PST
POLITIETS SIKKERHETSTJENESTE

Nasjonal trusselvurdering

2025

Nasjonal trusselvurdering 2025
Publisert i Norge i 2025 for Politiets sikkerhetstjeneste (PST)
pst.no

Opplag: 4000

Bilder i publikasjonen er hentet fra: Getty Images / NTB

Design og illustrasjoner: Aksell.no

Trykk: Aksell.no

Aksell AS er en Miljøfyrtårnbedrift

SVANEMERKET
Trykksak
2041 0379

TRYKT
I NORGE
NO - 1470

Politiets sikkerhetstjeneste (PST) er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste, underlagt Justis- og beredskaps-departementet. 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 etterretnings-tjeneste. 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 forebyggende sikkerhet. Direktoratets hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Gjennom rådgivning, tilsyn, testing, forskning og utvikling 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, NSMs årlige risikovurdering, skal gi norske virksomheter bedre forutsetninger for å se eget sikkerhetsarbeid i en større sammenheng. Rapporten beskriver sårbarheter trusselaktører forsøker å utnytte og tiltak for å redusere risikoen for at de lykkes.

Beate Gangås
Foto: Politiets sikkerhetstjeneste

Forord

Politiets sikkerhetstjenestes (PST) oppdrag er å forstå, formidle og motvirke de mest alvorlige truslene mot rikets sikkerhet. Vår nasjonale trusselvurdering (NTV) beskriver de truslene vi mener vil gjøre seg mest gjeldende i 2025.

Det er en urolig tid. Den sikkerhetspolitiske situasjonen er i endring og stiller krav til samfunnets tilpasningsevne. Krig, konflikt og rivalisering i verden vil fortsette å sette sitt preg på trusselbildet i Norge.

Russland forblir den største trusselen mot sikkerheten i Europa, og har det siste året vist vilje og evne til å gjennomføre sabotasjeaksjoner på europeisk jord. Det er sannsynlig at dette også kan treffe Norge. Samtidig er etterretningstrusselen fra Kina økende. Flere stater kan benytte proxy-aktører for å nå sine målsettinger i Norge.

Vi forventer at 2025 vil preges av sammensatte trusler. Dette inkluderer blant annet sabotasje, påvirkning og ulovlig etterretning. Slike virkemidler skaper usikkerhet, uro og frykt i befolkningen og angriper vårt demokrati. Samlet sett er truslene fra statlige aktører mot Norge mer uforutsigbare, mer omfattende og mer krevende enn på mange tiår.

Et voksende konfliktnivå i Midtøsten kan påvirke trusselaktører i Norge og føre til mer radikalisering, polarisering og uro. Vi ser at stadig yngre personer radikaliseres til ekstremisme, og mange av disse sliter med psykisk uhelse og ulike former for utenforskap.

Både ekstremister og statlige aktører ønsker å påvirke våre meninger og skaper utrygghet. Trusselaktørene forsøker å manipulere meningsdannelsen, enten for å øke oppslutningen om egne synspunkter eller for å svekke tilliten i samfunnet. Slik aktivitet kan bidra til polarisering. Vi forventer også hets og trusler mot myndighetspersoner når kontroversielle saker får mye medieoppmerksomhet, særlig i forbindelse med stortings- og sametingsvalget til høsten.

Et nært og godt samarbeid med andre samfunnsaktører er avgjørende for at vi lykkes i å motvirke truslene vi står overfor.

Beate Gangås
Sjef PST

Innledning

Nasjonal trusselvurdering (NTV) er en ugradert redegjørelse for trusselen fra statlige aktører, ekstremister og trusselen mot myndighetspersoner i det kommende året. Dette skal bidra til en felles nasjonal forståelse av trusselbildet.

NTV skal sette andre samfunnsaktører i stand til å beskytte seg mot trusler. Det er viktig at alle som leser rapporten, tar stilling til innholdet og vurderer relevans og konsekvens for seg selv eller egen virksomhet. Virksomheter og enkeltpersoner må selv kartlegge egne verdier og sårbarheter for å kunne sette inn egnede beskyttelsestiltak.

NTV skal også bidra til økt årvåkenhet i samfunnet generelt. Tips fra publikum er viktig for PST i arbeidet med å avverge og forebygge trusler mot Norge. Vi oppfordrer derfor alle som har en bekymring eller informasjon av interesse om å tipse oss. Det er lav terskel for å ta kontakt med PST.

Tips oss **PST.no/tips-oss**

TRUSSELKOMMUNIKASJON

Nasjonal standard	Beskrivelse
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

I vurderingen brukes et sett med standardiserte sannsynlighetsord. Formålet med disse er å skape en mer ensartet beskrivelse av sannsynligheten i vurderingene og derigjennom redusere uklarhet og misforståelser.

PSTs terrortrusselskala

PSTs terrortrusselskala har til hensikt å gi et samlet uttrykk for terrortrusselsituasjonen. Mens sannsynlighetsordene representerer PSTs vurdering av sannsynligheten for at det vil skje forsøk på en terrorhandling, gir skalaen uttrykk for graden av alvorlighet i situasjonen.

Det opereres med en skala på fem trinn, fra nivå 1 som betyr ingen terrortrussel til nivå 5 som betyr kritisk terrortrussel. I arbeidet med å fastsette et trusselnivå legger PST blant annet gjeldende trusselvurdering til grunn, sammen med en vurdering av (i) alvorlighetsgrad/skadepotensial ved en eventuell terrorhandling, (ii) usikkerhet og omfang av mangler i etterretningen knyttet til aktuelle trusselaktører, og (iii) vår/myndighetenes evne til å iverksette mottiltak før eventuelle trusler iverksettes.

Terrortrusselnivået fastsettes etter en kvalitativ vurdering. Terrortrusselnivået forsøker å beskrive flere komplekse forhold på en enkel måte.

En trusselvurdering vil alltid ligge til grunn ved en endring av terrortrusselnivået. Dette vil være en vurdering av hvordan relevante faktorer, aktører og hendelser påvirker trusselsituasjonen i Norge.

Nivå	Begrep
5	Kritisk terrortrussel
4	Høy terrortrussel
3	Moderat terrortrussel
2	Lav terrortrussel
1	Ingen terrortrussel

Kritisk terrortrussel: PSTs vurdering er at et terrorangrep er nært forestående eller et terrorangrep har blitt gjennomført og flere angrep kan inntreffe.

Høy terrortrussel: PSTs vurdering er at en eller flere personer har konkrete og realistiske planer og tar konkrete skritt for å gjennomføre terrorangrep og/eller at flere forhold forsterker terrortrusselen.

Moderat terrortrussel: PSTs vurdering er at en eller flere personer har en intensjon om å gjennomføre terrorangrep, men uten å ha tatt konkrete skritt eller å ha realistiske planer og/eller at noen forhold forsterker terrortrusselen.

Lav terrortrussel: PSTs vurdering er at det er få personer som har et ønske om å gjennomføre terrorangrep og/eller at få forhold forsterker terrortrusselen.

Ingen terrortrussel: PSTs vurdering er at ingen personer har et ønske om å gjennomføre terrorangrep, og det er ingen forhold som bidrar til en terrortrussel.

Figur: PSTs terrortrusselskala

HOVEDPUNKTER

Statlig etterretningsvirksomhet, påvirkning og sabotasje

Side 10

Russlands fullskala invasjon av Ukraina og det forverrede forholdet mellom Russland og vestlige land fortsetter å prege trusselbildet i Norge. I tillegg til kontinuerlig og omfattende etterretnings- og påvirkningsaktivitet er det økt sannsynlighet for at de russiske etterretningstjenestene vil forsøke å utføre sabotasjeaksjoner i Norge.

Norge er et etterretningsmål for Kina, og vi forventer at etterretnings-trusselen vil tilta på sikt. Vi ser også at påvirkningsaktivitet fra kinesiske aktører blir mer fremtredende, og at kinesiske aktører benytter både lovlige og fordekte metoder for å oppnå sine målsettinger i Norge.

Den spente sikkerhetspolitiske situasjonen og konflikter i Midtøsten vil fortsette å ha en innvirkning på trusselbildet i Norge. At terror-trusselnivået i Norge var høyt høsten 2024, blant annet som følge av trusselen fra Iran-tilknyttede aktører, illustrerer dette.

Fremmed etterretning vil bruke en rekke ulike virkemidler og metoder, som stadig tilpasses endrede forutsetninger og norske mottiltak. Flere av disse tiltakene inngår i det som ofte omtales som sammensatt virkemiddelbruk. Det inkluderer cyberoperasjoner, rekruttering av kilder, påvirkningsoperasjoner, sabotasje, fordekte anskaffelser og sikkerhetstruende økonomisk virkemiddelbruk. I tillegg vil flyktninger, dissidenter og regimekritikere bli utsatt for kartlegging og overvåking fra flere autoritære regimer.

Politisk motivert vold – ekstremisme

Side 28

Ekstrem islamisme og høyreekstremisme forventes å utgjøre de største terrortruslene mot Norge. Vi vurderer det som **mulig** at både ekstreme islamister og høyreekstremister vil forsøke å gjennomføre terrorhandlinger i Norge i 2025. Trusselen fra ekstreme islamister vurderes fortsatt å være noe mer alvorlig enn trusselen fra høyreekstremister. Dette skyldes blant annet økt ekstrem islamistisk angrepsaktivitet i Europa, at terrororganisasjonen Den islamske stat (IS) har økt angrepsintensjon i Vesten og at krigføringen mellom Israel og Hamas i Gaza har ført til mer radikalisering. Trusselen fra høyreekstremisme kommer primært fra høyre-ekstremister som deltar i transnasjonale voldsopp-fordrende digitale nettverk.

