoner i Vesten benytter Iran seg av proxyaktører. I Norge kan de for eksempel bruke svenske kriminelle nettverk med tilstedeværelse her.

Politisk motivert vold

- Vi forventer fortsatt høy angrepsaktivitet fra ekstreme islamister i Vesten.
- Den islamske stat (IS) og al-Qaida søker primært å inspirere sympatisører til terrorhandlinger i Vesten.
- Personer i Norge vil fortsatt ha tilknytning til utenlandske ekstreme islamistiske nettverk.
- Norge er ikke fremtredende i fiendebildet til IS og al-Qaida, men har en sentral plass i fiendebildet til norske ekstreme islamister.
- Vi forventer at den høyreekstreme terroraktiviteten i Vesten vedvarer. Antallet mindreårige gjerningspersoner som deltok i terrorangrep i Vesten, økte markant i 2025.
- Mange som radikaliseres til høyreekstremisme, finner også inspirasjon i voldsforherligende ideer uten noen tydelig ideologisk forankring.
- Digitale plattformer fortsetter å være en hovedarena for rekruttering og radikalisering.
- Utfordringen med mindreårige og unge voksne som radikaliseres, forventes å fortsette i 2026.
- Sårbare enkeltindivider som radikaliseres kan bestemme seg for å utføre en terrorhandling. Særlig kan personlige forhold – som sårbarhet på grunn av psykisk uhelse, utenforskap og livskriser – påvirke personer til å handle.

Trusselen mot myndighetspersoner

- Det er lite sannsynlig at myndighetspersoner vil bli utsatt for alvorlige voldelige handlinger, men de vil bli utsatt for etterretningsvirksomhet, digitale trusler og hets.



Illustrasjon
Getty / Dinamo Design

Kapittel 01

Trusselen fra statlige aktører

Trusselbildet i Norge er komplekst og påvirkes av mange forhold både her i landet og globalt. Den sikkerhetspolitiske utviklingen er alvorlig og preget av mye usikkerhet. Dette gjenspeiles i vår vurdering av trusselen fra statlige aktører i Norge for 2026 – en trussel som er betydelig.

I 2026 forventer vi mer aktivitet i Norge fra russiske etterretningstjenester, med vedvarende fokus på militære mål og alliert øvingsaktivitet, norsk støtte til Ukraina samt nordområdene og Arktis. De vil bruke et bredt spekter av virkemidler, inkludert påvirkningsoperasjoner, sabotasje, rekruttering av menneskelige kilder og etterretningsaktivitet om bord i sivile fartøy.

Etterretningstrusselen fra Kina er betydelig, og vi ser at kinesiske sikkerhets- og etterretningstjenester har økt evne til å operere i Norge, både gjennom cyberoperasjoner og gjennom innhenting av informasjon via menneskelige kilder. Også iranske etterretningstjenester vil gjennomføre operasjoner i Norge i 2026.

Samtidig som PST viderefører fokuset på Russland, Kina og Iran, kan utviklingen i den sikkerhetspolitiske situasjonen påvirke hvilke statlige trusselaktører som opererer på norsk jord. En rekke faktorer, inklusiv geopolitisk rivalisering, har potensial til å aktualisere trusselen i Norge også fra andre land som ikke er nevnt i dette produktet.

Dette kapittelet består av to hoveddeler:

I den første fokuserer vi på **trusselaktørene**, spesifikt Russland, Kina og Iran. Vi beskriver utviklingen i trusselen fra disse landene det siste året og hvilke mål som er særlig utsatt i 2026.

I den andre delen ser vi på **seks sentrale metoder** som statlige trusselaktører – både de tre nevnte og andre – kan benytte i Norge. De seks metodene er:

- cyberoperasjoner
- rekruttering av menneskelige kilder
- transnasjonal undertrykkelse
- påvirkning
- ulovlige anskaffelser av sanksjonert og eksportkontrollert teknologi
- sikkerhetstruende økonomiske virkemidler

De sentrale trusselaktørene

Russland

Russland fokuserer fortsatt på militære mål og norsk støtte til Ukraina

Den spente sikkerhetspolitiske situasjonen i Europa fører til at russisk etterretning har flere forhold av interesse knyttet til Norge og andre NATO-land. Russiske etterretningstjenester har i mange år fulgt nøye med på militære mål og alliertes aktivitet og kapasiteter i Norge. Med flere militære mål på norsk jord og mer alliert tilstedeværelse og øvingsaktivitet forventer vi mer aktivitet fra de russiske etterretningstjenestene. De kartlegger blant annet vår kritiske infrastruktur og identifiserer sårbarheter. Det de finner, kan senere bli utnyttet i etterretnings-, påvirknings- og sabotasjeaktivitet. I ytterste konsekvens kan Russland bruke det til sin fordel i en fremtidig væpnet konflikt.

> *Med flere militære mål på norsk jord og mer alliert tilstedeværelse og øvingsaktivitet, forventer vi mer aktivitet fra de russiske etterretningstjenestene*

Norsk støtte til Ukraina vil fremdeles prege etterretnings- og påvirkningstrusselen fra Russland. Forsvaret og en rekke statlige og private aktører er blant målene for denne aktiviteten – særlig når det gjelder informasjon om militær og sivil støtte, inkludert norske leveranser av våpen og annet materiell til Ukraina. I tillegg til å innhente informasjon vil russiske etterretnings- og sikkerhetstjenester trolig forsøke å forstyrre og forhindre denne støtten. Politiske beslutningsprosesser og den norske meningsdannelsen er mål for russiske påvirkningsoperasjoner. Hensikten er blant annet å svekke oppslutningen om norsk støtte til Ukraina.

Russland bruker et bredt spekter av virkemidler

Sanksjoner som følge av Russlands fullskalakrig mot Ukraina har redusert handlingsrommet for russiske etterretningstjenester på norsk jord. Norske myndigheter har siden 2022 redusert antallet russiske etterretningsoffiserer under diplomatisk dekke. Samtidig er diplomatiet fremdeles en viktig plattform for russisk etterretning. Strengere innreiseregler for russiske statsborgere og begrenset tilgang til anløp ved norske havner har innskrenket russiske etterretningstjenesters mulighetsrom for enkelte former for etterretningsaktivitet.

Norske mottiltak og mer årvåkenhet i den norske befolkningen gjør at russiske etterretningstjenester må finne nye metoder for å innhente informasjon. Vi ser at russiske etterretningstjenester bruker et bredt spekter av virkemidler, og at metoder justeres og tilpasses fortløpende. I 2026 forventer vi en økning i antallet cyberoperasjoner, påvirkningsoperasjoner og rekrutteringsforsøk via digitale kanaler.

Russisk etterretning vil også forsøke å øke sin tilstedeværelse på norsk territorium i 2026. Vi forventer at etterretningsoffiserer under diplomatisk dekke vil rekruttere kilder og bedrive innhenting. Tilreisende personer vil også bli brukt for etterretnings- og påvirkningsaktivitet.

■

Vi ser med økende bekymring på at russiske etterretnings- og sikkerhetstjenester forsøker å rekruttere ukrainske flyktninger i Norge til å gi dem informasjon eller utføre annen ulovlig virksomhet på deres vegne. Forsøkene retter seg først og fremst mot ukrainske borgere som kan utsettes for press eller trues til samarbeid. Det kan for eksempel skje gjennom trusler mot gjenværende familie eller eiendom i russiskokkuperte områder av Ukraina. De russiske etterretnings- og sikkerhetstjenestene kan også lokke med belønning eller opptre på en fordekt måte, slik at de som blir rekruttert på vegne av Russland, ikke nødvendigvis er klar over det selv.

Med omtrent 100 000 ukrainske flyktninger i Norge forventer vi at russiske etterretnings- og sikkerhetstjenesters forsøk på å rekruttere ukrainere vil bli en særskilt utfordring.

Sabotasje med hensikt å skape uro og påvirke

Russisk etterretning kan se seg tjent med å utføre sabotasjeaksjoner mot mål i Norge i 2026. De mest sannsynlige målene for slike aksjoner er eiendom og logistikkinfrastruktur knyttet til støtte til Ukraina, men også sivil infrastruktur kan rammes. Hensikten vil være å skape uro i samfunnet og utøve press mot evnen og viljen til å støtte Ukraina. Sabotasje kan også bli brukt for å påvirke.

Den sikkerhetspolitiske situasjonen og behovet for å utvide spekteret av virkemidler fører til en økt risikovilje blant russiske etterretningstjenester. Vi har de siste årene sett flere eksempler på gjennomføring av sabotasje og forstyrrende aktiviteter i Europa, med en liten nedgang i antall hendelser i 2025. Sabotasje og forstyrrende aktiviteter utføres ofte av **proxyaktører**. Det dreier seg om hendelser der formålet er å ødelegge eller alvorlig forstyrre mål av samfunnsmessig betydning. Det kan også dreie seg om mindre alvorlige hendelser, som skadeverk og spredning av propaganda, der hensikten er å skape uro i samfunnet.

Russiske mannskap utfører etterretningsaktivitet om bord på sivile fartøy

Norges kyst og havområder er av strategisk interesse også for andre stater. Russiske etterretningstjenester vil i 2026 ønske å samle inn informasjon om infrastruktur, teknologi og aktivitet langs norskekysten. For å skjule etterretningsaktiviteten vil de bruke sivile fartøy. Denne typen aktivitet kalles maritim fordekt etterretningsaktivitet (MFEA), og retter seg mot norske interesser på havet, i indre farvann og ved havner.

Russiske fartøy er underlagt omfattende restriksjoner og har ikke tilgang til havner på norsk fastland. Unntaket er russiske fiskefartøy i Båtsfjord, Kirkenes og Tromsø, men også deres tilgang er strengt begrenset. Russiske mannskap om bord på sivile fartøy registrert i et tredjeland utgjør en betydelig trussel innen MFEA i 2026.

Proxyaktører er personer eller organisasjoner uten formell tilknytning til etterretnings- og sikkerhetstjenester eller andre myndighetsorganer som vitende eller uvitende utfører aktivitet på oppdrag fra, eller til støtte for, myndigheter. Aktiviteten kan være politisk, ideologisk eller økonomisk motivert.

Norges nordligste fylker og Svalbard er utsatt for etterretnings- og påvirkningsaktivitet fra statlige aktører.

Foto
Getty

Russland bruker sivile fartøy til å få oversikt over norsk og alliert militær kapasitet og til å kartlegge infrastruktur langs kysten og på havbunnen. I tillegg kan fartøyene bli brukt til å iscenesette situasjoner til havs som tester hvordan norsk beredskap og krisehåndtering fungerer i praksis. Tilgang til havnene langs norskekysten kan bli utnyttet til å smugle varer som er underlagt sanksjoner eller eksportkontroll, og til å støtte ulovlig etterretningsvirksomhet.

Nordområdene og Arktis er strategisk viktige for Russland

Russiske etterretnings- og sikkerhetstjenester søker kontinuerlig innsikt i norske politiske prosesser og beslutninger som kan påvirke russiske interesser. Særskilt utsatte etterretningsmål er politikere, departementer og andre premissleverandører med kunnskap, evne og mulighet til å påvirke politiske beslutninger. Temaer som forsvars-, utenriks- og sikkerhetspolitikk samt nordområdepolitikk og spørsmål knyttet til Svalbard er av særlig interesse. Næringsliv, sivilsamfunn og akademia innenfor relevante tematiske områder vil også være utsatte mål for etterretnings- og påvirkningsaktivitet.

Russiske etterretnings- og sikkerhetstjenester har aktivitet i hele Norge. De nordligste fylkene og Svalbard er av særlig interesse og derfor spesielt utsatt for etterretnings- og påvirkningsaktivitet. Dette gjelder blant annet grenseområdene i Finnmark og den russiske tilstedeværelsen på Svalbard.

Kina

Kinesisk etterretning har økt kapasitet til å drive operasjoner i Norge

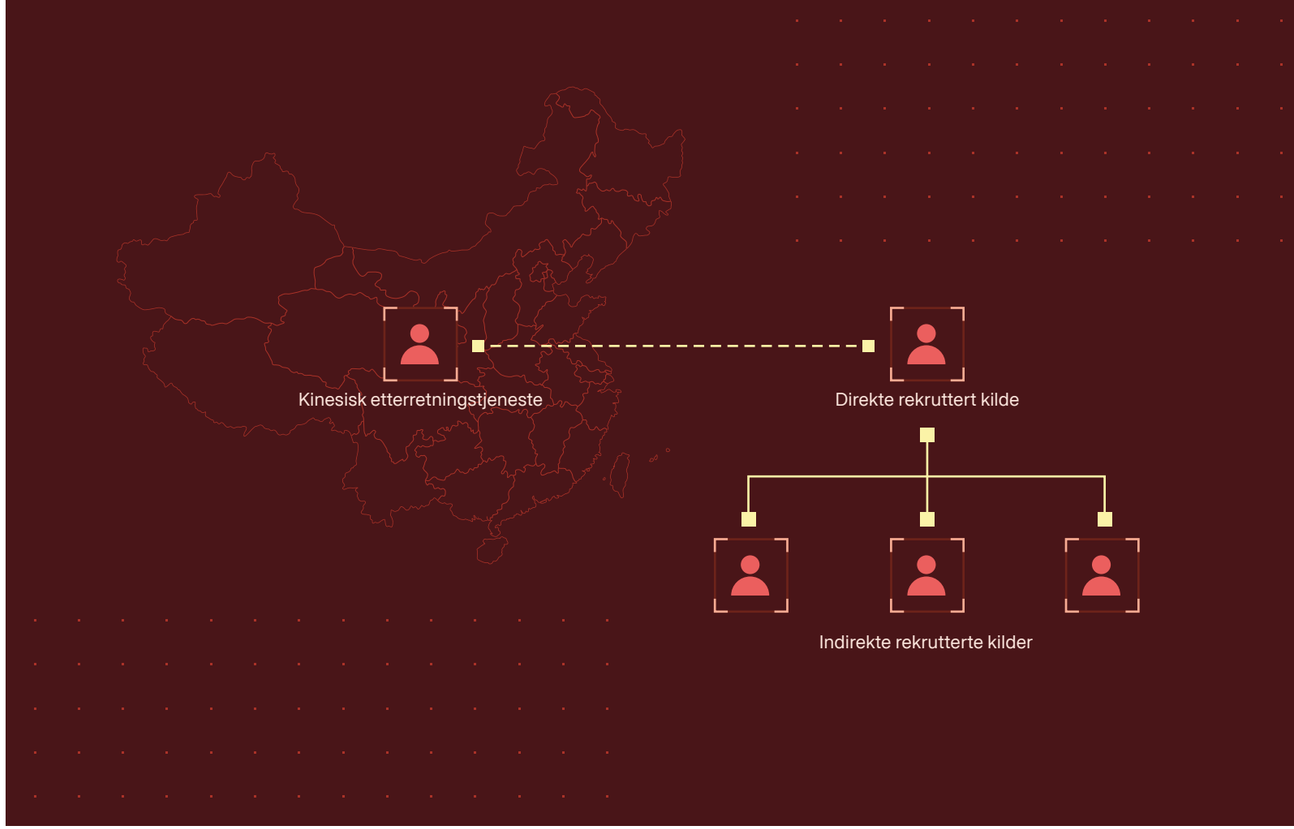
Kinesiske sikkerhets- og etterretningstjenester har økt evne til å drive etterretningsoperasjoner i Norge, både cyberoperasjoner og innhenting via menneskelige kilder. I 2026 vil kinesiske etterretningsaktører innhente informasjon, kartlegge norsk digital infrastruktur og true grupper og enkeltpersoner i befolkningen til å avstå fra kritikk av det kinesiske kommunistpartiet. Vi forventer at flere kinesiske etterretningsoperasjoner i Norge vil bli gjennomført av kommersielle cyberkontraktører og personer som ikke er trent etterretningspersonell, men som opererer på vegne av kinesiske sikkerhets- og etterretningstjenester.