Digitale plattformer er hovedarenaer for radikali-sering og rekruttering. Vi ser større spredning av ekstremistisk innhold på populære, kommersielle plattformer enn tidligere.

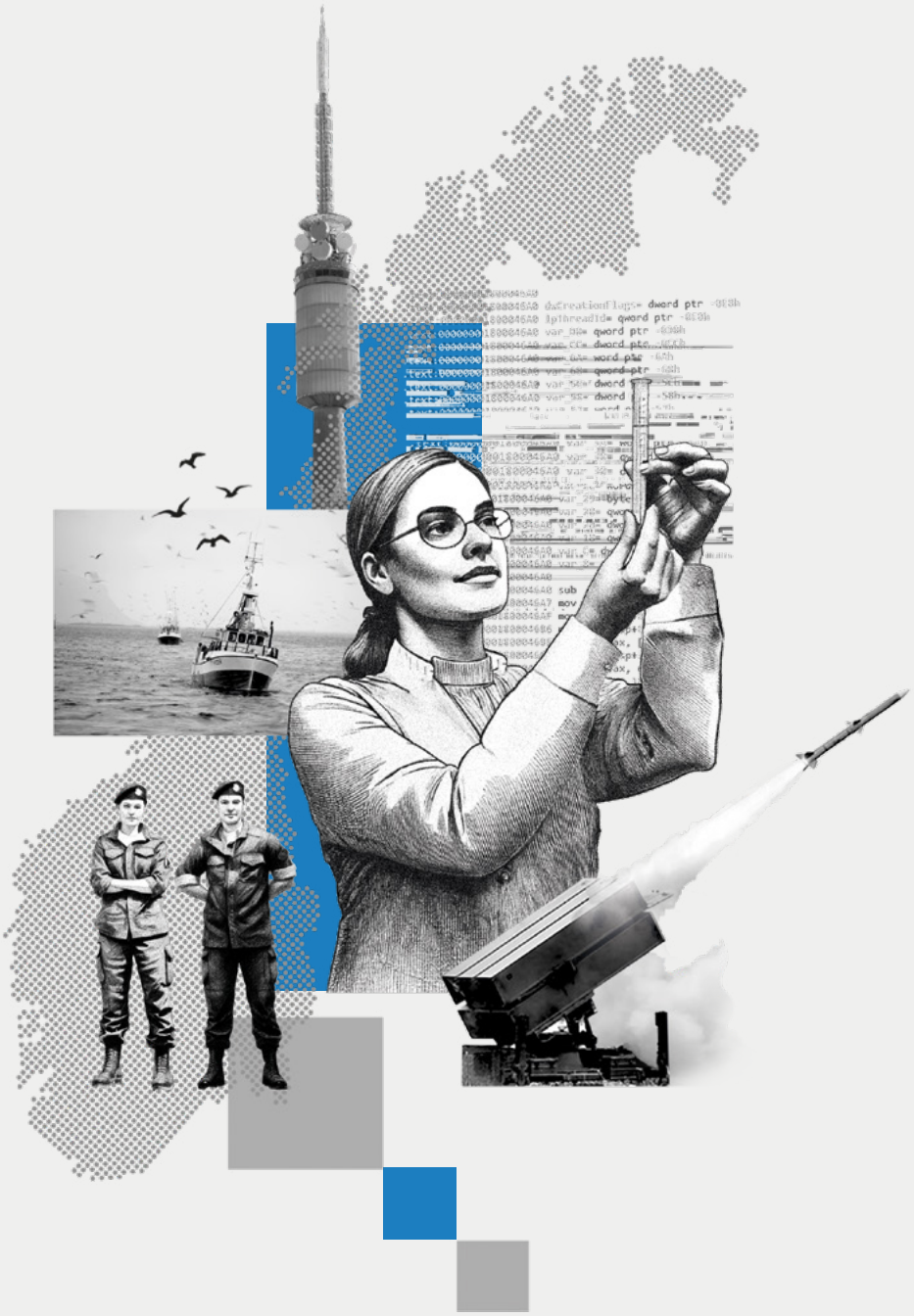
Vi observerer en negativ utvikling med flere unge som konsumerer voldsoppfordrende materiale på nett. Dette øker faren for radikalisering og rekruttering til ekstremisme blant unge mennesker i Norge. Bekymringen vår er at enkelte vil omsette ekstreme holdninger i terrorhandlinger.

Trusselen mot myndighetspersoner

Side 42

Vi vurderer det generelt som **lite sannsynlig** at noen vil forsøke å gjennomføre alvorlige voldelige handlinger mot myndighets-personer i Norge i 2025. Vi forventer mer hets og trusler mot myndighetspersoner når kontroversielle saker får mye medieoppmerksomhet – særlig i forbindelse med stortings- og sametingsvalget.

Myndighetspersoner vil fortsatt være utsatte mål for fremmede staters etterretningsvirksomhet.



Statlig etterretnings-virksomhet, påvirkning og sabotasje

Det siste året har vist flere eksempler på hvor alvorlig trusselen fra statlige aktører er. I løpet av 2024 har vi sett at Russland har lykkes i å gjennomføre flere titalls tilfeller av sabotasje og forstyrrende aktivitet på europeisk jord. I Norge har PST arrestert to norske borgere mistenkt for spionasje til fordel for Russland, Kina og Iran. Vi har sett at Russland har forsøkt å bygge opp igjen kapasiteten til å gjennomføre etterretning fra ambassaden i Oslo, etter at regjeringen erklærte en rekke etterretningsoffiserer uønsket i Norge i 2023. Vi har også hatt et høyt terrortrusselnivå store deler av høsten, blant annet grunnet faren for at Iran-tilknyttede aktører skulle gjennomføre terror i Norge.

Store deler av trusselbildet ligger fast i 2025. Russland og Kina fremheves som de mest sentrale aktørene, i tillegg til at vi forventer aktivitet fra Iran og Nord-Korea. Samtidig fremhever vi noen viktige endringer i trusselbildet i årets NTV: Sabotasjetrusselen fra Russland er større nå enn for ett år siden. Såkalte proxy-aktører er noe flere stater benytter. Cyberoperasjoner blir stadig mer krevende å avdekke. I tillegg forventer vi at påvirkningstrusselen fra blant andre Kina, blir mer fremtredende.

Norge vil i 2025 utsettes for etterretning, påvirkning, og potensielt sabotasje, fra statlige aktører. Dette er alle virkemidler som inngår i det som omtales som sammensatt virkemiddelbruk.

Det følgende kapittelet er vår vurdering av hva vi kan komme til å stå overfor det kommende året.

AKTØRENE OG DERES MÅL

Russland

Økt sabotasjetrussel fra Russland

Den sikkerhetspolitiske situasjonen har økt russiske etterretningstjenesters risikovilje i Europa. Siden slutten av 2023 har russisk etterretning gjennomført flere titalls sabotasjeaksjoner og forstyrrende aktiviteter ved bruk av *proxy-aktører*. Mål for aksjonene har primært vært eiendom og logistikkinfrastruktur knyttet til leveranser til Ukraina, men også ordinær sivil infrastruktur, blant annet transportmidler og butikker. Vi har så langt ikke observert forsøk på slike aksjoner i Norge.

PST vurderer det imidlertid som **sannsynlig** at russisk etterretning vil forsøke å utføre slike aksjoner mot mål i Norge i 2025. Hensikten med eventuelle aksjoner mot mål i Norge vil være å forhindre våre leveranser til Ukraina eller å påvirke opinionens holdning til Ukrainastøtte i negativ retning. Mål for eventuelle aksjoner i Norge vil sannsynligvis ligne på det vi har sett i Europa. I tillegg kan norskeid energiinfrastruktur også bli mål for sabotasje det kommende året. Om, hvordan og i hvilket omfang dette eventuelt vil skje, avhenger blant annet av Russlands intensjoner og utviklingen av krigen i Ukraina.

Proxy-aktører 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.

Fokus på militære mål, nordområdene og krigen i Ukraina

Som følge av den sikkerhetspolitiske situasjonen i Europa har Russland flere informasjonsbehov om NATO-land, som Norge. Forsvaret og allierte lands militære kapasiteter her til lands vil kontinuerlig være utsatt for russisk informasjonsinnhenting. Russisk etterretning vil også fortsette å kartlegge vår kritiske infrastruktur og forsøke å identifisere sårbarheter. Slik informasjon kan utnyttes for senere etterretnings-, påvirknings- og sabotasjeaktivitet, eller i ytterste konsekvens i en eventuell fremtidig væpnet konflikt med Norge. Vi forventer at aktører som er involvert i norsk politikkutforming, fremdeles vil være etterretningsmål for Russland. Dette gjelder særlig aktører knyttet til norsk forsvars-, utenriks- og sikkerhetspolitikk, men også innen sektorene justis og beredskap, næring og handel samt energi og miljø.

Forsvaret og en rekke andre statlige og private aktører i Norge er også mål på grunn av vår støtte til Ukraina. Vi forventer at russisk etterretning vil forsøke å innhente informasjon om norske donasjoner og direktesalg av våpen og annet materiell til Ukraina, men også forsøke å forstyrre, forsinke eller forhindre dette. I tillegg forventer vi at den norske meningsdannelsen

I 2022 ble en russisk borger pågrepet av Politiets sikkerhetstjeneste og siktet for forsøk på grov etterretningsvirksomhet til fordel for Russland. Mannen utga seg for å være en brasiliansk forsker, men innrømmet senere at han var russisk statsborger. I fjor var mannen en del av en utvekslingsavtale mellom Russland og Vesten. Bildet er fra da president Vladimir Putin tok imot russere som hadde sittet fengslet i vestlige land. Foto: Sergei Ilyin / Sputnik / NTB

vil være et mål for russiske påvirkningsoperasjoner, blant annet i den hensikt å påvirke holdninger knyttet til Russlands krig mot Ukraina.