Den største etterretningstrusselen fra Kina er i cyberdomenet

Norske virksomheter som har sensitiv eller skjermingsverdig informasjon, utsettes for kinesiske cyberoperasjoner. Kinesiske cyberaktører utnytter også norske rutere og servere for å utføre operasjoner mot tredjeland. Kinesiske sikkerhets- og etterretningstjenester utfører ikke bare cyberoperasjoner selv, men betaler også kommersielle cyberkontraktører for å utføre oppdrag på deres vegne. Disse kontraktørene har fått en mer sentral rolle og har bidratt til å øke kapasiteten til kinesiske etterretningstjenester i det digitale domenet. Noen av kontraktørene utfører også offensive cyberoperasjoner på eget initiativ og forsøker å selge tilganger de har skaffet seg etter å ha gjennomført kompromitteringer. Dette betyr at ikke alle kinesiske cyberoperasjoner i Norge nødvendigvis gjenspeiler intensjonene til de kinesiske sikkerhets- og etterretningstjenestene. Konsekvensen av denne utviklingen er et mer uforutsigbart og uoversiktlig aktørlandskap og større usikkerhet om hvilke virksomheter som kan bli rammet.

Forskningssamarbeid kan øke handlingsrommet til kinesiske cyberaktører

Kina utnytter forsknings- og utviklingssamarbeid systematisk som et virkemiddel for å bygge militær kapasitet og styrke sikkerhets- og etterretningstjenestene sine. Kinesisk lovgivning krever at alle programvaresårbarheter som avdekkes av kinesiske forskere, skal rapporteres til kinesiske myndigheter senest innen to dager etter at de avdekkes. Slike sårbarheter er et sentralt verktøy i kinesiske cyberoperasjoner, også mot Norge. Norsk-kinesisk forskningssamarbeid som innebærer avdekking av programvaresårbarheter, kan derfor utgjøre en nasjonal sikkerhetstrussel. Vi forventer at sårbarheter som avdekkes gjennom forskningssamarbeid, blir tilgjengeliggjort for kinesisk etterretning og kan utnyttes i fremtidige cyberoperasjoner.



Personer rekruttert av kinesisk etterretning etablerer egne kildenettverk

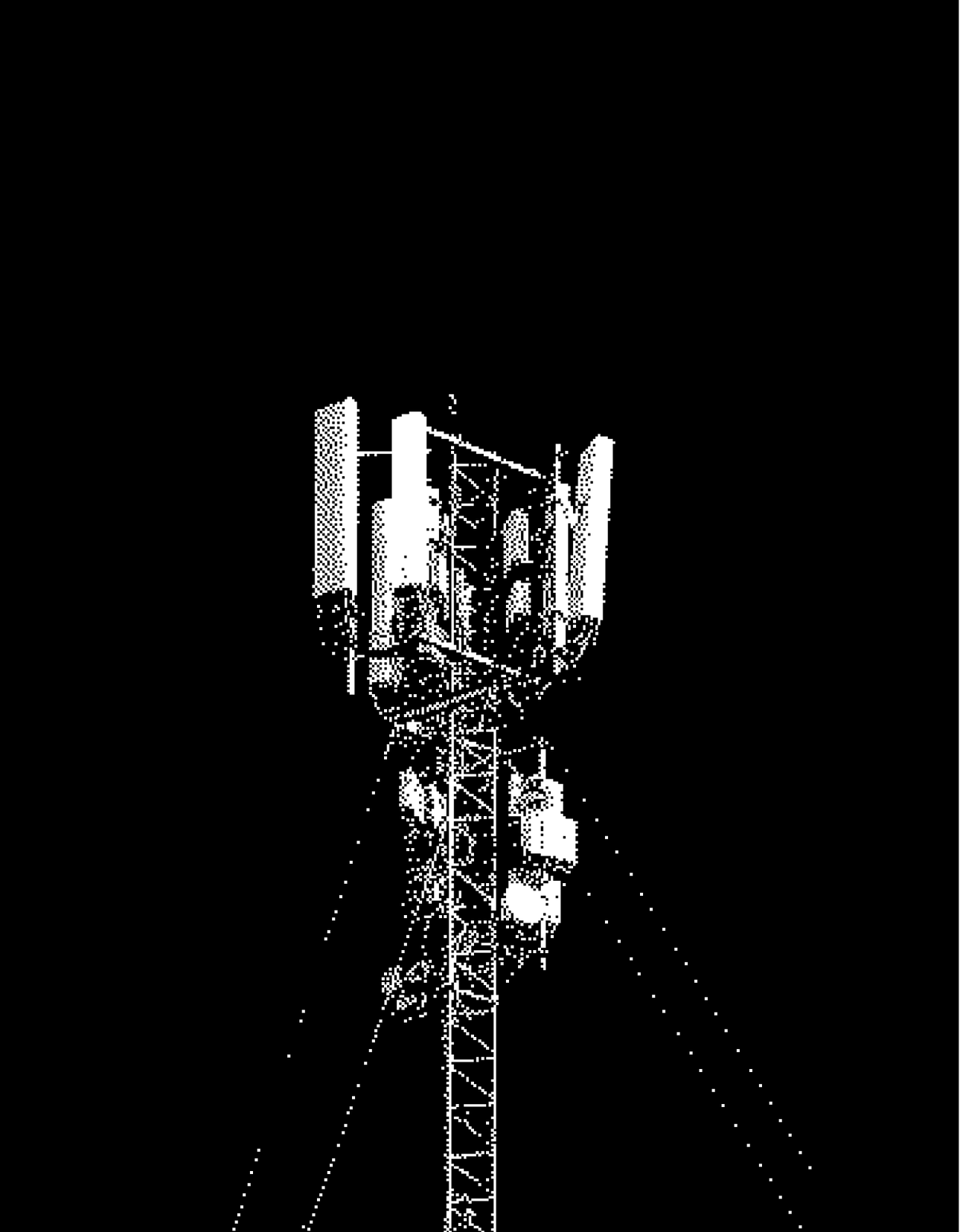
Kinesiske etterretningstjenester forsøker å rekruttere norske borgere for å få tilgang til sensitiv og gradert informasjon. De rekrutterer folk både direkte og indirekte. Personer som har en tilknytning til Kina gjennom studier, arbeid, venner eller familie, er mer utsatt, ettersom tilknytningen gir etterretningstjenestene et større handlingsrom for belønning eller press.

I tillegg er det en økende trend at kinesiske etterretningstjenester oppfordrer kildene sine til å rekruttere egne kildenettverk, for eksempel gjennom å lyse ut deltidsstillinger på jobbrekrutteringssider eller ved å tilnærme seg personer via LinkedIn. Et fellestrekk er at personer som rekrutteres indirekte, ikke nødvendigvis er klar over at de rapporterer til kinesisk etterretning. Hvem som er oppdragsgiveren, er ofte skjult; kildene blir gjerne fortalt at klienten er en tenketank, et internasjonalt selskap, et konsulentfirma eller lignende. I starten blir kildene bedt om å levere ikke-offentlig informasjon mot betaling, for eksempel om hva bedrifter, offentlige virksomheter eller politiske institusjoner gjør eller planlegger å gjøre. Etter hvert kan de få mer konkrete oppdrag. Denne trenden bidrar til å øke kinesiske etterretningstjenesters kapasitet til å innhente informasjon gjennom menneskelige kilder. Vi forventer at kinesisk etterretning vil forsøke å rekruttere norske borgere gjennom kilder i andre vestlige land.

↑

Personer rekruttert av kinesisk etterretning oppfordres i økende grad til å rekruttere egne kildenettverk. Dette skjer for eksempel gjennom å lyse ut deltidsstillinger på rekrutteringssider eller ved å tilnærme seg personer via LinkedIn. Et fellestrekk er at personer som rekrutteres indirekte, ikke nødvendigvis er klar over at de rapporterer til kinesisk etterretning. Hvem som er oppdragsgiver, er ofte skjult.

Figur
Getty / Dinamo Design



Kinesiske trusselaktører vil forsøke å true personer i Norge til taushet

Kinesiske trusselaktører bedriver vedvarende overvåkning og undertrykkelse av personer og miljøer i Norge som i offentligheten retter kritikk mot Kinas styresett og menneskerettighetssituasjon. Gjennom bruk av tvang, trusler og press rettet mot enkeltindivider forsøker de å skape en situasjon der de utsatte ikke ser noen annen løsning enn å avstå fra å kritisere regimet eller ufrivillig returnere til Kina. Skremselstaktikkene spenner bredt, fra hyppige oppringninger fra skjult nummer til direkte drapstrusler.

Trusselaktørene forsøker også å rekruttere personer i Norge for at de skal rapportere om personer i diasporamiljøer. Når den kinesiske partistaten ikke har direkte innflytelse over kritikerne eller deres familie, blir internett den foretrukne plattformen for å undertrykke motstandere. Eksempelvis sprer kinesiske cyberaktører skadevare gjennom tilsynelatende legitime mobilapplikasjoner som er utviklet for å appellere til tibetanske og uiguriske miljøer. Vi forventer at personer bosatt i Norge vil bli utsatt for slik digital overvåkning.

Kina vil forsøke å bruke forskning som en inngang til nordområdene våre

Flere mediesaker som problematiserer kinesisk aktivitet i nordområdene, og regjeringens nasjonale sikkerhetsstrategi bidrar til å innskrenke kinesiske aktørers handlingsrom i norske nordområder. Likevel forsøker kinesiske aktører fortsatt å posisjonere seg i nordområdene våre. Slik vi vurderer det, anser kinesiske aktører forsknings- og utdannelsessektoren i nord-områdene som en av få arenaer som fremdeles er åpne for kultivering og samarbeid. Kinesiske fremstøt i nordområdene våre vil vedvare, og vi forventer at de i stor grad vil bli utført på en fordekt måte av kinesiske forsknings-institusjoner og personer som opptrer på vegne av kinesiske sikkerhets- og etterretningstjenester.

Bildetekst
Kinesiske sikkerhets- og etterretningstjenester har økt evne til å drive etterretningsoperasjoner i Norge. I 2026 vil de blant annet kartlegge norsk digital infrastruktur.

Illustrasjon
Getty / Dinamo Design

Iran

Vi forventer at iranske etterretnings- og sikkerhetstjenester vil gjennomføre etterretnings- og påvirkningsoperasjoner i Norge i 2026. Det iranske regimet kan også forsøke å angripe vestlige mål gjennom hærverk, målrettede attentater, terrorhandlinger eller destruktive cyberoperasjoner. Det iranske regimet bruker slike angrep som et politisk verktøy for å utrykke misnøye, ta hevn eller stilne kritiske stemmer.

Iran ønsker å ramme dissidenter, kritikere og israelske mål i Norge

Målbildet til iranske etterretning- og sikkerhetstjenester i Norge og Vesten er relativt stabilt. Det omfatter flere grupper, som dissidenter, menneskerettighetsorganisasjoner, akademikere og journalister som kritiserer iranske styresmakter. Amerikanske, israelske og jødiske interesser, og ikke-iranske vestlige politikere som støtter én eller flere av disse gruppene, er også utsatte mål.

> *Bruken av kriminelle nettverk og andre proxyaktører gjør det vanskeligere å spore aktivitet tilbake til Iran.*

Felles for disse målgruppene er at de vurderes som potensielle trusler mot iranske styresmakters legitimitet og overlevelse. Hvordan Iran prioriterer mellom målgruppene, varierer, blant annet avhengig av geopolitiske hendelser i Midtøsten, som konflikten mellom Israel, Iran og USA, eller interne hendelser, som sosial uro i Iran.

Iran utnytter kriminelle nettverk i Norge

Iran benytter seg av proxyaktører for å gjennomføre operasjoner i Vesten. Det vil si aktører uten formell tilknytning til iranske myndighetsorganer, som vitende eller uvitende utfører aktivitet på oppdrag fra eller til støtte for iranske myndigheter. Proxyaktørene kan for eksempel være svenske kriminelle nettverk med tilstedeværelse i Norge.

Bruken av kriminelle nettverk og andre proxyaktører gjør det vanskeligere å spore aktivitet tilbake til Iran. Disse aktørene har også stor bevegelsesfrihet i Europa, god lokalkunnskap og tilgang til våpen. Samtidig kan dette redusere kontrollen Iran har over aktiviteten deres, og fordi aktørene gjerne er uerfarne, kan skadeomfanget bli både større og mindre enn planlagt.

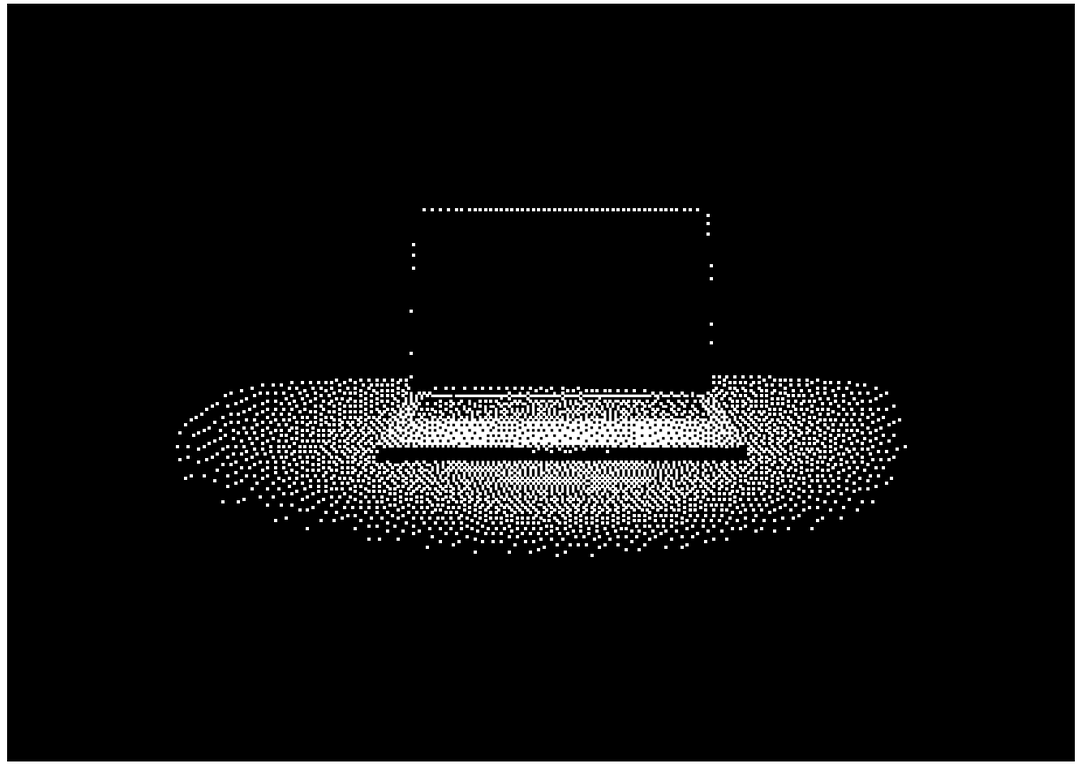
Iran kartlegger dissidenter i Norge

Iranske etterretnings- og sikkerhetstjenester kartlegger og presser iranske dissident- og separatistmiljøer i Norge på ulike måter. De bruker både fysiske og digitale virkemidler. Eksempelvis kompromitterer iranske cyberaktører blant annet e-postkontoer, kontoer på sosiale medier og private datamaskiner som tilhører dissidenter i Norge. Dette gjør de for å samle inn informasjon om dissidentene og deres nettverk. Iranske cyberaktører har høy kapasitet og vil fortsette å utvikle metodene sine for å gjennomføre mer målrettede og inntrengende operasjoner mot personer i Norge.

Kartlegging skjer også gjennom innhenting av informasjon via menneskelige kilder, for eksempel under demonstrasjoner eller markeringer. Dersom endringer i interne eller eksterne iranske forhold fører til at Iran vurderer utsatte grupper som betydelige trusler mot iranske myndigheter, kan de bruke slik informasjon som grunnlag for å utføre angrep mot personer i Norge.

Iran ønsker tilgang til flerbruksteknologi

Iran er underlagt et svært strengt internasjonalt sanksjonsregime. Som i tidligere år vil det også i 2026 motivere Iran til å fordekt forsøke å anskaffe varer og tilegne seg teknologi fra Norge som kan støtte deres militære kapasitetsutvikling.



Iran kartlegger dissidenter i Norge. De kompromitterer eksempelvis e-postkontoer, kontoer på sosiale medier og datamaskiner tilhørende dissidenter i Norge.

Illustrasjon
Dinamo Design

Fremhevede metoder

Cyberoperasjoner

Cyberoperasjoner er en viktig metode for fremmede staters etterretningsvirksomhet i Norge. Russland, Kina, Iran og Nord-Korea er eksempler på land som gjennomfører cyberoperasjoner i Norge, enten direkte eller ved hjelp av proxyaktører. Vi forventer at de vil gjøre det også i 2026, og flere av operasjonene vil lykkes. Formålet kan variere mellom informasjonsinnhenting, kartlegging, påvirkning, sabotasje og forstyrrende aktivitet. Formålet kan også være økonomisk vinning. Disse variasjonene gjør at cyberoperasjoner rammer mange ulike mål.

Trusselaktørene utnytter både tekniske og menneskelige sårbarheter

For å gjennomføre operasjoner i Norge bruker cyberaktører metoder som utnytter både tekniske og menneskelige sårbarheter. Dette gjelder særlig Russland og Kina, som i 2025 har benyttet sårbarheter i nettverksenheter, som rutere, for å etablere tilganger til norsk digital infrastruktur. Slike metoder benyttes også for informasjonsinnhenting. Trusselaktører har for eksempel fått tilgang til sensitiv informasjon gjennom å utnytte **nulldagssårbarheter** i e-posttjenester det siste året.

Også effektiv sosial manipulering var et sentralt element i vellykkede cyberoperasjoner i 2025. Sosial manipulering er ikke bare noe statlige cyberaktører benytter seg av, men er også utbredt i cyberkriminelle miljøer. Statlige trusselaktører er imidlertid ofte særlig effektive i bruken av sosial manipulering, ettersom de gjerne planlegger målrettede operasjoner tilpasset offeret og bruker tid på å bygge tillit.

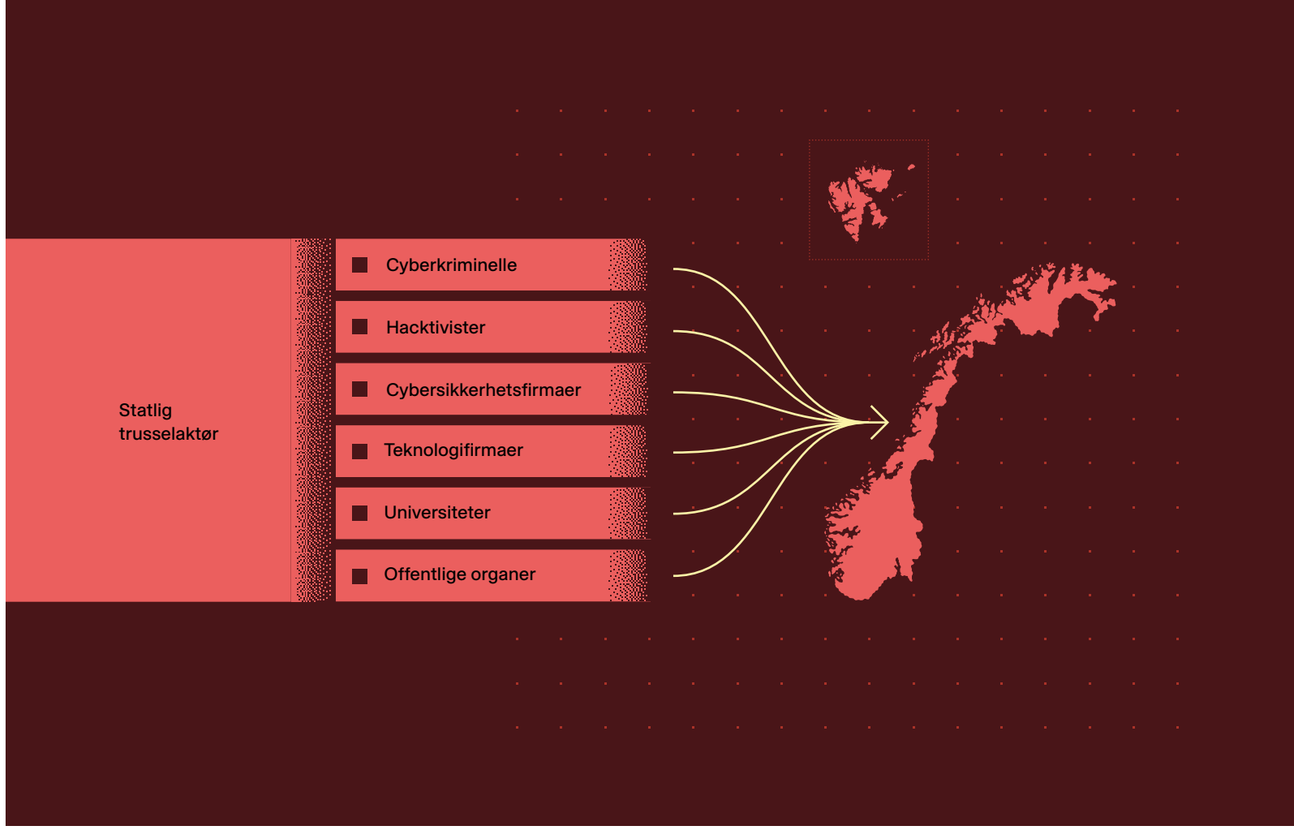
Dette ser vi eksempelvis i cyberoperasjoner hvor formålet er transnasjonal undertrykkelse rettet mot iranske dissidenter eller menneskerettighetsaktivister i Norge. Iranske cyberaktører tar gjerne kontakt med en aktivist og utgir seg for å være en journalist med interesse for aktivistens arbeid. Ofte sier de at de ønsker et digitalt møte med personen. Gjennom en lengre dialog lurer de så personen til å laste ned skadevare på datamaskinen sin eller til å oppgi påloggingsdetaljer. Iran benytter tilgangen de får, til å samle inn informasjon om offeret og hens nettverk.

Den kinesiske cyberaktøren kjent som Salt Typhoon er et eksempel på en trusselaktør som har kompromittert sårbare nettverksenheter hos norske virksomheter. Salt Typhoon blir av amerikanske myndigheter beskrevet som en aktør som har spesialisert seg på cyberoperasjoner mot telekominfrastruktur. Aktøren knyttes til private kinesiske cybersikkerhetsfirmaer. Dette illustrerer den mer sentrale rollen private kontraktører har i kinesiske cyberoperasjoner, og hvordan de bidrar til å øke kapasiteten til kinesiske sikkerhets- og etterretningstjenester.

Cyberaktører fra Nord-Korea er kjente for kreativ sosial manipulering. I en pågående kampanje mot norske og andre vestlige mål blir bedrifter manipulert til å ansette nordkoreanske IT-utviklere. Både rekrutteringen og selve arbeidet skjer fra hjemmekontor, og trusselaktørene bruker en rekke metoder, som falske identitetspapirer, for å skjule hvor de kommer fra. Bedriftene er derfor uvitende om opprinnelseslandet til personene de ansetter. Vi forventer at lønnsinntektene nordkoreanske ansatte mottar gjennom slike stillinger, går til å finansiere landets våpen- og atomvåpenprogram.

Kunstig intelligens gir nye muligheter for cyberaktører

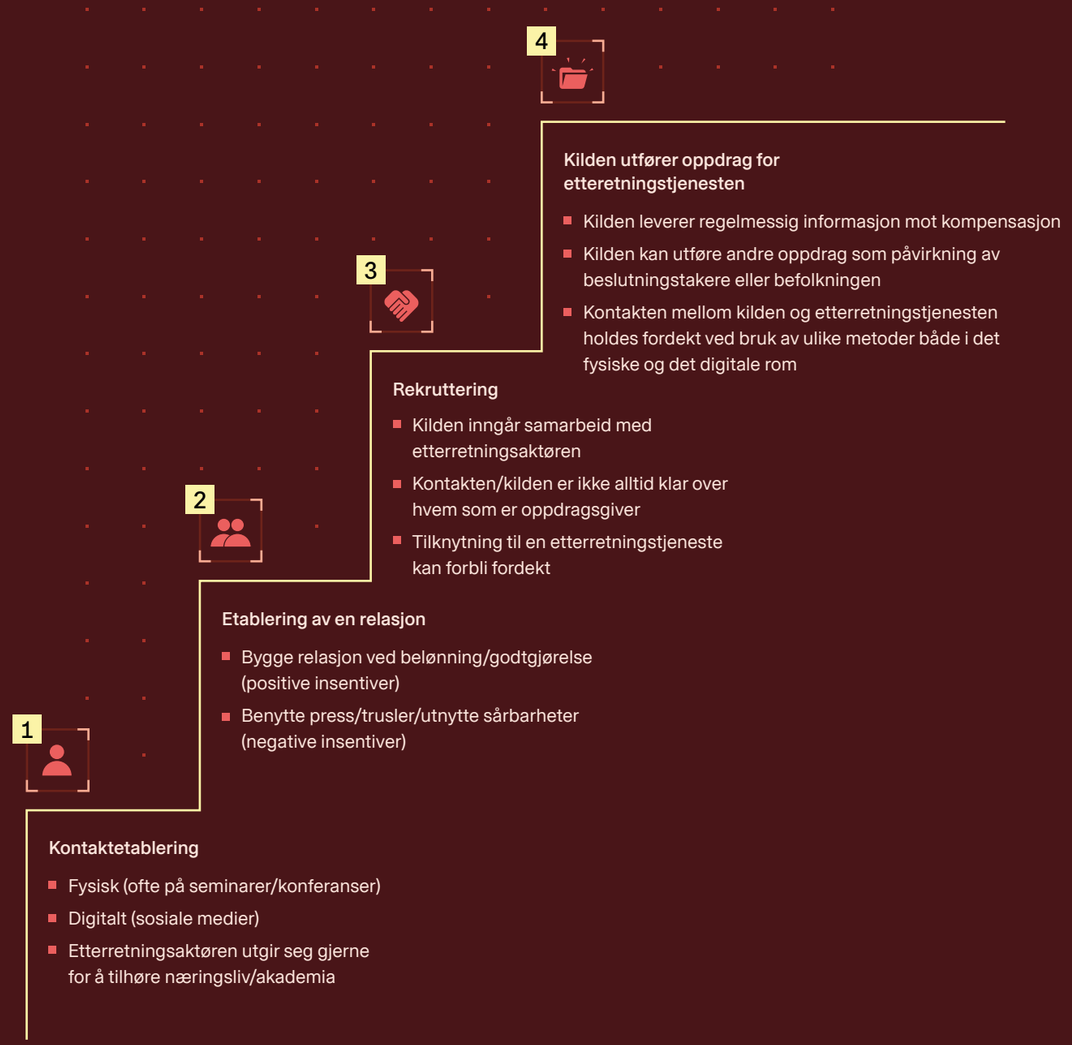
Kunstig intelligens (KI) øker statlige cyberaktørers evne til å gjennomføre cyberoperasjoner i Norge. KI kan benyttes i alle fasene av et datainnbrudd og begrense behovet for menneskelige operatører. Bruk av KI har også et stort potensial innenfor sosial manipulering. Med KI-verktøy kan cyberaktører for eksempel lage falske bilder, videoer, tekst eller lyd de kan bruke til å underbygge falske identiteter. Vi forventer at norske virksomheter i 2026 vil bli utsatt for cyberoperasjoner fra statlige cyberaktører hvor KI-verktøy er sentrale i gjennomføringen.