Russland er underlagt et stadig mer omfattende sanksjonsregime som følge av fullskala invasjonen av Ukraina. Dette gjør at russiske aktører også i 2025 vil utføre fordekt anskaffelsesvirksomhet mot virksomheter i Norge som produserer eller utvikler varer, tjenester og teknologi av militær nytteverdi.

De russiske etterretningstjenestene vil utføre aktivitet mot mål i hele Norge. Samtidig vil nordområdene være av særlig interesse for Russland. Dette skyldes blant annet grenseområdene i Finnmark og den russiske tilstedeværelsen på Svalbard, samt at Arktis har fått økt strategisk betydning i en mer spent sikkerhetspolitisk situasjon. Politikere, departementer og andre premissleverandører for norsk nordområdepolitikk vil derfor være utsatte mål for russisk etterretnings- og påvirkningsaktivitet. Dette inkluderer næringslivsledere, sivilsamfunnet og akademia.

Kina

Russisk etterretning tilpasser virkemiddelbruken i møte med mottiltak

De russiske etterretningstjenestene benytter et bredt spekter av virkemidler og metoder mot mål i Norge. Virkemidlene tilpasses stadig endrede forutsetninger og norske mottiltak.

Siden Russlands fullskala invasjon av Ukraina i 2022 har Norge redusert antall russiske etterretningsoffiserer under diplomatisk dekke i Norge. I tillegg utfordrer strengere innreiseregler Russlands mulighet til å benytte seg av tilreisende, og restriksjoner for russiske fartøys anløp i våre havner har gjort det mer krevende for Russland å drive maritim fordekt etterretningsaktivitet.

Som følge av denne utviklingen forventer vi at Russland i økende omfang vil gjennomføre sin etterretnings- og påvirkningsaktivitet fra russisk territorium. Dette inkluderer blant annet digital påvirkningsaktivitet, *signaletterretning,* cyberoperasjoner og rekruttering av kilder via digitale kanaler.

Samtidig vil russisk etterretning fremdeles være fysisk aktiv på norsk territorium. Vi forventer blant annet at etterretningsoffiserer under diplomatisk dekke vil forsøke å rekruttere kilder og bedrive annen etterretnings- og påvirkningsaktivitet. Russland vil videre forsøke å sende tilreisende til Norge for å bedrive etterretningsvirksomhet. Det er også vår vurdering at russiske fartøy, samt russisk mannskap om bord på tredjelands fartøy, fremdeles utgjør en etterretningstrussel mot mål langs hele norskekysten.

Etterretningstrusselen fra Kina er betydelig og vil tilta på sikt

Norge er et etterretningsmål for Kina på grunn av vår geografiske plassering, innflytelse i internasjonale fora som Arktisk råd og vår nære allianse med Kinas største globale utfordrer, USA. I tillegg har vi teknologiske fagmiljøer innen felt Kina ønsker kompetanse på.

I det kommende året vil kinesiske etterretnings- og sikkerhetstjenester fortsatt forsøke å innhente informasjon, stilne kritiske stemmer og påvirke grupper og enkeltpersoner i Norge. Kinesisk etterretning utnytter eksterne aktørers spesialkompetanse, tilganger og ressurser i sine operasjoner. Dette gir kinesisk etterretning økt evne til å utføre avanserte operasjoner mot mål i Norge.

Kinas påvirkningsaktivitet blir mer fremtredende

I takt med Kinas stormaktsambisjoner blir landets påvirkningsarbeid mer fremtredende. Kina utviser i økende grad evne og vilje til å gjennomføre påvirkningsoperasjoner direkte rettet mot vestlige staters innbyggere. Kina har et omfattende system for påvirkningskampanjer i det digitale rom. En ny trend er at kommersielle selskaper bidrar til å profesjonalisere Kinas digitale påvirkningsoperasjoner. Dette omfatter for eksempel salg av falske

Signaletterretning (SIGINT) er innsamling av signaler, enten fra kommunikasjonsplattformer eller fra elektroniske signaler.

Digital påvirkningskampanje rettet mot et norsk publikum

I 2023 ble det for første gang avdekket en digital kinesisk påvirkningskampanje rettet mot et norsk publikum. Den angivelige norske nettavisen «Viking United News» var del av en større internasjonal kampanje der et kommersielt kinesisk selskap lagde over hundre falske nettsider, hvor kinesisk propaganda ble flettet inn i en strøm av nyhetsartikler som var stjålet fra legitime nyhetssider.

brukerkontoer, produksjon av videomateriale og ansettelse av influensere. Vi forventer derfor at kvaliteten på kinesisk desinformasjon vil styrkes, og at omfanget av digitale påvirkningskampanjer vil øke i årene fremover.

Mål for kinesiske etterretningsoperasjoner i Norge

Kinesisk etterretning forsøker å få innsyn i politiske beslutningsprosesser og å kartlegge lokale og nasjonale beslutningstakere og personer som kritiserer Kina. For å oppnå dette vil Kina fortsette å utføre cyberspionasje mot norske myndigheter, virksomheter og organisasjoner.

Kinesisk etterretning vil også forsøke å rekruttere norske borgere for å få tilgang til sensitiv og gradert informasjon. Kinesiske tjenester er generelt interessert i å rekruttere næringslivsaktører, militært personell, forskere og personer som sitter i sensitive stillinger i ulike myndighetsorganer og politiske organisasjoner. Utenrikspolitiske miljøer er særlig utsatt.

Personer i Norge vil bli forsøkt truet til taushet

Kinas globale og omfattende transnasjonale undertrykkelse er en vedvarende trussel mot enkeltpersoners demokratiske rettigheter og handlefrihet. Personer i Norge som uttaler seg kritisk om menneskerettighetssituasjonen og styresettet i Kina, er utsatt. Eksempelvis har

Norsk borger utsatt for digitalt rekrutteringsforsøk

I 2024 ble en norsk borger kontaktet via WhatsApp av en person som oppga å representere et kinesisk institutt. Personen ønsket kandidater, som kan ha egne kilder, til å levere rapporter basert på ikke-offentlig informasjon, mot betaling. Aktøren ønsket innsideinformasjon om temaer som er relevante for kinesiske sikkerhetsinteresser, som f.eks. tidlig varsling av sanksjoner og det aktøren omtalte som «anti-Kina-grep» som USA og Vesten kan innføre.

Kinesiske aktører har over tid vist interesse for å utvikle Kirkenes havn og etablere den som et transportknutepunkt i Arktis. Samtidig har PST pekt på den økende etterretningstrusselen fra Kina og partistatens ønske om kontroll over forsyningskjeder og om posisjonering i Arktis.
Foto: Adam Ihse / TT Nyhetsbyrån / NTB

representanter fra den kinesiske stat oppsøkt en menneskerettighetskonferanse i Oslo i den hensikt å true og skremme deltakere. Vi forventer at kinesisk etterretning fortsatt vil forsøke å overvåke dissidenter og opposisjonelle og forsøke å rekruttere kilder i kinesiske diaspora- og dissidentmiljøer i Norge. Mye av denne aktiviteten vil foregå digitalt. Ofte presses personene til å rapportere til kinesiske myndigheter gjennom trusler mot familiemedlemmer bosatt i Kina.

Kina bruker både lovlig samarbeid og fordekte metoder for å innhente kunnskap om teknologi med militært bruksområde

Kappløpet om å omsette ny teknologi til militær bruk er en del av den geopolitiske rivaliseringen. Kina søker å dra nytte av private aktører for å sikre rask militær modernisering. I praksis visker dette ut skillet mellom den sivile og militære sfæren. Forskningsledere, gjesteforskere og studenter fra institusjoner tilknyttet det kinesiske forsvaret (PLA) jobber i Norge med teknologi som kan brukes militært. Konferanser og seminarer er også arenaer som blir forsøkt utnyttet til å innhente informasjon av militær nytteverdi, og til å etablere relasjoner til personer med slike tilganger. I løpet av 2024 har personer fra institusjoner tilknyttet PLA deltatt på teknologivitenskapelige konferanser i Norge. Videre forsøker kinesisk etterretning å rekruttere norske borgere blant annet via LinkedIn, for å få informasjon fra forsvarssektoren om avansert teknologi og utstyr. Norske forskere som vurderer å reise til Kina for å jobbe i talentprogrammer og forskningsparker, bør ta høyde for at kompetansen de tar med seg, kan bli utnyttet til militære formål til fordel for den kinesiske stat.

Kinas viktigste virkemidler er økonomiske

Selv om Kina vil benytte sin betydelige etterretningskapasitet i Norge, forblir Kinas viktigste virkemidler økonomiske – som investeringer og oppkjøp. Den kinesiske interessen for Kirkenes havn er et eksempel på dette. Utbygging av eller kinesisk involvering i for eksempel logistikkinfrastruktur tilrettelegger for en langsiktig tilstedeværelse som styrker muligheten til å få informasjon fra og utøve press mot norske myndigheter.

Iran

Iran bruker terror som utenrikspolitisk verktøy

Iranske etterretningstjenester vil gjennomføre etterretnings- og påvirkningsoperasjoner i Norge det kommende året. Det iranske regimet kan også benytte terrorangrep, attentat og vold mot personer og grupper i Vesten for å stilne kritiske røster, hevne seg eller gi uttrykk for politisk misnøye.