Proxyaktører bidrar til gjennomføring av cyberoperasjoner i Norge. Slike bidrag kan variere, fra faktisk gjennomføring av operasjoner på vegne av en etterretningstjeneste, til utvikling av verktøy som benyttes i cyberoperasjoner.

Figur
Getty / Dinamo Design

En **nulldagssårbarhet** er en sårbarhet i et produkt som noen kjenner til, men som ikke er kjent for offentligheten, leverandøren eller produsenten av produktet. Dermed har verken leverandøren eller produsenten hatt mulighet til å utbedre sårbarheten før en trusselaktør utnytter den.



Rekruttering av menneskelige kilder

Fremmede staters etterretningstjenester vil også i 2026 forsøke å rekruttere kilder og medhjelpere i Norge. Denne trusselen er størst fra russiske og kinesiske etterretningstjenester. Personer med tilgang til sensitiv eller gradert informasjon og personer som har viktige roller og verv, er spesielt utsatt for rekrutteringsforsøk. Personer med familiær eller annen tilknytning til autoritære stater er også utsatt, ettersom tilknytningen åpner for et bredere spekter av både press og belønning.

Rekruttering og kontaktetablering foregår både i det fysiske og i det digitale rom. Etterretningsoffiserer under dekke, noen under dekke av å være diplomat, vil forsøke å rekruttere personer i Norge i 2026. Forsøkene kan skje på seminarer, konferanser og andre møteplasser for relevante fagmiljøer. Bruk av sosiale medier er også en etablert metode for utenlandske etterretningstjenester og gjør at de kan nå ut til en større andel av befolkningen. Digital rekruttering er kostnadseffektivt og enkelt å utføre, uavhengig av om etterretningsoffiseren befinner seg i Norge. Kontakt kan innledes ved bruk av falske kontoer på LinkedIn, gjennom tilsynelatende legitime henvendelser. Norske personer kan også bli utsatt for rekrutteringsforsøk når de oppholder seg i tredjeland. I dagens sikkerhetspolitiske situasjon må norske borgere som oppholder seg i Russland, forvente å bli utsatt for rekrutteringsforsøk. Det gjelder særlig personer med påvirkningsmuligheter eller tilgang til informasjon av interesse.

Høsten 2024 pågrep PST en norsk statsborger som selv hadde tatt kontakt med russiske og iranske myndigheter for å gi dem informasjon. Mannen ble i 2025 dømt for grov etterretningsvirksomhet mot statshemmeligheter, men dommen er anket og dermed ikke rettskraftig. Saken er et eksempel på at kontakten noen ganger blir initiert av den som lar seg rekruttere.

Rekrutterte personer kan bli bedt om å utføre en rekke ulike oppgaver, og over tid blir oppgavene ofte mer omfattende. I tillegg til gradert informasjon er utenlandske etterretningstjenester interessert i ugradert sensitiv informasjon. Rekrutterte personer kan også bli bedt om å rekruttere egne kilder, og de kan få praktiske oppgaver som å kjøpe sanksjonsbelagte varer og installere teknisk overvåkningsutstyr. Videre kan de få i oppdrag å utføre sabotasje, forstyrrende aktiviteter, voldshandlinger eller terror.

Rekrutterte innsidere i norske virksomheter kan bli bedt om å fremskaffe informasjon om uenigheter, interne konflikter, misnøye og andre sårbarheter, for eksempel i rutiner, sikkerhetstiltak og IKT-infrastruktur. Slike sårbarheter kan bli utnyttet i fremtidige etterretnings-, påvirknings- og sabotasjeoperasjoner.

Rekruttering av menneskelige kilder steg for steg.

Figur
Dinamo Design

Transnasjonal undertrykkelse

Autoritære staters transnasjonale undertrykkelsesaktivitet drives av en frykt for at opposisjon på sikt kan utfordre regimets maktposisjon. Særlig Kina og Iran, men også Russland, søker å forhindre ytringer som er kritiske til politikken deres, eller som kan skade omdømmet deres. Dissidenter og regimekritikere er mest utsatt, men andre offentlige meningsbærere kan også rammes.

Enkelte stater er villige til å ta stor risiko for å stilne politiske motstandere. De utøver transnasjonal undertrykkelse i form av press, trusler og i ytterste konsekvens dødelig vold. Dissidenter kan bli presset til å returnere til hjemlandet, for eksempel ved at familiemedlemmer som er igjen i hjemlandet, blir truet eller fengslet. Fremmede stater kan benytte sine diplomatiske representasjoner, tilreisende etterretningsoffiserer, organiserte kriminelle eller infiltratører i diasporagrupper til å stilne sine kritikere i Norge.

Trusselaktørene oppsøker og filmer eller fotograferer deltakere på demonstrasjoner og menneskerettighetsarrangementer for å kartlegge kritikere. De benytter også cyberoperasjoner for å innhente data om miljøer av interesse. Dette gjør de blant annet ved å spre skadevare via linker til nyhetsartikler, kulturelle videoer og annet innhold som kan vekke interesse hos spesifikke målgrupper.

Omfanget av transnasjonal undertrykkelse i Norge påvirkes av hvor synlige kritiske grupper og individer er i offentligheten, og tilstedeværelsen av prominente lederskikkelser. Når trusselaktørene ikke har direkte innflytelse over dem de vil ramme, eller deres familie, bruker de internett som en plattform for å undertrykke motstandere. I dagens sikkerhetspolitiske situasjon, med tiltakende konflikt mellom liberale demokratier og autoritære stater, kan de sistnevnte øke sin innsats for å stilne kritikere i andre land, særlig ved bruk av internett.

Påvirkning

Vi forventer at autoritære stater vil gjennomføre påvirkningsoperasjoner i Norge i 2026. Formålet vil være å sikre eget lands interesser, ofte på bekostning av norske interesser og det vestlige sikkerhetsfellesskapet. Påvirkningsoperasjoner gjennomføres både i det fysiske og i det digitale rom. De kan rette seg mot ulike målgrupper – fra diasporamiljøer til personer involvert i norsk politikk. Fremmede stater har en vedvarende interesse av å rekruttere og påvirke personer som har politisk innflytelse, formell eller uformell makt. Dette kan gjøres både gjennom personbasert relasjonsbygging, ved bruk av trusler og i ytterste konsekvens gjennom målrettede svertekampanjer. Personer rekruttert av fremmede etterretningstjenester kan bli instruert til å påvirke beslutninger i det skjulte.

Både Russland og Kina har et omfattende påvirkningsapparat bestående av blant annet sikkerhets- og etterretningstjenester, ulike myndighetsorganer og proxyaktører. De utvikler stadig nye teknikker for å produsere og spre påvirkningsmateriale. Dette inkluderer salg av falske brukerkontoer, produksjon av videomateriale og ansettelse av influensere som skal spre propaganda og desinformasjon.

En operasjon fra en fremmed stats etterretningsaktør kan ha flere formål. Å påvirke den allmenne meningsdannelsen ved å skape uro og oppmerksomhet kan være ett av flere mål. Dette opplevde vi i 2025, da en prorussisk hacktivistgruppe gjennomførte en cyberoperasjon mot en norsk demning. Operasjonen var lite sofistikert og hadde begrenset skadepotensial, men fikk likevel mye oppmerksomhet da aktøren omtalte hendelsen på sosiale medier.

Ulovlige anskaffelser av sanksjonert og eksportkontrollert teknologi

Norske virksomheter som utvikler, selger og forsker på teknologi med både sivile og militære bruksområder, vil fortsatt være utsatt for ulovlige anskaffelsesforsøk i 2026. Statlige trusselaktører benytter ulovlige, fordekte metoder i forsøk på å anskaffe norsk teknologi som er underlagt eksportkontroll og sanksjonsregelverk.

Slike omgåelsesforsøk er kreative. For å skjule den reelle sluttbrukeren benytter trusselaktørene ofte mellomledd i tredjeland som mottakere av eksporterte varer. Mellomleddene videresender så varene ulovlig til eksempelvis Russland. Omgåelsesforsøkene kan involvere flere mellomledd, og aktører fra ulike land samarbeider. Et eksempel er at russiske aktører, som er strengt sanksjonerte, forsøker å anskaffe sanksjonerte varer fra Norge via kinesiske mellomledd. Mellomleddene kan være vitende eller uvitende og fra en rekke land, også i Europa.

Henvendelser fra aktører i alle land kan derfor medføre en risiko. Norske virksomheter må dermed fokusere på indikatorer som kan avdekke henvendelser med særlig risiko for avledning til ulovlig aktivitet.

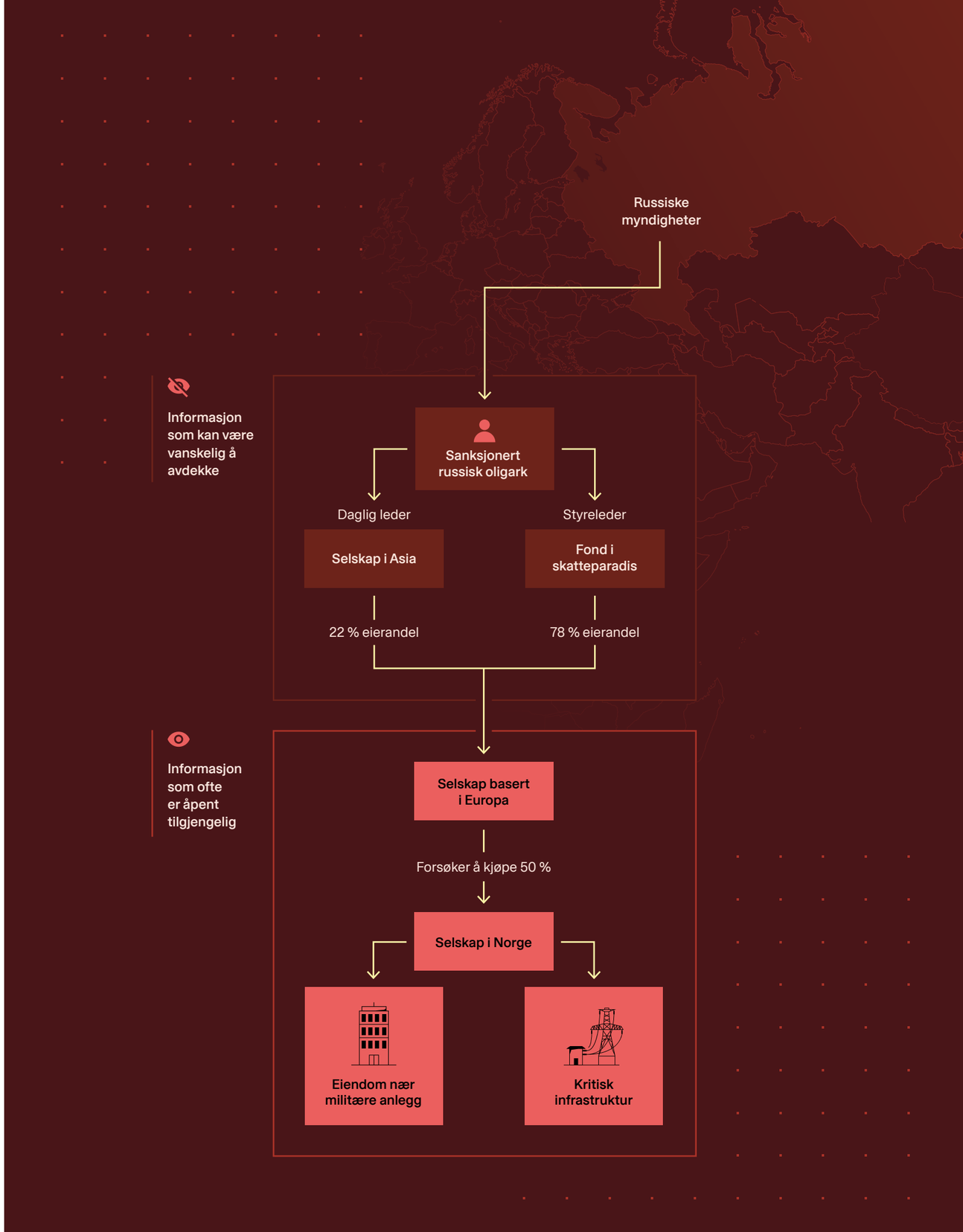
■

Eksempler på indikatorer på fordekte anskaffelsesforsøk kan være:

- Det mangler informasjon om sluttbrukeren i bestillingen (nettside, adresse og telefonnummer er ikke oppgitt).
- Kunden har ingen nettside, eller nettsiden virker uprofesjonell. Det finnes ikke noe telefonnummer til kunden.
- Spesifikasjoner på emballasje, fraktruter, deklarasjoner eller betalingsmetoder er uvanlige.
- Et spedisjonsfirma, et lager eller en havn er oppgitt som sluttbruker.
- Det bestilles uvanlig små eller store kvantum, eller kvantumet samsvarer ikke med formålet som er oppgitt.

«Kjenn din kunde og teknologi» er et viktig prinsipp for å avdekke ulovlig anskaffelsesaktivitet.

Trusselaktørers teknologibehov er varierte og utvikler seg stadig. Et bredt spekter av norsk teknologi og norske virksomheter er således utsatt for ulovlige anskaffelsesforsøk. Flere anskaffelsesforsøk er profesjonelt utført og vanskelige å avdekke. Likevel blir mange anskaffelsesforsøk forhindret takket være årvåkne norske virksomheter.



Sikkerhetstruende økonomisk aktivitet

Illustrasjonen viser et fiktivt eksempel på hvordan statlige aktører benytter komplekse eierstrukturer for å fordekke sin involvering i sikkerhetstruende økonomisk aktivitet. Eksempelet baserer seg på en sammensetning av ulike modus observert i Norge.

Figur
Getty / Dinamo Design

Forskningsmiljøer vil fortsatt være utsatt

Fremmede stater prøver ikke bare å få tak i fysiske varer, men også teknologien og kunnskapen bak produkter med militær anvendelse. Målet er å styrke egen evne til å utvikle og produsere slike produkter. For eksempel kan land som Kina eller Iran forsøke å tilegne seg teknologi fra norske forsknings- og utviklingsmiljøer ved å skaffe seg tilgang til forskningsfasiliteter og fagmiljøer i Norge.

Vi forventer at trusselaktører vil forsøke å utnytte mulighetsrom tilknyttet blant annet gjesteforelesningsordninger og tilganger til spesialisert forskningsinfrastruktur til å utføre aktivitet utover det som er avtalt. Trusselaktører misbruker også data og informasjon delt i internasjonale forskningssamarbeid. At informasjonen skal utnyttes militært, er ikke nødvendigvis kjent for forskerne som deltar. Forskere ved norske institusjoner kan dermed være utsatt uten å vite det.

Sikkerhetstruende økonomiske virkemidler

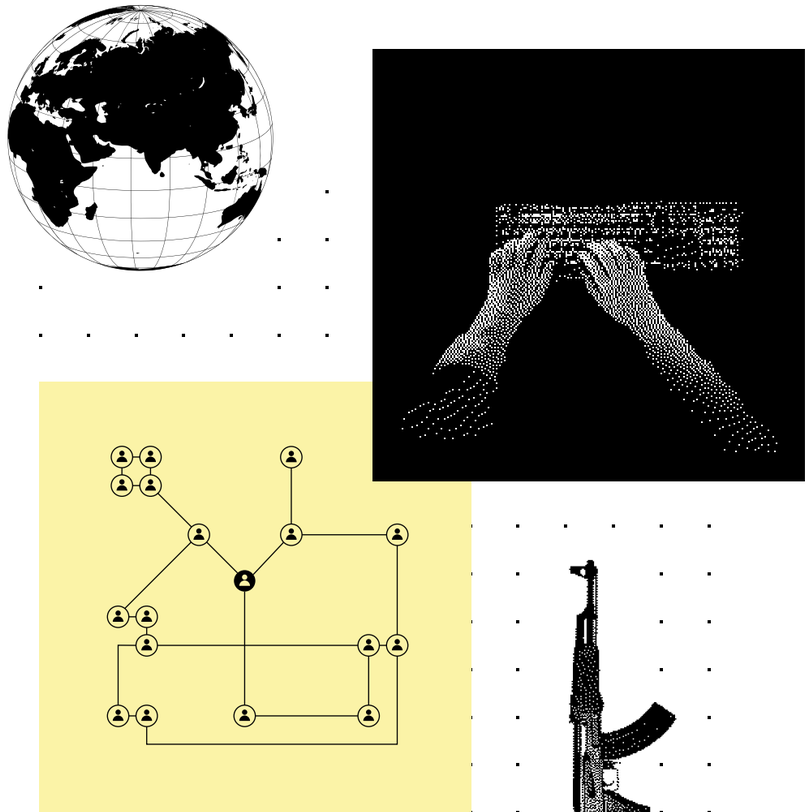
Statlige trusselaktører vil i 2026 fortsette med fordekte pengestrømmer, investeringer og andre økonomiske virkemidler som kan true nasjonal sikkerhet. De bruker slike virkemidler for å få tilgang til teknologi, påvirke beslutninger og innhente sensitiv informasjon.

Ved å kjøpe strategisk plassert eiendom kan statlige trusselaktører få tilgang til informasjon om norsk og alliert militær aktivitet, kritisk infrastruktur og andre forhold av sikkerhetsmessig betydning. Vi har sett tilfeller der personer knyttet til det russiske myndighetsapparatet har forsøkt å kjøpe eiendom i nærheten av norske militærbaser. Gjennom slike eiendommer kan russiske aktører skaffe seg verdifull informasjon om militære forhold.

Statlige aktører benytter seg av tilsynelatende normal forretningsaktivitet som oppkjøp og investeringer i norske virksomheter for å få kontroll over kritisk infrastruktur og innsikt i virksomhetenes beslutningsprosesser. Gjennom eierskap i sentrale virksomheter oppnår stater kontroll over verdikjeder og skaper ensidige avhengighetsforhold de kan bruke som pressmiddel mot norske beslutningstakere.

Gjennom anbudsprosesser og leverandøravtaler kan trusselaktører skaffe seg informasjon om og tilgang til fysisk og digital infrastruktur. Når kinesisk teknologi blir brukt i kritisk infrastruktur, oppstår et mulighetsrom for informasjonsinnhenting, siden kinesiske selskaper plikter å samarbeide med kinesiske myndigheter og deres etterretningstjenester.

Sikkerhetstruende økonomisk virkemiddelbruk kan være utfordrende å avdekke, ettersom statlige trusselaktører på ulikt vis prøver å skjule at de er involvert i slik aktivitet. Samtidig utnytter de det at aktiviteten beveger seg i en gråsone mellom det lovlige og ulovlige. Vi har sett flere eksempler på at russisk eierskap i norske virksomheter tilsløres gjennom komplekse eierstrukturer med investeringsfond og selskaper i flere land. De komplekse strukturene gjør det utfordrende å avdekke de reelle eierinteressene og hvem som har kontroll i norske selskaper.



Illustrasjon
Getty / Dinamo Design

Kapittel 02

Politisk motivert vold

Terrortrusselnivået i Norge er MODERAT, det vil si nivå 3 på terrortrusselskalaen (se side 7).

Selv om vi er på MODERAT terrortrusselnivå, er terrortrusselbildet mer komplekst og uforutsigbart enn tidligere. Det er også preget av flere aktører med ulike motivasjoner. For eksempel ser vi at statlige aktører, terror og organisert kriminalitet flyter sammen. Det gjør at det kan være utfordrende å skille mellom terror og annen kriminalitet i det tidlige forløpet av en hendelse.

Radikalisering av mindreårige og unge voksne forblir en utfordring. Mange er sårbare på grunn av psykisk uhelse og utenforskap. Trusselbildet kompliseres ytterligere av at ideologi og voldsfascinasjon blandes sammen på en måte som gjør det vanskeligere å avdekke potensielle terrorhandlinger.

Terroraktiviteten i Vesten har de siste par årene vært høyere enn på mange år. Selv om sikkerhets- og etterretningstjenestene avverger en stor del av angrepsplanene, er det utfordrende å avdekke planene til enkeltpersoner.

I dette kapittelet tar vi for oss de mest alvorlige truslene innenfor politisk motivert vold i Norge: **ekstrem islamisme** og **høyreekstremisme**. I tillegg omtaler vi **antistatlig ekstremisme**, ettersom det utviklet seg til å bli mer aktuelt gjennom 2025.

Med **radikalisering** mener vi en prosess der en person utvikler aksept for eller vilje til aktivt å støtte eller delta i voldshandlinger for å nå politiske, religiøse eller ideologiske mål.

Med **ekstremisme** mener vi aksept for eller støtte til bruk av vold for å nå politiske, religiøse eller ideologiske mål.

Trusselen fra ekstrem islamisme

Hva er **ekstrem islamisme**?
Ekstreme islamister aksepterer eller støtter bruk av vold for å oppnå politiske, religiøse og ideologiske mål.

Ekstreme islamister har andre oppfatninger av hva islam er, og hvordan islam skal praktiseres, enn det som er vanlig blant muslimer flest i Norge.

PST vurderer det som ***mulig*** at ekstreme islamister vil forsøke å gjennomføre terrorangrep i Norge i 2026.

Vi forventer fortsatt høy angrepsaktivitet i Europa, særlig på grunn av situasjonen i Gaza og Midtøsten. Israels krigshandlinger i Gaza kan inspirere nye aktører til å angripe israelske og jødiske mål i Europa. En endring i aktørbildet kan innebære større usikkerhet om hvordan angrep planlegges og gjennomføres.

Radikalisering på internett, og særlig unge som konsumerer, produserer og deler ekstremistisk materiale, fortsetter å være en reell bekymring.

Den høye angrepsaktiviteten i Europa forventes å fortsette

Terrortrusselen fra ekstrem islamisme kommer fra personer som sympatiserer med ideologien til de internasjonale terrororganisasjonene Den islamske stat (IS) og al-Qaida, eller fra personer som er mobilisert av forhold de opplever som provokasjoner, krenkelser eller undertrykkelse av religionen islam og muslimer. Disse personene har Vesten sentralt i sitt fiendebilde, blant annet fordi de mener Vesten er i krig med islam og muslimer. Norge har bare sporadisk blitt nevnt spesifikt i internasjonale ekstremisters propaganda og retorikk, men inngår i fiendebildet som en del av Vesten. Norge har derimot en sentral plass i fiendebildet til norske ekstreme islamister.

Ekstreme islamisters angrepsaktivitet i Vesten, og særlig i Europa, har økt markant etter Hamas' terrorangrep 7. oktober 2023 og Israels påfølgende militæroperasjon i Gaza. Den høye angrepsaktiviteten fortsatte i 2025. De fleste angrepsplanene blir imidlertid avverget av sikkerhets- og etterretningstjenester.

Vi forventer at den høye angrepsaktiviteten i Europa vil fortsette i 2026. Det skyldes særlig den radikaliserende effekten av Israels krigføring i Gaza og påfølgende oppfordringer fra både IS og al-Qaida om å angripe blant annet israelske og jødiske mål i Vesten. Slik vi vurderer det, vil den negative påvirkningen på trusselbildet fortsette selv om våpenhvileavtalen overholdes eller krigen avsluttes.

Vi ser også indikasjoner på at krigshandlinger i Gaza inspirerer nye aktører til å angripe israelske og jødiske mål i Europa. Det er en ny utvikling at personer som sympatiserer med eller har tilknytning til Hamas, inngår i mulig angrepsaktivitet i Europa. Siden dette er nytt, kan det bli vanskeligere å vite hvordan eventuelle angrep planlegges og gjennomføres. I tillegg kan Iran forsøke å benytte seg av proxyaktører til dette.

Vi forventer at IS og al-Qaida i 2026 primært vil forsøke å inspirere sympatisører i Europa til å utføre terror. Årsaken er at særlig IS på ny er svekket i flere områder som følge av antiterroroperasjoner. IS-filialene som de siste årene har forsøkt å gjennomføre angrep i Europa, IS i Khorasan-provinsen (ISKP) og IS i Somalia, har midlertidig fått svekket angrepsevne. Al-Qaida fortsetter på sin side å prioritere lokal vekst. Filialen deres på den arabiske halvøy (AQAP) har samtidig en vedvarende intensjon om å inspirere til eller legge til rette for angrep i Europa, hvis muligheten byr seg.

I 2025 har både offisiell og sympatisørprodusert propaganda fortsatt å oppfordre sympatisørene til angrep og gitt operativ veiledning.

Samtidig som terrororganisasjonene primært vil ønske å inspirere sympatisører til terror, vil internasjonale ekstremistiske nettverk fortsatt ha en intensjon om å rekruttere personer som allerede befinner seg i Europa. Rekrutteringsforsøk vil som hovedregel være opportunistiske og fokusere på å veilede, eventuelt inspirere, sympatisørene.

Trusselen fra ekstreme islamister i Norge vedvarer

Selv om det ikke har blitt gjennomført ekstreme islamistiske terrorhandlinger i Norge siden 2022, jobber PST jevnlig med å avklare og forebygge alvorlige bekymringer. Trusselen fra ekstreme islamister er derfor vedvarende, til tross for at det fortsatt er få personer i Norge som støtter ekstrem islamisme.

Flere personer i Norge har forbindelser til europeiske og andre internasjonale ekstreme islamistiske nettverk. Slike nettverk kan potensielt be personer i Norge om å tilrettelegge for eller utføre terror. Alternativt kan nettverkene legge til rette for at personer i Norge får kontakt med andre som kan bistå dem i terrorhandlinger.

I Norge er det fortsatt ingen tydelige åpne fysiske eller digitale ekstremistiske grupper med et felles mål. Mange ekstreme islamister er likevel knyttet til hverandre i løsere ideologiske nettverk eller andre typer relasjoner, for eksempel via slektskap, felles møtesteder, historiske nettverk eller tidligere terrorrelatert aktivitet. Tidvis ser vi forsøk på å danne grupper som forfekter ekstrem islamisme. Om det skjer, kan det skjerpe trusselbildet fordi det i ytterste konsekvens kan bidra til mobilisering, mer nettverksbygging utover landegrensene og styrket evne og vilje til å begå terror.

Terrortrusselen er derfor i stor grad relatert til enkeltpersoner som gjerne har en uklar tilknytning til nasjonale eller internasjonale nettverk, og som kan la seg inspirere og rekruttere til terror. Dette gjør at trusselen blir mer uforutsigbar og vanskeligere å avdekke.

Tidligere etablerte grupper er lite aktive, men det er lite som tilsier at veletablerte ekstremister er deradikaliserte. Denne situasjonen forventer vi vil vare ut 2026.

> *Terrortrusselen er derfor i stor grad relatert til enkeltpersoner som gjerne har en uklar tilknytning til nasjonale eller internasjonale nettverk, og som kan la seg inspirere og rekruttere til terror*

Det er mulig at enkelte norske ekstreme islamister forsøker å reise ut som fremmedkrigere i 2026. Vi forventer likevel fortsatt liten reell interesse for dette det neste året. Dette er positivt for terrortrusselen fordi fremmedkrigeraktivitet kan bidra til radikalisering, nettverks- og kapasitetsbygging. Samtidig kan selv enkeltpersoner som blir fremmedkrigere, gjøre trusselbildet mer alvorlig.

Videre forventer vi at personer i Norge vil støtte terrorvirksomhet i andre land finansielt.

Tilfeldige sivile rammes oftest ved et ekstremt islamistisk terrorangrep

Foto
Lise Åserud / NTB

I stadig flere saker PST jobber med, ser vi at personer sender penger til utlandet via digitale betalingstjenester, og i noen tilfeller er det mistanke om at de som mottar pengene støtter terrorisme. Ikke alle tjenestetilbyderne plikter å rapportere til norske myndigheter. I tillegg vil betalingstjenestene være i stadig endring. Vi forventer at denne utviklingen vil fortsette.

Trusselbildet i Norge kan endre seg raskt dersom det oppstår hendelser eller politiske saker som virker særlig provoserende på norske eller internasjonale ekstreme islamister. Propaganda kan også påvirke hva som trigger enkeltpersoner, og kan være vanskelig å forutse. Eksempler på triggerhendelser som kan virke negativt på terrortrusselen, inkluderer norsk militær deltakelse i muslimske land, oppfattet støtte til en konflikt som resulterer i lidelser for muslimer, og hendelser som oppfattes som krenkelser av islam eller muslimer.