Regimet vil trolig benytte seg av proxy-aktører til å forsøke å utføre vold og terror i Vesten i 2025. Det kan også ramme Norge. Slike proxy-aktører er personer eller grupper uten formell eller ideologisk tilknytning til det iranske regimet, og kan være kriminelle og andre som selger sine tjenester til iranske etterretningstjenester. Blant annet mistenker svenske myndigheter at svenske kriminelle nettverk utførte angrep mot Israels ambassader i Stockholm og København i oktober 2024 på vegne av det iranske regimet.

Voldelige handlinger på vegne av det iranske regimet rammer ikke bare iranske dissidenter, men også jødiske, israelske og amerikanske mål. I tillegg utpekes personer eller institusjoner som oppfattes som islamfiendtlige. Hvorvidt Iran vil utføre denne typen handlinger i Norge i 2025, avhenger blant annet av hvordan konfliktene i Midtøsten utvikler seg.

En eskalering av konflikten kan for eksempel føre til at det iranske regimet prioriterer å ramme jødiske og israelske interesser også på norsk jord.

Vi forventer at den iranske diasporabefolkningen i Norge vil utsettes for overvåking, hets og trusler fra iranske etterretningstjenester og fra aktører som agerer på vegne av disse. Personer tilknyttet akademiske institusjoner og media, menneskerettighetsforkjempere og personer som åpent kritiserer det iranske regimet, er særlig utsatt. Denne virksomheten skaper utrygghet og frykt, og kan føre til selvsensur.

I 2025 vil Iran også forsøke å innhente informasjon om norsk flerbruksteknologi, våpenteknologi og akademisk forskning. På den måten søker regimet å omgå internasjonale sanksjoner.

Anskaffelsesvirksomhet og spredning av masseødeleggelsesvåpen

Norsk teknologi er ettertraktet av statlige aktører

I 2025 forventer vi at fremmede stater vil forsøke å anskaffe norske varer, tjenester og teknologi på fordekte måter. Flere norske virksomheter produserer teknologi som er ettertraktet av en rekke statlige aktører, inkludert Russland, Kina og Iran.

Et bredt spekter av avansert teknologi er i dag sikkerhetspolitisk sensitivt fordi den kan benyttes til militære formål. Eksport av militær teknologi og sivil teknologi med militære bruksområder – såkalt «flerbruksteknologi» – er derfor strengt regulert gjennom eksportkontrollregelverket og sanksjonsregelverket.

Vi forventer at norske selskaper også i 2025 vil være utsatt for en betydelig trussel fra utenlandske aktører som opererer innenfor militære anskaffelsesnettverk. Særlig Russland har behov for vestlig teknologi for å opprettholde sin militære kapasitet og evne til krigføringen i Ukraina. Russland søker å anskaffe både avansert og enklere teknologi for å dekke sitt militære behov. Dermed vil et bredere spekter av norske virksomheter bli utsatt for anskaffelsesforsøk enn før invasjonen.

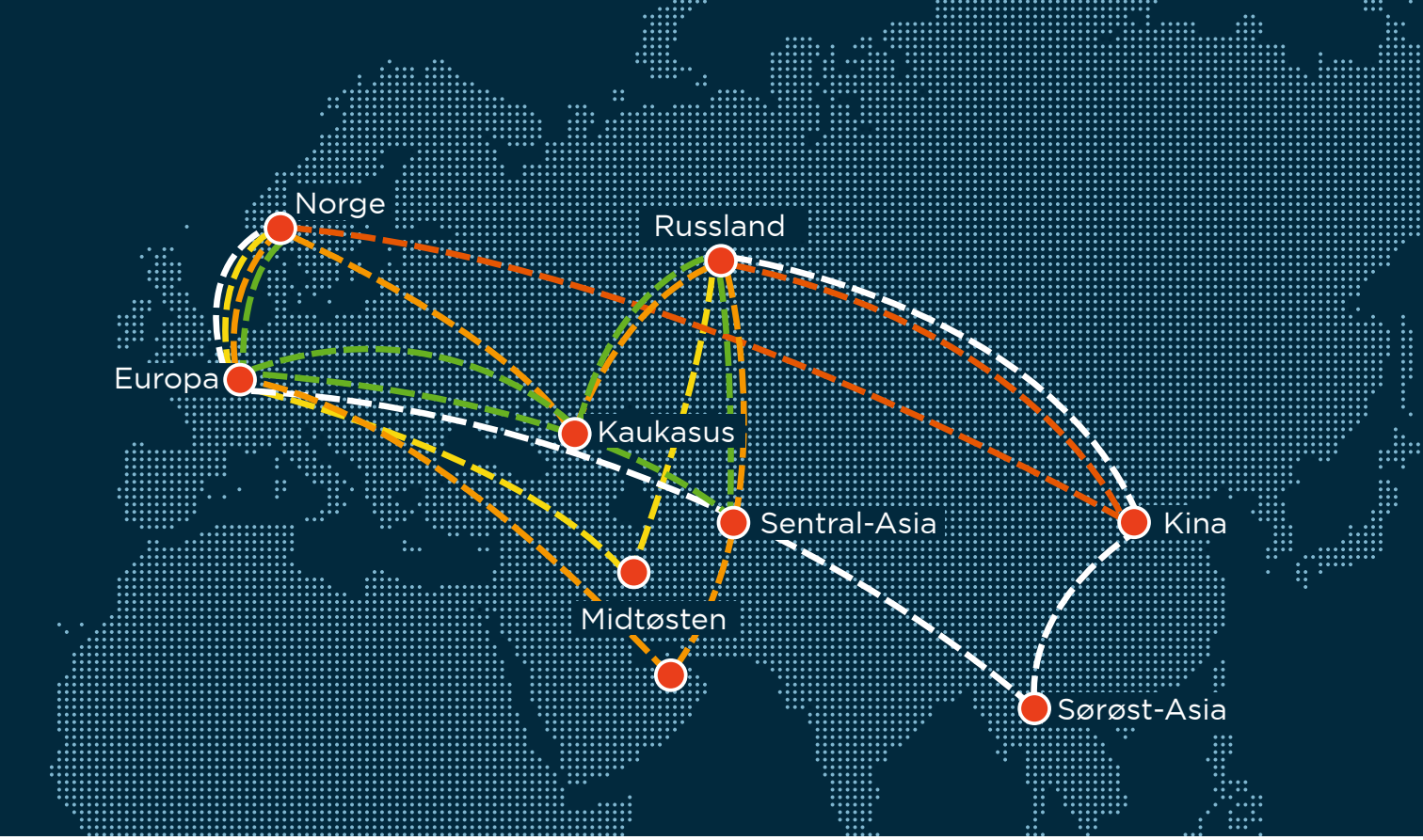
Anskaffelsesforsøk involverer ofte flere mellomledd i tredjeland. I 2024 har Russland eksempelvis forsøkt å anskaffe sanksjonert teknologi fra flere norske selskaper ved bruk av kinesiske mellomledd. Også selskaper i Europa blir utnyttet som ledd i fordekte anskaffelsesforsøk.

Russland benytter fordekte metoder for å omgå et stadig strengere sanksjonsregime. Blant annet forsøker russiske kjøpere ofte å villede norske virksomheter og tollmyndigheter ved å oppgi feilaktig dokumentasjon, for eksempel falsk sluttbrukererklæring.

Akademiske institusjoner og bedrifter er utsatte mål

Stater Norge ikke har et sikkerhetssamarbeid med vil i 2025 forsøke å tilegne seg sensitiv kunnskap fra norske forskningsinstitusjoner og kunnskapsbedrifter. Det siste året har vi særlig observert interesse fra Kina og Iran. Vi forventer at interessen fra disse, men også fra andre land det er knyttet bekymring til, vil vedvare i 2025.

Overføring av teknologi og kunnskap til fremmede stater kan utgjøre en trussel mot den nasjonale sikkerheten. Norske forskningsinstitusjoner og kunnskapsbedrifter har kompetanse og produserer teknologi på et høyt internasjonalt nivå. Dette inkluderer fagkunnskap som kan benyttes til å utvikle teknologi eller komponenter til militære formål. I den nåværende sikkerhetspolitiske situasjonen er enkelte lands myndigheter



Illustrasjonen viser hvordan norsk teknologi eller norske varer kan ende hos russiske sluttbrukere. Selv om de spesifikke rutene i grafikken er fiktive, baserer de seg på russisk metode for sanksjonsomgåelser. Illustrasjon: Aksell

Eksempler på trusselutsatte teknologiområder

- **Bioteknologi**
- **Materialteknologi og metallurgi**
- **Kjernefysikk**
- **Kryptografi**
- **Kvanteteknologi**
- **Nanoteknologi**
- **Romfart og fremdriftsteknologi**
- **Sensorteknologi**
- **Navigasjonsteknologi**
- **Robotikk og autonomi**
- **Mikroelektroniske systemer**

villige til å strekke seg langt for å få tilgang til og kontroll over slik kunnskap.

Forskningsinstitusjoner og andre kunnskapsbedrifter vil i 2025 være særlig utsatte mål for tilnærmelser fra fremmede stater. Statlige aktører vil blant annet forsøke å få tilgang til ansattes fasiliteter, slik som laboratorier og instrumenter, og vitenskap eller nettverk. De vil også bruke forskningssamarbeid, internasjonale konferanser og andre møtearenaer for å sikre seg tilgang til sensitiv teknologi eller skjermingsverdig informasjon.

METODENE

Fremmede staters etterretningstjenester bruker en rekke ulike metoder mot mål i Norge. I denne delen skisserer vi hvordan enkeltpersoner og virksomheter kan bli utsatt for følgende fenomener og virkemidler:

- **Cyberoperasjoner**
- **Rekruttering av menneskelige kilder**
- **Etterretning ved bruk av sivile fartøy**
- **Påvirkningsoperasjoner**
- **Sikkerhetstruende økonomiske virkemidler**
- **Transnasjonal undertrykkelse**

Statlige cyberaktører opererer stadig mer fordekt

Trusselen mot Norge i cyberdomenet er betydelig, men samtidig uforutsigbar. Det digitale trusselbildet påvirkes av et dynamisk aktørlandskap, geopolitiske hendelser og kontinuerlig teknologi- og metodeutvikling. Statlige cyberaktører opererer stadig mer fordekt, og dette utfordrer vår evne til å avdekke operasjonene og identifisere hvem som står bak. Det fører også til at det trolig er store mørketall for hvor mange virksomheter i Norge som rammes.

Vi forventer at norske virksomheter fortsatt vil rammes av cyberoperasjoner fra land som Russland, Kina, Nord-Korea og Iran i året som kommer. Russland og Kina har betydelig cyberkapasitet og forventes å stå bak de fleste cyberoperasjonene i Norge det kommende året. Samtidig har også iranske og nordkoreanske cyberaktører evne til å utføre operasjoner med betydelig skadepotensial.

Statlige cyberaktører benytter ulike typer proxy-aktører

For å kunne operere mer fordekt bruker statlige cyberaktører proxy-aktører. Eksempelvis bruker statlige aktører cybersikkerhets- og teknologiselskaper, cyberkriminelle og hacktivist-grupper til å utføre cyberoperasjoner eller utvikle kapasitet på sine vegne. Enkelte statlige cyberaktører utgir seg også for å være proxyaktører, eksempelvis ved å kopiere den digitale

signaturen til en hacktivist-gruppe. Både slik fordekt opptreden, og den faktiske bruken av proxy-aktører, gjør det vanskelig å avdekke hvem som egentlig står bak.

Utvikling av metoder og teknikker gjør trusselbildet mer uforutsigbart

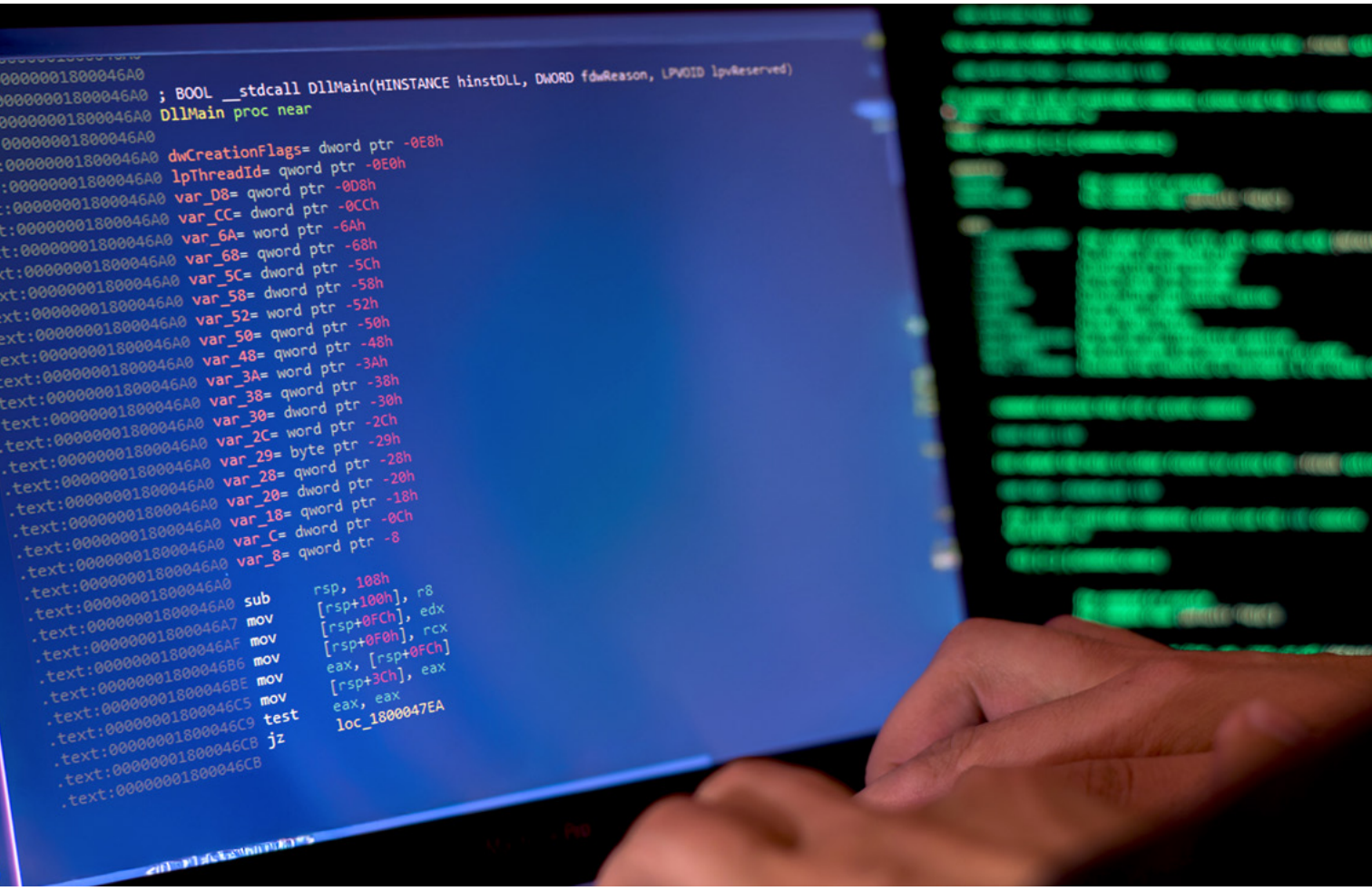
Statlige cyberaktører utvikler kontinuerlig egne metoder og teknikker. De siste årene har vi eksempelvis sett økt bruk av *nulldagssårbarheter* og *verdikjedeangrep*. Nulldagssårbarheter gir cyberaktørene mulighet til å utnytte en sårbarhet den utsatte ikke har kjennskap til. I enkelte operasjoner kan cyberaktøren ha tilgang til systemet i lang tid før sårbarheten blir kjent og tilstedeværelsen oppdaget.

En annen metode vi har sett i Norge, er at statlige aktører leier servere i datasentre under dekke av å være legitime virksomheter. Serverne som leies, kan benyttes til å kompromittere mål her til lands og i resten av verden.

I tillegg ser vi at statlige cyberaktører utnytter eksisterende og kjente sårbarheter i produktene til globale programvareprodusenter. De spiller også i stor grad på menneskelige sårbarheter i form av spearphishing-operasjoner. Aktørene blir stadig bedre på å skreddersy måter å tilnærme seg på som gjør det vanskeligere for offeret å avsløre operasjonen.

Nulldagssårbarhet. En nulldagssårbarhet er en sårbarhet som noen kjenner til, men som ikke er kjent for offentligheten, leverandøren eller produsenten av produktet. Det vil si at leverandøren eller produsenten av produktet ikke har fått mulighet til å utbedre sårbarheten, før en trusselaktør utnytter sårbarheten.

Verdikjedeangrep. Verdikjedeangrep er cyberoperasjoner rettet mot svake og mer perifere punkt i en virksomhets verdikjede, for eksempel hos underleverandører. Virksomheter med solide datasikkerhetssystemer og –rutiner er sårbare dersom deres underleverandører ikke har iverksatt tilsvarende sikkerhetstiltak.



Bildet på skjermen viser et utdrag fra skadevare utviklet av en statlig aktør. **Foto/illustrasjon: Politiets sikkerhetstjeneste/Aksell**

«Living Off the Land»

Flere cyberaktører bruker «Living Off the Land»-teknikker (LOTL) i cyberoperasjoner. Dette er en type teknikker som benyttes etter at cyberaktøren har utført et datainnbrudd og kommet seg inn i systemet, dvs. teknikkene aktøren bruker fra systemets dørterskel til selve målet for operasjonen. Teknikkene innebærer at en cyberaktør utnytter programvarer og funksjoner som allerede er en del av et IT-system til å forflytte seg rundt i systemet. Eksempelvis kan de gi seg selv flere tilganger i systemet. Ettersom cyberaktøren benytter eksisterende verktøy i systemene i stedet for skadevare, etterlates ingen spor, noe som gjør det mer utfordrende å avdekke en eventuell operasjon og finne ut hvem som står bak.

Personer i Norge vil bli forsøkt rekruttert

Kunstig intelligens skaper nye muligheter

Kunstig intelligens (KI) vil øke evnen og effektiviteten til samtlige cyberaktører, og det forventes at statlige aktører vil bruke KI i cyberoperasjoner i Norge i 2025. Flere stater investerer i utviklingen av teknologien og eksperimenterer med bruk av KI for å bedre egne metoder og teknikker. Bruk av KI kan blant annet øke kvaliteten på sosial manipulering og sette cyberaktørene bedre i stand til å identifisere og utnytte sårbarheter. Det er derimot vel så viktig å påpeke at KI gir betydelige muligheter til å forsvare seg mot trusler. Det er fremdeles vanskelig å vurdere om effekten vil være størst for trusselaktørene eller de som skal beskytte seg.