Vi forventer å se flere tilfeller av koranbrenning i Norge i 2026. De siste årene har koranbrenninger og opplevde krenkelser av islam fått begrenset offentlig oppmerksomhet. Trusselbildet kan imidlertid endre seg raskt hvis oppmerksomheten om slike hendelser øker igjen. Historisk har vi for øvrig sett at terrorhandlinger som respons på oppfattede krenkelser av islam kan komme flere måneder og år etter de aktuelle hendelsene.

Digitale plattformer fortsetter å være hovedarena for radikalisering og rekruttering

Mye av aktiviteten blant ekstreme islamister i Norge i dag er relatert til radikalisering og rekruttering. Radikaliseringen vil fortsatt foregå på digitale og fysiske arenaer som kan overlappe og utfylle hverandre. I det fysiske rom forventer vi at radikalisering blant annet vil finne sted mellom venner, i familier, i fengsler og på treningsarenaer, skoler og religiøse arenaer. Aktiviteten foregår imidlertid i stor grad på nettet. I nasjonale og transnasjonale digitale nettverk på krypterte plattformer kan brukerne opptre og kommunisere anonymt, samt bygge relasjoner og tillit som er nødvendig for terrorplanlegging og støttevirksomhet.

Støtte til og videreformidling av ekstrem islamistisk ideologi er noe mer utbredt enn for få år siden. Sympatisørene viser generelt sin støtte på tvers av tidligere skillelinjer mellom IS og al-Qaida, og de gjenbruker propaganda fra tidligere år. Dessuten kombinerer de gjerne ideologi med argumentasjon basert på egne opplevelser og holdninger. Noe av materialet som konsumeres uttrykker en fascinasjon for vold. Ideologien er imidlertid fortsatt det sentrale utgangspunktet for radikaliseringsprosessen, eventuelt sammen med sekundære elementer som nettopp voldsfascinasjon.

Vår bekymring er at enkeltpersoner på egen hånd utvikler en terrorintensjon som følge av at de er blitt eksponert for ekstrem ideologi, voldsmateriale og et miljø som normaliserer holdninger om at vold er en legitim aksjonsform. Eventuelle personlige sårbarheter, som psykisk uhelse, utenforskap eller livskriser, kan medvirke til at bekymringen øker.

Terrororganisasjonene og sympatisørene deres vil også fremover produsere propaganda med høy grafisk kvalitet og klare, lettfattelige budskap som oppfordrer til terror. De vil fortsatt publisere propaganda på flere språk, og de vil kontinuerlig tilpasse seg endringer på digitale

plattformer. De vil benytte kunstig intelligens (KI) til oversetting og til å produsere blant annet video- og bildemateriale. Bare en liten del av propagandamaterialet som produseres og deles i dag, er på norsk. Vi forventer imidlertid at ekstremistisk materiale vil bli oversatt til norsk i enkelttilfeller.

Radikalisering blant unge ekstreme islamister er en utfordring

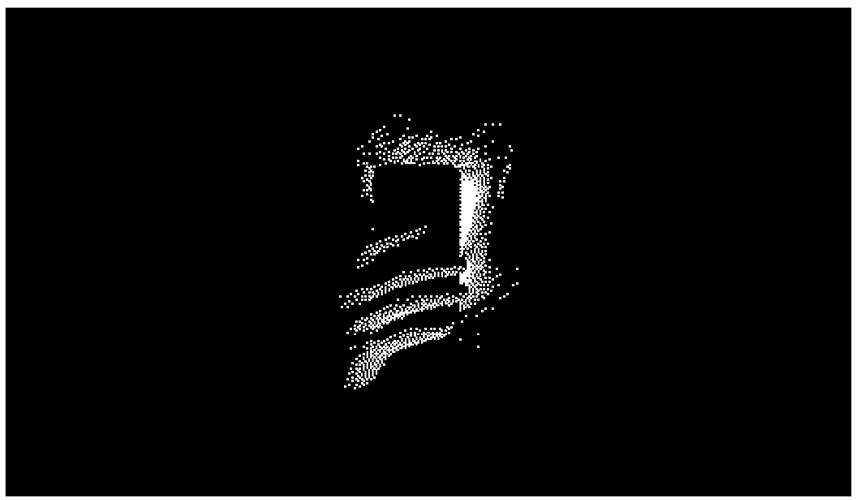
Vi forventer at radikaliseringen av mindreårige og unge voksne vil fortsette. PST har det siste året iverksatt en rekke forebyggende tiltak overfor personer i denne aldersgruppen. I noen tilfeller er bekymringen at de unge skal utvikle en terrorintensjon. De unge konsumerer, produserer og distribuerer tidvis grovt ekstremt islamistisk materiale på populære digitale plattformer som TikTok, uten at materialet nødvendigvis inneholder eksplisitte oppfordringer til vold. Vi ser også at offisiell og sympatisørprodusert propaganda gjerne retter budskapet mot ungdom og formidler det på plattformer som særlig unge bruker.

Aktiviteten blant de unge synes så langt hovedsakelig å handle om å spre ideologi, gi uttrykk for meninger og frustrasjon, søke etter fellesskap og oppnå anseelse. Den er likevel bekymringsfull, også fordi den sprer ekstrem ideologi til andre unge i Norge som ikke tidligere har vært eksponert for ekstremistisk materiale. Vi ser blant annet noe innhold på norsk og at det spres via formater og plattformer som er tilgjengelige og attraktive for unge.

→

PST er bekymret for at unge som radikaliseres på nett kan utvikle en terrorintensjon.

Illustrasjon
Getty / Dinamo Design



Mål og handlemåte ved et eventuelt ekstremt islamistisk terrorangrep i Norge

En eventuell ekstrem islamistisk terrorhandling i Norge vil mest sannsynlig bli utført av én eller få gjerningspersoner. De vil ofte være i kontakt med andre ekstremister i forkant av handlingen, enten digitalt eller fysisk.

Ekstreme islamister i Vesten velger fortsatt i hovedsak tradisjonelle angrepsmidler som kniv, skytevåpen, improviserte eksplosive innretninger (IED-er) og kjøretøy. Disse angrepsmidlene vil fortsatt være aktuelle i angrepsplanlegging, også i Norge. Vi ser for øvrig noe interesse for bruk av droner til både angreps- og rekognoseringsformål. Dessuten kan verktøy som utnytter kunstig intelligens, for eksempel såkalte KI-chatboter, bli brukt i forbindelse med angrepsplanlegging.

Ekstreme islamister anser alle mål i Vesten som legitime. Vi forventer fortsatt at tilfeldige sivile er den gruppen som vil bli rammet oftest, etterfulgt av politi- og forsvarspersonell. Personer og institusjoner som oppfattes å krenke religionen islam, er også aktuelle mål. I tillegg har samlingssteder for LHBT+-personer blitt mer aktuelle mål de siste årene.

Vi forventer at særlig israelske og jødiske mål blir utsatt for noe mer angrepsplanlegging det neste året enn det vi har sett tidligere. Siden 2014 har slike mål utgjort en liten andel av mål i angrepsplanlegging. Fra 2023 har derimot ekstreme islamister vist noe mer interesse for disse målene, i tillegg til kristne mål.

Hva kan føre til at trusselen fra ekstreme islamister i Norge skjerpes?

Hva som utløser at personer radikaliseres, og at enkelte ønsker å utføre terrorhandlinger, varierer og kan være utfordrende å forutse. Her fremhever vi likevel tre forhold som kan skjerpe trusselen fra ekstreme islamister dersom de skulle inntreffe.

- **Triggerhendelser i eller relatert til Norge** kan – dersom de får stor oppmerksomhet – føre til at Norge får en mer sentral posisjon i fiendebildet til ekstreme islamister.
- **Økt deltakelse i nasjonale eller internasjonale ekstreme islamistiske nettverk på fysiske og/eller digitale arenaer** kan bidra til økt mobilisering og i ytterste konsekvens styrket evne og vilje til å begå terror.
- **Uttalelser og propaganda fra internasjonale terrororganisasjoner som eksplisitt oppfordrer til angrep mot Norge**, kan bidra til at antallet potensielle trusselaktører øker, og gjøre Norge mer aktuelt som mål for både nasjonale og internasjonale ekstreme islamister.

Trusselen fra høyreekstremisme

PST vurderer det som ***mulig*** at høyreekstremister vil forsøke å gjennomføre terrorangrep i Norge i 2026.

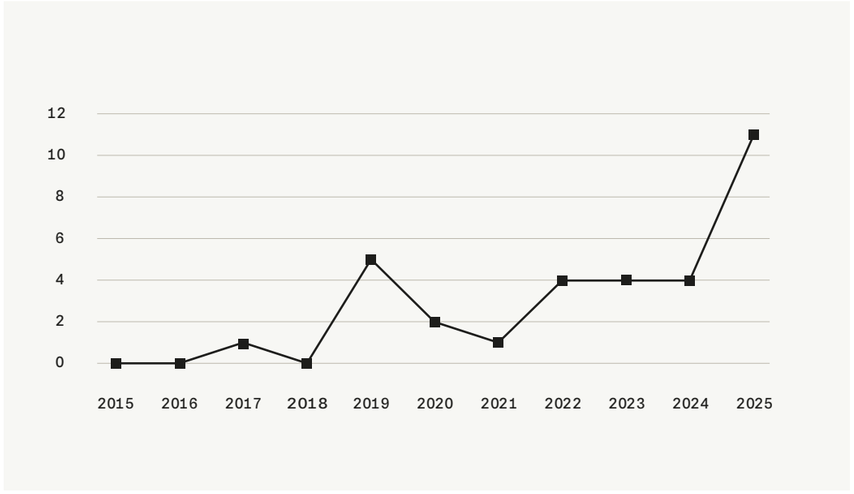
Flere som radikaliseres finner inspirasjon i voldsforherligende ideer uten en tydelig ideologi, blant annet gjennom nettfora som forherliger grotesk vold. Trusselbildet kompliseres derfor av at ideologi og voldsfascinasjon blandes sammen. Det gjør det mer krevende å peke på hva som er den utløsende årsaken til at en person utvikler aksept for vold.

Vi ser også en økning i antallet mindreårige gjerningspersoner som er involvert i høyreekstrem angrepsaktivitet i Vesten.

Høyreekstrem angrepsaktivitet i Vesten vedvarer – flere mindreårige er involvert

Den høyreekstreme angrepsaktiviteten i Vesten – det vil si gjennomførte og avvergede terrorangrep – har ligget på et stabilt nivå siden 2020. Vi forventer at det fortsatt vil være personer som forsøker å gjennomføre høyreekstreme terrorangrep i Vesten fremover.

Antallet mindreårige som har vært involvert i høyreekstrem angrepsaktivitet, har økt markant det siste året. Mindreårige var delaktige i bortimot 50 prosent av alle gjennomførte og avvergede angrep i 2025; i årene før var andelen rundt 20 prosent. Radikalisering av mindreårige er et tema som har vært tatt opp ved flere anledninger de siste årene. At mindreårige nå også involveres i angrepsaktivitet i Vesten, er en bekymringsfull utvikling.



Utviklingen i høyreekstrem angrepsaktivitet i Vesten der mindreårige har vært involvert i perioden 2015-2025

Kilde
Politiets sikkerhetstjeneste

Et enda mer mangfoldig og komplekst idélandskap

Høyreekstremisme omfatter et bredt spekter av retninger. De siste årene har idélandskapet utviklet seg til å bli enda mer mangfoldig og komplekst enn før. Mange som radikaliseres til høyreekstremisme, inspireres nå i større grad av ulike bevegelser og fellesskap. Videre ser vi at flere som radikaliseres, henter inspirasjon fra ideer som ikke har noen tydelig ideologi. Ideene finner de blant annet i nettfora som forherliger grotesk vold. Vår bekymring er at kombinasjonen av voldsforherligende ideer og høyreekstrem ideologi kan føre til raskere radikalisering av sårbare enkeltpersoner.

Tilhengere av ytre høyre viser stor bredde når det gjelder fremgangsmåter for å oppnå det samfunnet de ønsker seg. Blant høyreekstremister er det både de som oppfordrer til terror, de som gjennomfører terrorhandlinger, og de som jobber mer langsiktig gjennom høyreekstreme grupper. I tillegg omfatter ytre høyre også høyreradikale aktører som handler innenfor demokratiske rammer. Selv om vår bekymring for bruk av terror som fremgangsmåte primært retter seg mot høyreekstreme miljøer, kan fremtidige terrorister også bli inspirert av høyreradikale ideer. Enkelte kan finne inspirasjon og legitimitet i lovlige meningsytringer som fremsettes.

Voldsfascinasjon eller ideologi – hva kommer først?

Det mangfoldige idélandskapet gjør det vanskeligere å peke på hva som er de utløsende årsakene til at personer utvikler en aksept for vold. Én faktor kan være høyreekstrem ideologi. En annen faktor kan være en grunnleggende voldsfascinasjon, som kommer før en ideologisk overbevisning. Dette gjør trusselen mer uoversiktlig og uforutsigbar. Høyreekstremisme som fenomen blir også vanskeligere å avgrense, ettersom den ideologiske overbevisningen tidvis kan fremstå som overfladisk. Sammenblandingen av ideer gjør også at personer som radikaliseres, oftere faller i en gråsone mellom politiets og PSTs ansvarsområder. Dette gjør trusselbildet mer komplekst.

Den største terrortrusselen kommer fra aktører i digitale fora der det oppfordres til vold

Digitale plattformer vil fortsatt være hovedarenaen for rekruttering og radikalisering til høyreekstremisme. Det er en arena hvor det er lett å knytte kontakt, hente inspirasjon og spre ekstremistisk materiale på tvers av landegrenser og kontinenter.

Terrortrusselen fra høyreekstremisme vil særlig komme fra personer som deltar i digitale fora der det oppfordres til vold og terror. Spesielt er dette en utfordring i høyreekstreme transnasjonale fora der voldelig innhold florerer. I slike fora blir tidligere terrorister hyllet for sine gjerninger, og deltakerne oppfordres til nye terrorhandlinger. De får også veiledning i å bruke og produsere angrepsmidler og i hvordan de kan utføre terrorhandlinger. Vi mener at innholdet i disse foraene bidrar både til å radikalisere og til å styrke personers evne og vilje til å gjennomføre terrorhandlinger.