Statlige cyberaktører bruker KI til sosial manipulering

Kunstig intelligens kan øke aktørers evne og treffsikkerhet når det gjelder sosial manipulering. I 2024 ble det rapportert i åpne kilder at kinesiske, iranske, russiske og nordkoreanske cyberaktører benyttet store språkmodeller som støtte til sosial manipulering. Blant annet er KI blitt benyttet til å oversette tekst til forskjellige språk, å støtte cyberaktøren i lengre dialog med ofre innenfor spesialiserte fagfelt, og til å generere bilder, lyd og video. Dette benyttes blant annet i desinformasjonskampanjer og spearphishing-operasjoner.

Rekruttering og føring av kilder og andre medhjelpere er en sentral del av fremmede staters etterretningsvirksomhet i Norge. I 2025 er det særlig de russiske og kinesiske etterretningstjenestene som forventes å utgjøre den største trusselen når det gjelder rekrutteringsforsøk i Norge.

De siste årene har både Russland og Kina i stadig større grad utført rekrutteringsforsøk via digitale kanaler, som sosiale medier og andre applikasjoner. Publisering av jobbtilbud er en gjenganger i disse rekrutteringsforsøkene.

PST er blant annet kjent med at flere nordmenn er blitt spurt, for eksempel via LinkedIn, om å skrive rapporter for kinesiske tenketanker mot betaling. Dette fremstår innledningsvis som tilforlatelig og legitimt. Kina bruker reelle, men også fiktive, tenketanker som er opprettet for å rekruttere kilder.

De russiske etterretnings- og sikkerhetstjenestene utfører digitale rekrutteringsforsøk blant annet ved publisering av vage jobbannonser på grupper i sosiale medier, eller ved at fiktive brukere oppretter direkte kontakt med personer som ønskes rekruttert.

Digital rekruttering er kostnadseffektivt, relativt enkelt å videreføre over tid, og innebærer lav risiko for å bli oppdaget.

Fremmede etterretningstjenester vil også forsøke å rekruttere kilder fysisk. Dette kan skje i Norge, for eksempel ved bruk av etterretningsoffiserer under diplomatisk dekke. I enkelte tilfeller kan det imidlertid være enklere for fremmede etterretningstjenester å gjøre

rekrutteringsfremstøt mot norske borgere som oppholder seg i tredjeland.

PST vurderer det slik at personer med familiær eller annen tilknytning til autoritære stater, vil være særlig utsatt for rekrutteringsforsøk, både fysisk og digitalt. I dagens sikkerhetspolitiske situasjon må norske borgere som reiser til Russland forvente å bli utsatt for rekrutteringsforsøk under opphold i landet.

Personer rekruttert av fremmedes staters etterretningstjenester kan bli bedt om å utføre en rekke ulike oppgaver. Gradert informasjon vil alltid være av interesse, men vi ser også at fremmed etterretning ofte er interessert i ugradert, sensitiv informasjon som ikke er åpent tilgjengelig. Rekrutterte personer kan også bli bedt om å rekruttere sine egne kilder og å utføre praktiske gjøremål som å kjøpe sanksjonsbelagte varer, installere teknisk overvåkningsutstyr, og å utføre sabotasje, terroraksjoner eller voldshandlinger.

Etterretning ved bruk av sivile fartøy

Fremmed etterretning vil i 2025 fremdeles benytte sivile fartøy til etterretningsformål. Dette blir referert til som maritim fordekt etterretningsaktivitet (MFEA). MFEA rettes mot norske interesser på havet, i indre farvann og ved havner.

Langs norskekysten finnes det infrastruktur, teknologi og aktivitet som er interessant for fremmede stater. Fartøy kan bli brukt til å kartlegge norsk og alliert militær kapasitet samt kritisk infrastruktur på havbunnen og langs kysten. Fartøyene kan også konstruere situasjoner til havs for å avdekke svakheter ved norsk beredskap eller krisehåndtering.

Tilgangen til norske havner kan benyttes til å støtte ulovlig etterretningsvirksomhet. Denne tilgangen kan brukes til å smugle varer som er underlagt sanksjoner eller eksportkontroll og til å infiltrere etterretningspersonell inn på norsk fastland.

Russland utgjør den største trusselen innen MFEA. Per i dag er Russland underlagt omfattende restriksjoner, og russiske fartøy har ikke adgang til havner på norsk fastland. Det er gitt unntak fra havneforbudet for russiske fiskefartøy i Båtsfjord, Kirkenes og Tromsø,

Norske borgere vil bli utsatt for påvirkning fra fremmede stater

men med betydelige restriksjoner. Vi forventer likevel at russiske etterretningstjenester fortsatt vil søke å utnytte sivile fartøy som plattform for etterretningsaktivitet. Russisk mannskap om bord på fartøy som seiler under flagg fra tredjeland, vil også kunne utføre etterretningsvirksomhet mot norske mål.

Kina har også mulighet for å benytte MFEA. Den kinesiske etterretningsloven pålegger alle kinesiske personer, selskaper og organisasjoner å bistå de kinesiske etterretningstjenestene. Dette gjør at kinesiske personer og fartøy kan bli pålagt å bistå i kinesiske tjenesters innhenting av informasjon om norske forhold.

«Fartøy kan bli brukt til å kartlegge norsk og alliert militær kapasitet samt kritisk infrastruktur på havbunnen og langs kysten.»

Vi forventer at autoritære stater vil gjennomføre påvirkningsoperasjoner i Norge i 2025. I en tid med økt geopolitisk konflikt har fordekte påvirkningsoperasjoner og desinformasjon blitt sentrale virkemidler som fremmede stater benytter i forsøk på å endre beslutninger og holdninger til sin fordel. Hensikten er å bevare sikkerheten til eget regime gjennom å svekke det vestlige verdi- og sikkerhetsfellesskapet og styrke landets globale posisjon.

Påvirkningsoperasjoner kan foregå både i det fysiske og i det digitale rom. Russlands sabotasjeoperasjoner mot forsyningskjeder for forsvarsmateriell til Ukraina kan eksempelvis ha som mål å skape uro i samfunnet for å påvirke beslutninger om å sende forsyninger til Ukraina. Digitale påvirkningsoperasjoner kan eksempelvis være avsløringer av informasjon, anskaffet gjennom cyberoperasjoner, for å svekke tilliten til viktige samfunnsinstitusjoner. Dette omtales som «hack-and-leak».

I 2023 ble Norge rammet av en påvirkningsoperasjon fra en cyberaktør med tilknytning til iransk etterretningstjeneste, under dekknavnet Anzu team. Cyberaktøren gjennomførte først et datainnbrudd hos et svensk firma som tilbyr tekstmeldingstjenester. Deretter sendte aktøren ut tekstmeldinger til personer i Norge der de oppfordret unge muslimer til å hevne koranbrenninger.

Kinesiske digitale påvirkningsoperasjoner har tradisjonelt fokusert på kvantitet fremfor kvalitet. Kina og flere autoritære stater eksperimenterer med ulike teknikker for produksjon og spredning av påvirkningsmateriale, som på sikt vil øke dets kvalitet og overbevisningsevne. Selv om spredning av russisk og kinesisk desinformasjon ofte foregår på et globalt nivå, vil norske nettsamfunn likevel bli indirekte påvirket.

Russisk forsøk på å påvirke utvelgelsen av fredsprisvinneren

I 2015, et drøyt år etter at Russland vedtok å annektere den ukrainske Krimhalvøya, ble Norge utsatt for en russisk informasjonsoperasjon med mål om å påvirke Nobelkomiteen. Operasjonen innebar «lekkasje» av et falskt brev fra presidenten for det ukrainske parlamentet til en ansatt ved den amerikanske ambassaden i Oslo. I det falske brevet ble det hevdet at USA forsøkte å presse Nobelkomiteen til å gi fredsprisen for 2015 til den daværende ukrainske presidenten.

Statlige aktørers bruk av økonomiske virkemidler vil true nasjonale sikkerhetsinteresser

Vi forventer at både Russland og Kina ønsker å sikre sine nasjonale sikkerhetsinteresser gjennom investeringer i og oppkjøp av selskaper og eiendom i Norge. Bruk av sikkerhetstruende økonomiske virkemidler omfatter et bredt spekter av aktivitet. Dette kan blant annet innebære oppkjøp av eiendom i nærheten av kritisk infrastruktur, militære installasjoner eller infrastruktur av militær betydning. Strategisk plassert eiendom kan for eksempel benyttes til å utføre etterretningsaktivitet, og kan derfor utgjøre en trussel mot nasjonal sikkerhet.

I andre sammenhenger kan oppkjøp av eiendom dreie seg om strategisk plassering for å skaffe fotfeste eller innflytelse over tid. Eksempelvis besluttet regjeringen i 2024 at salg av eiendommen Søre Fagerfjord på Svalbard ikke vil kunne gjennomføres uten statens samtykke. Bakgrunnen for dette tiltaket er å redusere risikoen for at nasjonale sikkerhetsinteresser blir truet. Vi ser i tillegg at flere eiendommer i tilknytning til militære områder og områder av strategisk betydning, eies av russiske statsborgere med tilknytning til det russiske maktapparatet.

Aktiviteten kan også realiseres gjennom deltakelse i anskaffelsesprosesser eller investeringer i eller oppkjøp av selskaper, som gir nye eiere tilgang til sensitiv teknologi eller skjermingsverdig informasjon. Dette kan også gi stater kontroll over selskaper som er viktige for den nasjonale sikkerheten, eller over verdikjeder, som kan skape avhengigheter og benyttes som pressmiddel. Statlige aktører forsøker ofte å skjule sin involvering ved å benytte kompliserte eierskapsstrukturer eller tredjeparter.