Høyreekstremistenes grunntanke er ideen om at staten og folket skal være en homogen enhet. Denne tanken bygger på forestillingen om en felles «hvit rase» eller «hvite» kulturelle kjennetegn. Ideen underbygges av konspirasjonsteorier om at den «hvite rasen» og «hvite kulturen» er i ferd med å bli utslettet. De som ikke tilhører dette fellesskapet, blir ansett som en trussel. Særlig beskyldes jøder, muslimer, personer med ikke-vestlig utseende, myndigheter, politikere, tradisjonelle medier, LHBT+-personer og aktører på den politiske venstresiden for å stå bak en slik utslettelse. Høyreekstremister mener det er legitimt å utøve vold for å forhindre denne utslettelsen de opplever.

PST er stadig bekymret for nordmenn som deltar i fora som forherliger vold og terror. Vi forsetter å identifisere nordmenn i slike fora. De fleste vi identifiserer, er mindreårige gutter og unge menn som har blitt introdusert for høyreekstremisme gjennom digitale kanaler.

Flere av gjerningspersonene bak gjennomførte og avvergede høyreekstreme terrorangrep i Vesten har vært aktive i slike transnasjonale digitale fora. Det er likevel viktig å understreke at potensielle terrorister ikke nødvendigvis deltar i slike fora; de kan også ha blitt radikalisert på andre måter.

Vi ser også at spillplattformer, som Roblox og Minecraft, har blitt aktuelle arenaer for høyreekstrem aktivitet. Spillplattformer er særlig relevante for rekruttering av mindreårige, ettersom mange mindreårige spiller på nett.

Vi forventer at det digitale høyreekstreme landskapet vil være dynamisk. Grupper vil bli opprettet og nedlagt fortløpende. Høyreekstremister vil også bruke flere digitale plattformer, ofte samtidig. Åpne plattformer, som TikTok, bidrar blant annet til å spre propaganda og til at likesinnede får knyttet kontakt. Krypterte plattformer, som Telegram og Signal, har funksjoner som legger til rette for anonym og kryptert kommunikasjon. Vi ser også at spillplattformer, som Roblox og Minecraft, har blitt aktuelle arenaer for høyreekstrem aktivitet. Spillplattformer er særlig relevante for rekruttering av mindreårige, ettersom mange mindreårige spiller på nett.

Det norske høyreekstreme aktørlandskapet – arenaer for rekruttering og radikalisering

I Norge finnes det et fåtall fysiske og flere digitale møteplasser for høyreekstremister. De har ulik størrelse, organisering, aktivitetsnivå og ideologisk forankring. Flere av dem har kontakt med likesinnede i andre land.

Etter vår vurdering utgjør det norske høyreekstreme aktørlandskapet en mindre terrortrussel enn flere av de transnasjonale. Grunnen til det er at vi ikke ser oppfordringer til terror eller en tydelig vilje til å begå terror blant norske aktører. Likevel er det vår vurdering at det norske høyreekstreme aktørlandskapet har betydning for rekruttering og radikalisering.

De fysiske høyreekstreme gruppene vil fortsatt finnes, men vi forventer at de vil være få og små. For å skape grupper som varer over lengre tid, er de fysiske miljøene avhengige av lederfigurer eller enkeltpersoner som klarer å rekruttere, skape samhold og radikalisere.

Parallelt med de fysiske gruppene vil det finnes en rekke digitale arenaer der norske høyreekstreme deler ideologi og propaganda. Vi forventer at mange av disse vil bli opprettet og nedlagt raskt, mens andre vil bestå over tid.

Det er mange måter å bli radikalisert på. Én mulig vei inn er å bli eksponert for høyreekstremt innhold på åpne sosiale medier. Derfra kan man bli sluset videre til mer ekstremt innhold på nye plattformer, noe målrettede algoritmer bidrar til. TikTok er en viktig inngangsport til

Radikalisering til høyreekstremisme skjer i stor grad på digitale plattformer.

Foto
Getty

høyreekstremisme. I tillegg er spillplattformer en sentral arena for rekruttering og radikalisering, spesielt blant yngre personer. I starten kan høyreekstremt innhold se ut som humor og virke ufarlig, også for dem som i utgangspunktet ikke søker etter slikt innhold.

Vi forventer at utfordringen med mindreårige og unge voksne som radikaliseres, vil vedvare. Flere av dem vil ha ulike former for sårbarheter, som psykisk uhelse og utenforskap. Blant de mindreårige og unge voksne ser sårbarheter ut til å spille en viktigere rolle for radikaliseringsprosessen enn ideologi. De er ofte drevet av en søken etter fellesskap, sosialt samhold og bekreftelse på egen verdi. Det kan gjøre dem mer mottakelige for ekstremistiske budskap. Trusselen kommer særlig fra enkeltpersoner som kan bestemme seg for å utføre en terrorhandling. Disse personene kan ha ulik tilknytning til høyreekstreme nettverk. Særlig kan personlige forhold, som sårbarhet og livskriser, påvirke dem til å ville handle. Radikaliserte enkeltpersoner er alltid krevende for etterretnings- og sikkerhetstjenester å fange opp.

> *Blant de mindreårige og unge voksne ser sårbarheter ut til å spille en viktigere rolle for radikaliseringsprosessen enn ideologi. De er ofte drevet av en søken etter fellesskap, sosialt samhold og bekreftelse på egen verdi.*

Høyreekstremister i Norge kan bli brukt som et ledd i statlig påvirkningsaktivitet. Særlig kan høyreekstreme digitale fora være egnede arenaer for å spre desinformasjon. Dette kan bidra til å nøre oppunder mistillit og dermed skape splid rundt vestlige politiske institusjoner og liberale verdier.

Mål og handlemåte ved et eventuelt høyreekstremt terrorangrep i Norge

En eventuell høyreekstrem terrorhandling i Norge vil mest sannsynlig bli utført av en enkeltperson.

Personer eller grupper som inngår i fiendebildet til høyreekstremister, er de mest utsatte terrormålene. Dette kan være personer med ikke-vestlig utseende, muslimer, jøder, politikere, myndighetspersoner, LHBT+-personer, tradisjonelle medier og aktører på den politiske venstresiden.

Økningen av mindreårige gjerningspersoner kan i større grad føre til angrep på steder der de ferdes, for eksempel skoler. Skoler kan være et kjent og lett tilgjengelig mål, der det også kan oppholde seg grupper de har i sitt fiendebilde.

De mest sannsynlige formene for angrep er masseskadeangrep og målrettede drapsforsøk mot enkeltpersoner. Ulike former for skadeverk eller ødeleggelse av eiendom, bygg og anlegg er også aktuelle angrepsformer. Formålet vil være å utløse en «rasekrig» og samfunnskollaps.

Skytevåpen, IED-er og stikkvåpen er de angrepsmidlene som har vært mest benyttet i høyreekstrem terrorangrep i Vesten de siste årene. Det forventer vi også at de vil være i 2026. I tillegg kan brannstiftelse være et aktuelt angrepsmiddel.

Enkelte høyreekstremister i Vesten vil vise interesse for ny teknologi til bruk i angrep. Vi forventer fortsatt en interesse for og forekomst av 3D-printede våpen. Det vil imidlertid fortsatt være krevende å lage funksjonelle improviserte skytevåpen med høy kapasitet ved hjelp av 3D-teknologi. Droner har til nå vært lite benyttet, men kan være nyttige til rekognoseringsformål. Videre kan KI-verktøy bli brukt i angrepsplanlegging, først og fremst til innhenting av informasjon.

Hva kan føre til at trusselen fra høyreekstremister i Norge skjerpes?

Hva som utløser at personer radikaliseres, og at enkelte ønsker å utføre terrorhandlinger, varierer og kan være utfordrende å forutse. Her fremhever vi likevel tre momenter som kan føre til at terrortrusselen fra høyreekstremister skjerpes i 2026:

- **Triggerhendelser:** Hendelser eller utviklingstrekk i samfunnet som høyreekstremister opplever som en trussel mot «den hvite rase», kan trigge enkelte til å ville utføre terror. Hvordan høyreekstremister evner å utnytte slike hendelser eller utviklingstrekk til å fronte sitt verdensbilde, kan også ha betydning. Nye høyreekstreme terrorangrep kan også inspirere enkelte til handling. Triggerhendelser kan inntreffe raskt og være vanskelige å forutse. Det gjør trusselbildet uforutsigbart, og trusselen fra høyreekstremister kan endre seg raskt.
- **En betydelig økning i antallet nordmenn som deltar i transnasjonale høyreekstreme fora der det oppfordres til vold:** Slik deltakelse kan styrke personers evne og vilje til å begå terrorhandlinger og øke antallet potensielle trusselaktører.
- **Sammenblanding av voldsforherligende ideer og voldsfremmende høyreekstrem ideologi:** Sammenblanding av groteske voldsuttrykk og høyreekstrem ideologi, særlig ideologiske retninger som eksplisitt fremmer vold og terror, kan føre til en raskere radikalisering av særlig sårbare individer, der enkelte bestemmer seg for å begå en terrorhandling.

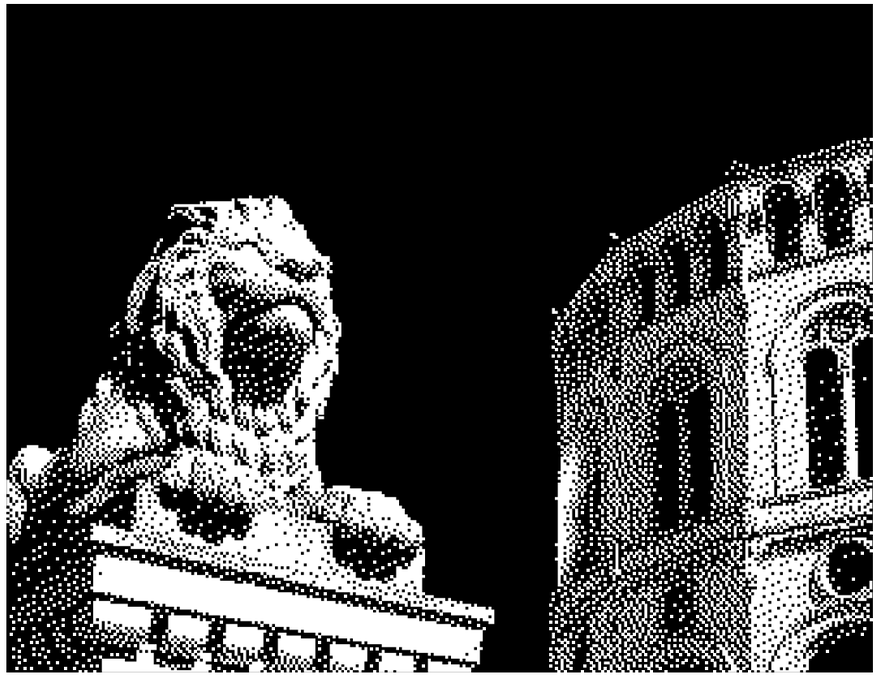
Antistatlig ekstremisme

Konspirasjonsteorier handler i stor grad om å finne forklaringsmodeller. Teoriene hevder at en elite eller mektig gruppe konspirerer, og det råder en forestilling om at disse sammensverger for å fremme en skjult plan eller agenda.

Altoppslukende konspirasjonsteorier radikaliserer

I kjernen av antistatlige overbevisninger ligger store og altoppslukende **konspirasjonsteorier**. Konspirasjonsteoriene kan radikalisere og motivere personer som tror på dem til å utføre voldelige handlinger basert på deres verdensbilde. Konspirasjonsteorier brukes gjerne som enkle forklaringer på komplekse problemstillinger og utviklingstrekk.

Antistatlige ekstremister har ikke én felles overordnet ideologi, men danner fellesskap der de fremmer mistillit og alternative forklaringer i konspirasjonspregede teorier. De skiller seg dermed fra høyreekstremister og ekstreme islamister, som har en dypere ideologisk eller religiøs forankring. Vi ser fortsatt at antistatlige ideer delvis overlapper med høyreekstemt tankegods. Akkurat som høyreekstreme arenaer kan også antistatlige arenaer bli brukt i statlige påvirkningsoperasjoner som kan spre desinformasjon via digitale fora.



Myndigheter er sentrale i fiendebildet til antistatlige aktører

Illustrasjon
Getty / Dinamo Design

I Norge ser vi to retninger innenfor antistatlig ekstremisme som kan akseptere, støtte og legitimere bruk av vold. Den ene retningen er opptatt av konspirasjonsteorier om **dypstaten** og andre altoppslukende konspirasjonsteorier. Den andre retningen anser seg som **suverene borgere** og mener at staten er illegitim og derfor ikke har grunnlag for å utøve makt. Retningene er imidlertid overlappende.

Antistatlige aktører er ofte eldre enn de som radikaliseres til høyreekstremisme eller ekstrem islamisme. I tillegg har de ofte hatt en negativ opplevelse med myndighetene, og de har gjerne konsumert konspiratorisk innhold på nettet i flere år.

Fienden demoniseres

Personer som fremstår som representanter for myndighetene, for eksempel politi og myndighetspersoner, kan bli sett på som legitime mål for vold fra antistatlige aktører. For dem som sympatiserer med antistatlige ideer, er staten, «systemet» og myndighetsapparatet fienden, gjerne omtalt som en ond elite som handler på bekostning av befolkningen. Ifølge sympatisørene består denne eliten av globalister, pedofile og satanister med onde intensjoner. Fienden omtales tidvis som så farlig og ond at noen til slutt mener at vold er nødvendig.

Antistatlig ekstremisme er fortsatt et relativt marginalt fenomen i norsk kontekst. Etter pandemien har vi imidlertid sett at flere av de store konspirasjonsteoriene fortsetter å radikalisere enkeltpersoner, også i Norge. Enkelte antistatlige aktører fokuserer i økende grad på såkalt **militant prepping**. I andre vestlige land har vi sett tilfeller av at antistatlige aktører bygger kapasitet for å velte styresmaktene og avsløre den påståtte onde elitens skjulte planer. Etter vår vurdering kan kapasitetsbygging og militant prepping forsterke en radikaliseringsprosess, ettersom det kan styrke kombinasjonen av å ha både kapasiteten til og intensjonen om å gjennomføre en politisk motivert voldshandling.