Autoritære stater fortsetter å true regimekritikere

Flere autoritære stater vil fortsette å kartlegge og true flyktninger, dissidenter og regimekritikere bosatt i Norge i 2025. Dette skjer både fysisk og digitalt. Enkelte kan også bli rekruttert, gjennom press eller kultivering, til å utlevere informasjon om diasporamiljøer og opposisjonsaktivitet i Norge.

Autoritære stater utøver transnasjonal undertrykkelse i form av press, trusler og i ytterste konsekvens dødelig vold for å stilne kritikk mot sine regimer. Noen stater bruker sine diplomatiske representasjoner til å begrense sine kritikeres ytringsfrihet her i landet, for eksempel til å overvåke demonstrasjoner. De benytter også tilreisende etterretningsoffiserer, kriminelle eller infiltratører i diasporagrupper til dette formålet.

Transnasjonal undertrykkelse (TNU) er statlig bruk av virkemidler mot personer bosatt i andre land som vurderes å utgjøre en trussel mot regimet i den utøvende/ansvarlige staten. Hensikten bak virksomheten er å undergrave eller nøytralisere politisk opposisjon og kritikk.

Stater bruker cyberoperasjoner i transnasjonal undertrykkelse

Opposisjonelle, diasporaer og flyktninger er utsatt for cyberoperasjoner fra fremmede staters etterretningstjenester. Cyberaktørene benytter eksempelvis overvåkingsskadevare eller spearphishing-operasjoner til å kompromittere enkeltpersoner. Til sistnevnte benytter cyberaktørene ulike kommunikasjonsplattformer og sosiale medier, som LinkedIn og WhatsApp, i tillegg til tradisjonelle plattformer som e-post og SMS. Gjennom vellykkede cyberoperasjoner kan aktøren blant annet få tilgang til informasjon som gir etterretningstjenestene mulighet til å kartlegge nettverk og bevegelsesmønstre.


POLITI

Politisk motivert vold – ekstremisme

Terrortrusselen i Norge er på MODERAT nivå. De mest alvorlige terrortruslene i og mot Norge vil fortsatt komme fra ekstreme islamister og høyreekstremister. Selv om vi vurderer det som **mulig** at både ekstreme islamister og høyreekstremister vil forsøke å gjennomføre terrorangrep i Norge i løpet av 2025, anser vi trusselen fra ekstreme islamister som den mest alvorlige.

Dette skyldes blant annet økt ekstrem islamistisk angrepsaktivitet i Europa, at terrororganisasjonen Den islamske stat (IS) har økt angrepsintensjon i Vesten og at krigføringen mellom Israel og Hamas i Gaza har ført til mer radikalisering. Trusselen fra høyre-ekstremisme kommer primært fra høyreekstremister som deltar i transnasjonale voldsoppfordrende digitale nettverk.

Felles for kontraterrorfeltet er at digitale plattformer er hoved-arenaen for radikalisering og rekruttering. Vi ser større spredning av ekstremistisk innhold på populære kommersielle plattformer enn tidligere. Dette øker faren for radikalisering og rekruttering til ekstremisme i Norge. Radikalisering vedvarer, og erfaringsmessig kan en radikaliseringsprosess både ta kort og lang tid. Bekymringen vår er at enkelte vil omsette ekstreme holdninger i terrorhandlinger. Innen ekstrem islamisme og høyreekstremisme ser vi at mindreårige utgjør en økende andel av dem som radikaliseres.

Mindreårige som radikaliseres

Innen hele kontraterrorfeltet i Norge ser vi at stadig flere barn og unge radikaliseres. Vi forventer at denne negative utviklingen vil vedvare. Mindreåriges bruk av digitale plattformer bidrar særlig til denne radikaliseringen.

Ekstremistisk innhold er lett tilgjengelig på digitale plattformer. Her konsumerer og distribuerer mindreårige ekstremistisk materiale, og innholdet er tidvis svært voldsoppfordrende. Spredningen av denne type innhold på populære kommersielle plattformer, som TikTok og Instagram, øker faren for at unge mennesker i Norge rekrutteres til ekstremisme.

I Vesten ble det i fjor utført og avverget langt flere ekstreme islamistiske terrorangrep der mindreårige gjerningspersoner var involvert enn tidligere. Også innen høyreekstremisme blir gjerningspersonene yngre, men det er i hovedsak personer over 18 år som gjennomfører og planlegger høyreekstreme terrorangrep i Vesten. For mindreårige generelt ser vi et vedvarende fokus på skoler som mål. For disse er skoler et kjent og lett tilgjengelig mål, der det oppholder seg personer som inngår i deres fiendebilde.

Flere av de mindreårige som radikaliseres, har ulike utfordringer som gjør dem sårbare og dermed lett mottakelige for et ekstremistisk budskap, blant annet utenforskap og psykisk uhelse. Samhandling med andre samfunnsaktører er derfor særlig viktig i PSTs forebyggende arbeid med mindreårige.

TRUSSELEN FRA EKSTREM ISLAMISME

Vi vurderer det som **mulig** at ekstreme islamister vil forsøke å gjennomføre terrorangrep i Norge i 2025.

Trusselen kommer fra personer og nettverk som er inspirert av ideologien til Den islamske stat (IS) og til dels al-Qaida. Disse personene deltar eksempelvis i digitale fora hvor det deles ekstremistisk propaganda, og flere har tilknytning til ekstremistiske nettverk i Europa. Personene mobiliseres av nasjonale så vel som internasjonale hendelser. Den negative utviklingen vi har sett i 2024 med økt angrepsaktivitet i Vesten, forventes å fortsette. Konsekvensene av Israels krigføring i Gaza forventes fortsatt å være en radikaliserende faktor. Vi forventer ikke at Norge vil være et prioritert mål for ekstreme islamister i 2025. Nye hendelser, kriger og utviklingstrekk utenfor Norge vil kunne påvirke trusselbildet i Norge i 2025. Dersom utviklingen resulterer i at Norge nevnes i offisielle oppfordringer om terrorhandlinger fra terrororganisasjonene, vil dette påvirke trusselbildet betydelig i negativ retning.

PST vurderer trusselen fra IS og al-Qaida som sentral, fordi disse er terrororganisasjoner som har en global ekstrem islamistisk agenda. De hevder at Vesten er i krig med islam, både i og utenfor Vesten. Vestlig militær intervensjon i muslimske land og det de opplever som undertrykkelse og krenkelse av muslimer i Vesten, brukes til å legitimere terrorangrep. Fordi man i vestlige land velger sine egne ledere, oppfattes hele befolkningen som ansvarlig. Sivilbefolkningen blir dermed også et legitimt mål.

Negativ utvikling i internasjonal terrorisme

PST forventer fortsatt høy angrepsaktivitet i Europa fra personer som mobiliseres av Israels krigshandlinger og de sivile lidelsene i Gaza, og fra personer i nettverket til IS. IS har et sterkere fokus på å angripe i Vesten nå enn på flere år, og dette bidrar til at terrortrusselen i Europa øker.

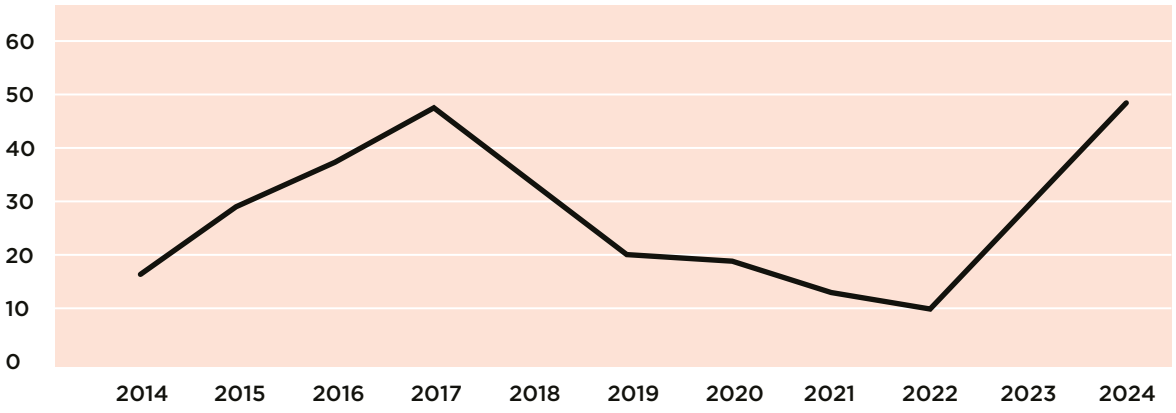
De to siste årene har angrepsaktiviteten økt betydelig, selv om de aller fleste angrepsplanene blir avverget av politi og sikkerhets- og etterretningstjenester. I 2024 gjennomførte ekstreme islamister 9 terrorangrep i Vesten. Det blir imidlertid avverget minst fire ganger så mange angrep. Dette viser at det har vært en kraftig økning i angrepsviljen, men også en økning i hva sikkerhets- og etterretningstjenester har evnet å forhindre. Mesteparten av angrepsaktiviteten i Vesten skjer i Europa.

Hovedandelen av de som blir pågrepet for angrepsaktivitet, er enkeltpersoner som sympatiserer med ekstrem islamistisk ideologi og

Med ekstremisme mener vi aksept for bruk av vold for å nå politiske, religiøse eller ideologiske mål. En ekstremist aksepterer bruk av vold, men bruker ikke nødvendigvis vold selv.