Alvorlighetsgrad og voldspotensial kan bli underkommunisert og misforstått

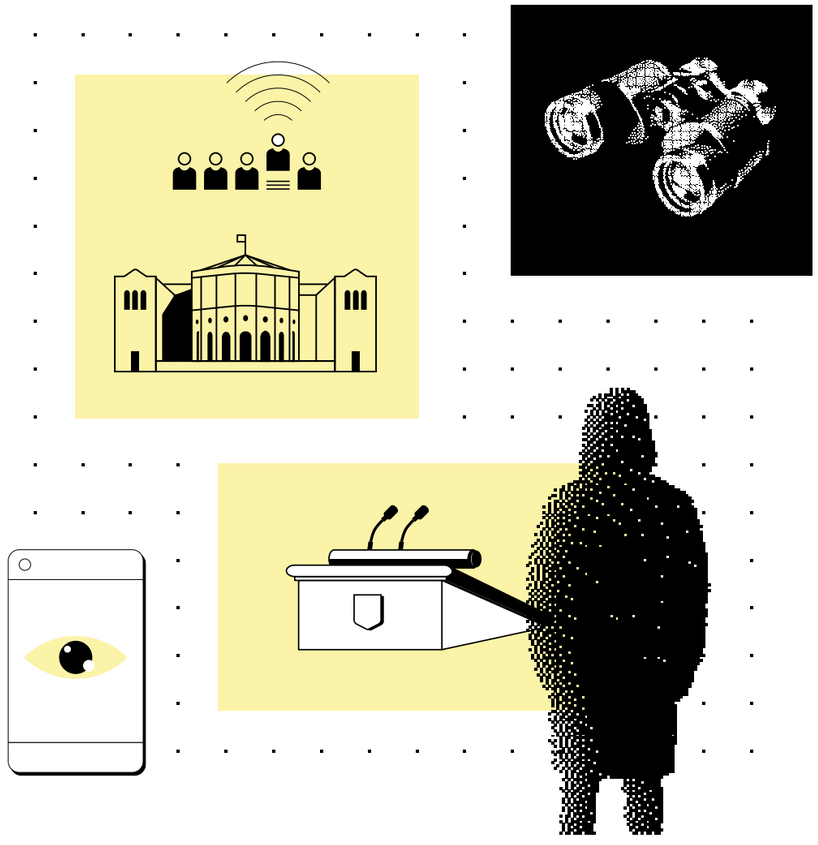
Antistatlige overbevisninger kan tidvis bli forvekslet med vrangforestillinger. Da kan alvorlighetsgraden og voldspotensialet i de ekstreme overbevisningene bli underkommunisert og misforstått. Kombinasjonen av antistatlig ekstremisme og andre sårbarhetsfaktorer, som psykisk uhelse, kan sameksistere og forsterke voldsrisikoen.

> *Kombinasjonen av antistatlig ekstremisme og andre sårbarhetsfaktorer, som psykisk uhelse, kan sameksistere og forsterke voldsrisikoen*

Dypstaten:
Ideen om at myndigheter og samfunnstopper konspirerer med, eller jobber for, et hemmelig nettverk eller en skjult elite som ønsker å ta over makten i verden.

Suverene borgere:
Ideen om at staten ikke har legitimt grunnlag for sin maktutøvelse, og at statens lover og regler er maktmidler som krenker den enkelte borgers frihet og suverenitet.

Militant prepping er når noen forbereder seg på voldelig forsvar mot myndighetene. Forberedelsene er forenelige med dommedagsfokuset i de antistatlige konspirasjonsteoriene.



Illustrasjon
Getty / Dinamo Design

Kapittel 03

Trusselen mot myndighetspersoner i Norge

Myndighetspersoner har det øverste beslutningsansvaret for områder som har stor påvirkning på menneskers liv. De får derfor mye oppmerksomhet i ulike medier og blant folk. Beslutningsansvaret fører også til at bakgrunnen deres og personlige hendelser havner i søkelyset. Derfor er myndighetspersoner utsatt for digital hets og trusler, hensynsløs adferd og potensielt mindre voldshandlinger. Det er **lite sannsynlig** at norske myndighetspersoner blir utsatt for alvorlige voldelige handlinger. De vil imidlertid bli utsatt for etterretningsvirksomhet.

Utenlandske myndighetspersoner på besøk i Norge kan ta med seg sitt nasjonale trusselbilde hit. Hvis de for eksempel representerer en internasjonal konflikt som vekker engasjement i Norge, kan de bli utsatt for digital hets og trusler eller forsøk på å bli oppsøkt.

Myndighetspersoner er medlemmer av kongehuset, Stortinget, regjeringen og Høyesterett samt representanter for tilsvarende organer i andre stater som oppholder seg i Norge. PST har et særskilt ansvar for å forebygge og etterforske trusler mot myndighetspersoner. Også partiledere og ledere for ungdomspartiene faller inn under PSTs ansvarsområde.

Med **personlig motiverte trusselaktører** mener vi personer som gjerne er opptatt av én bestemt sak som berører dem personlig. De er ofte svært frustrerte, uten at det ligger en ekstrem ideologi til grunn. Slike personer kan ha psykisk uhelse og vanskelige livsforhold.

Med **verbal konfrontasjon** mener PST trusler eller hets som blir ytret direkte til myndighetspersonen. Hvis adferden overfor myndighetspersonen er svært skremmende eller hensynsløs, vil det også falle inn under begrepet.

Hets og trusler på digitale arenaer leder ikke direkte til voldshandlinger

Når myndighetspersoner kommer i medias søkelys i forbindelse med kontroversielle saker, kan det generere store mengder hets og trusler på digitale arenaer. Som oftest går hetsen og truslene over, men mot enkelte sentrale statsråder fremsettes hets og trusler kontinuerlig. PST har ikke observert at slik truende aktivitet leder til forsøk på eller planer om voldshandlinger.

De aller fleste som fremsetter hets og trusler på digitale arenaer, er det vi kaller **personlig motiverte trusselaktører.**

PST og politiet undersøker de mest alvorlige truslene. Vi erfarer at disse trusselaktørene sjelden har noe ønske om å begå vold, men heller et behov for å få utløp for frustrasjon.

Hets og trusler mot myndighetspersoner er en vedvarende utfordring for demokratiet fordi det kan få myndighetspersoner til å kvie seg for å komme med ytringer, avstå fra arrangementer og trekke seg fra verv. Hets og trusler kan også hindre rekruttering til politikken, særlig blant de unge.

Myndighetshat på digitale arenaer kan radikalisere enkeltpersoner

Vi er bekymret for at hets og trusler på digitale arenaer over tid vil svekke tilliten til myndighetene og skape en intensjon om vold for enkelte. Ventilering på digitale arenaer kan gi grobunn for konspirasjonsteorier mot myndighetspersoner. Myndighetshat på digitale arenaer kan bidra til radikalisering til høyreekstremisme og antistatlig ekstremisme. Myndighetshat i kombinasjon med konspirasjonsteorier eller høyreekstrem ideologi kan lede til voldsintensjon hos noen.

De fleste myndighetspersoner blir ikke utsatt for konfrontasjoner

Når myndighetspersoner blir oppsøkt, er det som oftest av politiske aktivister som er følelsesmessig engasjert i en enkeltsak. Dette skjer gjerne i forbindelse med offentlige arrangementer, og aktivistene ønsker å komme nær myndighetspersonene for å ytre et politisk budskap. Vi forventer at aktivister fortsatt vil forsøke å komme ansikt til ansikt med myndighetspersoner, men at intensjonen deres vil være å ytre budskapet sitt uten bruk av vold.

Oppsøkende adferd fra politiske aktivister kan oppleves ubehagelig og truende for myndighetspersonen. Slike hendelser kan påvirke hvordan de utfører arbeidsoppgavene sine og bli regnet som **verbal konfrontasjon**. Vi forventer å se tilfeller av verbal konfrontasjon i 2026.

En del personer ønsker å oppsøke medlemmer av kongehuset. Mange av disse personene har psykisk uhelse. Når noen gjør slike forsøk, er det som regel fordi de vil be om hjelp; de har ingen intensjon om å begå vold. Noen kan også innbille seg at de står i en spesiell relasjon til den kongelige (såkalt fiksering). Kontaktforsøkene retter seg i stor grad mot Slottet.

Det har ikke vært tilfeller av **fysiske konfrontasjoner** mot myndighetspersoner i Norge på flere år. Vi forventer som nevnt noen verbale konfrontasjoner fremover, og det er en risiko for at slike konfrontasjoner kan eskalere til mindre voldshandlinger uten at det var hensikten. Noen få sentrale politikere kan også bli utsatt for en planlagt fysisk konfrontasjon.

Myndighetspersoner inngår i ekstremisters fiendebilde

Som omtalt i kapittelet om politisk motivert vold inngår myndighetspersoner i fiendebildet til flere ekstremismeretninger.

Blant høyreekstremister knyttes myndighetene ofte til konspirasjonsteorier om at de jobber i det skjulte for å utrydde «den hvite rase». Enkelte triggerhendelser kan aktualisere myndighetspersoner i det høyreekstreme fiendebildet.

Myndighetene er sentrale i fiendebildet til antistatlige ekstremister. Staten, «systemet» og myndighetsapparatet i stort omtales gjerne som en ond elite som handler på bekostning av befolkningen. Dagsaktuelle hendelser som kobles til konspirasjonsteorier, kan forsterke mistilliten og dermed myndighetspersoners posisjon i det antistatlige fiendebildet.

Myndighetspersoner inngår også i ekstreme islamisters fiendebilde – som representanter for Vesten. Hvis en myndighetsperson kommer med uttalelser eller knyttes til en triggerhendelse som bygger opp under forestillingen av Vesten som fiende av islam, kan myndighetspersonen bli utsatt for negativ oppmerksomhet. Fiendebildet er imidlertid mangfoldig, og andre mål er i utgangspunktet mer utsatt.

Myndighetspersoner vil bli utsatt for etterretningsvirksomhet

Myndighetspersoner og personer tilknyttet dem er utsatte mål for fremmede staters etterretningsvirksomhet i Norge. Trusselen er størst fra Russland og Kina, men også andre land driver med denne typen aktivitet.

En utbredt form for etterretningsaktivitet er cyberoperasjoner, særlig i form av phishing. Phishingoperasjoner kan utføres via e-post, SMS, sosiale medier eller andre kommunikasjonsplattformer. Formålet er å lure folk til å laste ned skadevare eller oppgi innloggingsdetaljer. Konsekvensen kan være at en aktør får tilgang til en myndighetspersons private og profesjonelle korrespondanse, kalender og kontakt-nettverk. Denne typen sensitiv informasjon kan bli misbrukt til både etterretnings- og påvirkningsoperasjoner.

Myndighetspersoner er attraktive mål for fremmede staters påvirkningsoperasjoner både på grunn av tilgangene de har, og som representanter for norsk politikk og opinion. Statlige aktører kan forsøke å påvirke befolkningens tillit til politikere og politiske prosesser, for eksempel gjennom svertekampanjer, desinformasjon og forstyrrende aktivitet som er ment å skape uro. Påvirkning fra fremmede stater kan i ytterste konsekvens føre til økt polarisering og øke mengden trusler og hets mot myndighetspersoner.

Med **fysisk konfrontasjon** mener vi en konfrontasjon der det er fysisk kontakt mellom myndighetspersonen og trusselutøveren. Også kasting av gjenstander eller væske faller inn under begrepet.

EOS-tjenestene PST, Etterretningstjenesten og NSM

Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet har oppgaver og ansvarsområder som grenser til hverandre innenfor etterretning, overvåkning og sikkerhet (EOS) og kalles med en samlebetegnelse EOS-tjenester. De presenterer sine årlige offentlige vurderinger samtidig.

Politiets sikkerhetstjeneste (PST) er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste, underlagt Justis- og beredskapsdepartementet. PST har som oppgave å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet. Som ledd i dette skal tjenesten identifisere og vurdere trusler knyttet til etterretning, sabotasje, spredning av masseødeleggelsesvåpen, terror og ekstremisme samt trusler mot myndighetspersoner. Vurderingene skal bidra i utformingen av politikk og støtte politiske beslutningsprosesser. PSTs nasjonale trusselvurdering (NTV) er en del av tjenestens åpne samfunnskommunikasjon der det redegjøres for forventet utvikling i trusselbildet.

Etterretningstjenesten (E-tjenesten) er Norges utenlands etterretningstjeneste. Tjenesten er underlagt forsvarssjefen, men arbeidet omfatter både sivile og militære problemstillinger. E-tjenestens hovedoppgaver er å varsle om ytre trusler mot Norge og prioriterte norske interesser, støtte Forsvaret og forsvarsallianser Norge deltar i og understøtte politiske beslutningsprosesser med informasjon av spesiell interesse for norsk utenriks-, sikkerhets- og forsvarspolitikk. I den årlige vurderingen «FOKUS» gir E-tjenesten sin analyse av status og forventet utvikling innenfor tematiske og geografiske områder som tjenesten vurderer som særlig relevant for norsk sikkerhet og nasjonale interesser.

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal forebyggende sikkerhet. Tjenestens hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Gjennom rådgivning, kontrollaktiviteter, tilsyn, testing og forskning bidrar NSM til at virksomheter sikrer sivil og militær informasjon, systemer, objekter og infrastruktur med betydning for nasjonal sikkerhet. NSM er ansvarlig for et nasjonalt varslingssystem (VDI) som skal avdekke og varsle om cyberoperasjoner mot digital infrastruktur. NSM har også et nasjonalt ansvar for å koordinere håndteringen av alvorlige cyberoperasjoner. «Risiko»-rapporten er NSMs årlige vurdering av risikobildet for nasjonal sikkerhet. Rapporten anbefaler tiltak og vurderer hvordan sårbarheter i norske virksomheter og samfunnsfunksjoner påvirker risikobildet i lys av det trusselbildet som er beskrevet av Etterretningstjenesten og PST.

Nasjonal trusselvurdering 2026

Publisert i Norge i 2026 for Politiets sikkerhetstjeneste (PST)

pst.no

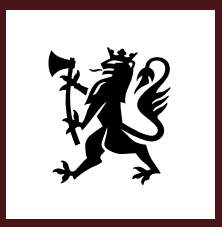
Opplag: 4000

Bilder i publikasjonen er hentet fra: Getty / NTB

Design og illustrasjoner: Dinamodesign.no

Trykk: Konsis.no

Trykksak
2041 0785



POLITIETS
SIKKERHETSTJENESTE

pst.no