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.

Avvergede og gjennomførte ekstreme islamistiske angrep 2014–2024



Grafen viser avvergede og gjennomførte ekstreme islamistiske terrorangrep som PST har registrert i Vesten over en tiårsperiode. Vesten defineres her som Vest-Europa, USA, Canada, Australia og New Zealand. Graf: Politiets sikkerhetstjeneste

som ikke er tilknyttet en terrororganisasjon. Den økte angrepsaktiviteten i Europa i 2024 tilskrives særlig radikalisering som følge av Israels krigføring i Gaza samt påfølgende angrepsoppfordringer fra IS og al-Qaida som en følge av krigen.

Vi vurderer det samtidig slik at IS har en økt intensjon om å gjennomføre angrep i Vesten. IS utnytter personer og nettverk som allerede befinner seg i europeiske land og kan eksempelvis initiere eller forhåndsgodkjenne et terrorangrep utført av sympatisører. IS blir også kontaktet av potensielle gjerningspersoner som ønsker å utføre terrorhandlinger i IS sitt navn. På denne måten kan utøverne få veiledning og praktisk støtte til å planlegge angrep.

Europeiske sikkerhets- og etterretningstjenester har ved flere anledninger det siste året avverget angrepsrelatert aktivitet med tilknytning til IS. IS-filialen i Afghanistan og omland, Den islamske staten i Khorasan-provinsen (ISKP), utgjør den største terrortrusselen mot Europa. Samtidig vil også andre IS-filialer forsøke å initiere angrep i Europa, slik vi har sett at IS Somalia har forsøkt i Sverige i 2024. IS sin geografiske spredning på ulike kontinenter vanskeliggjør imidlertid effektive mottiltak fra sikkerhets- og etterretningstjenester. Internasjonale antiterroroperasjoner har ikke i tilstrekkelig grad klart å slå ned på IS-filialer i Afrika og Asia. Til tross for stadige tap av ledere, har gruppen klart å ekspandere.

IS har i sin propaganda særlig oppfordret sympatisører til å reise til de afrikanske filialene. Det er mulig at enkelte norske ekstremister kan forsøke å reise ut som fremmedkrigere i 2025. Det forventes imidlertid ingen større strøm av fremmedkrigere slik vi så for et drøyt tiår siden.

Al-Qaida fortsetter å prioritere lokal vekst. Det er særlig i afrikanske områder at al-Qaida har lyktes med å vokse. Al-Qaida har det siste året økt sin propagandaproduksjon betydelig. De vektlegger at krigshandlingene i Gaza må hevnes, og det er særlig israelske og amerikanske interesser som fremheves som angrepsmål.

Trusselbildet i Norge påvirkes av den internasjonale utviklingen

Vi er kjent med at det er forbindelser mellom personer i Norge og ulike ekstremistiske nettverk i Europa som er i kontakt med IS-filialer i Afrika og Asia. Gitt at IS har en økt intensjon om å ramme Vesten, øker slik kontakt vår bekymring. Norske kontakter kan bli bedt om å tilrettelegge for eller i verste fall utføre terrorhandlinger.

Vår vurdering er at krigføringen mellom Israel og Hamas i Gaza har bidratt til radikalisering i Norge i 2024. Både IS og al-Qaida utnytter krigen i rekrutterings- og radikaliseringsøyemed. Al-Qaida har det siste året økt sin propagandaproduksjon betydelig, og vektlegger at krigshandlingene i Gaza må hevnes. Begge terrorgruppene oppfordrer til angrep på israelske, jødiske og amerikanske mål, men også andre vestlige mål som våpenprodusenter og kirker har vært nevnt i den sammenheng.

Vi forventer at konflikten i Gaza vil bidra til ytterligere radikalisering og vil fortsette å påvirke terrortrusselen fra ekstreme islamister negativt i 2025. Denne vurderingen baserer seg på at krigføringen og lidelsene har hatt et stort omfang samtidig som dette har fått svært stor oppmerksomhet. Vi vurderer det slik at terrororganisasjonene vil søke å utnytte dette også i tiden fremover.

Situasjonen etter Bashar al-Assad-regimets fall i Syria er ved inngangen av 2025 uoversiktlig. Det er særlig muligheten for at IS vil styrkes i Syria som bekymrer ut i fra et kontraterrorperspektiv

Terrortrusselen i Norge kan skjerpes på kort varsel hvis internasjonale radikalisatorer eller terrorgrupper retter fokuset mot norske forhold. De siste årene har for eksempel koranbrenninger i Norge fått lite oppmerksomhet i tradisjonelle og sosiale medier. Trusselbildet i Norge kan imidlertid endres raskt dersom koranbrenninger i Norge får større medieoppmerksomhet, eller dersom det spres falske nyheter og misforståelser om dette. Andre hendelser eller handlinger som oppleves å krenke islam i Norge, vil også kunne skjerpe trusselen.

Terrorfinansiering

Vi mener det gjennomføres pengetransaksjoner fra Norge som har til formål å støtte terrorvirksomhet i andre land. I større grad enn tidligere gjennomføres transaksjonene ved bruk av tjenestetilbydere eller finansinstitusjoner som ikke er rapporteringspliktige til norske myndigheter. Eksempelvis brukes kryptovaluta og utenlandske finansinstitusjoner som rekrutterer kunder via Internett.

Vi forventer at denne utviklingen vil fortsette, og at vi vil se et marked for betalingsformidlinger og overføringer i stadig endring.

En ny generasjon ekstreme islamister

I Norge ser vi nå konturene av nye nettverk av unge ekstreme islamister. Nettverksbyggingen foregår primært på nett, og de har i liten grad kontakt med tidligere kjente ekstremistiske nettverk.

Flere ekstreme islamister i Norge deltar i transnasjonale digitale nettverk som kommuniserer via krypterte plattformer. Slik blir unge som deltar i disse nettverkene, påvirket av de samme sakene som ekstreme islamister i andre land er opptatt av.

Vi ser særlig en økning av mindreårige og unge voksne som konsumerer og distribuerer ekstremt islamistisk materiale på digitale plattformer. Eksempler på innhold er glorifisering av voldelig jihad og ytringer som kan forstås som støtte til IS eller al-Qaida.

Utviklingen der flere mindreårige og unge voksne konsumerer ekstremistisk materiale ses i sammenheng med reaksjoner på Israels krigføring i Gaza og større spredning av ekstremistisk innhold på digitale plattformer. Både IS og al-Qaida vektlegger propaganda til å formidle sitt budskap, rekruttere og komme med angrepsoppfordringer.

Spredningen av denne typen innhold på populære kommersielle plattformer, som Instagram og særlig TikTok, øker faren for at unge i Norge rekrutteres til islamistisk ekstremisme. Propagandaen er lett tilgjengelig og laget i et format som appellerer til mange unge. Vi forventer derfor økt radikalisering på nett, fortrinnsvis blant unge.

Skillet mellom digitale og fysiske nettverk vil fortsatt være flytende. Radikalisering vil foregå på begge arenaer, og disse har potensial til å forsterke hverandre. I fysiske nettverk forventer vi at radikalisering vil finne sted mellom venner, i familier, på skoler, på religiøse arenaer og i fengsler.

Mange ekstremister konsumerer propaganda fra både IS og al-Qaida. Vi ser også at propaganda av eldre dato blir distribuert på nytt. Det forventes at kunstig intelligens (KI) i større grad vil bli benyttet i propagandaproduksjon, ved for eksempel effektiv oversettelse til mange språk, bilde- og videogenerering og forfalskninger av bilder eller videoer. Sympatisører vil fortsette å produsere terroroppfordrende propaganda med høy grafisk kvalitet og klare, lettfattelige budskap. Vi forventer at ekstremistisk materiale i økende grad vil oversettes til norsk. Dette vil gjøre propagandaen mer tilgjengelig for norske brukere.

«Vi ser særlig en økning av mindreårige og unge voksne som konsumerer og distribuerer ekstremt islamistisk materiale på digitale plattformer.»

Enkle og lett tilgjengelige angrepsmidler

En eventuell ekstrem islamistisk terrorhandling i Norge vil mest sannsynlig utføres av én eller få gjerningspersoner som er inspirert av ideologien til IS eller al-Qaida. Gjerningspersonene vil ofte være i kontakt med andre ekstremister i forkant av terrorhandlingen, enten digitalt eller fysisk.

Vi forventer fortsatt at angripere vil benytte enkle og lett tilgjengelige angrepsmidler som hugg- og stikkvåpen, brannstiftelse eller kjøretøy. Avvergede angrep viser imidlertid at ekstreme islamister helst ønsker å forårsake massedrap ved å benytte improviserte eksplosive innretninger og skytevåpen. Skytevåpen kan omfatte både pistoler, hagler og rifler, og være anskaffet på lovlig eller ulovlig vis. Improviserte eksplosive innretninger vil sannsynligvis være relativt enkelt oppbygget, men kan fortsatt ha et betydelig skadepotensial. Fremover kan den teknologiske utviklingen påvirke valg av angrepsmidler. Det kan gi økt interesse for 3D-printede skytevåpen og droner som angrepsmiddel. Vi ser eksempelvis at droner i økende grad brukes i krig og konflikt, noe som kan være til inspirasjon for angrepsplanlegging i Norge.

I Vesten ble det i fjor utført flere terrorangrep av mindreårige enn tidligere. I tillegg var mindreårige involvert i mange avvergede angrep. Frem til 2024 har mindreårige sjelden klart å gjennomføre angrep, og kun et fåtall avvergede angrep har involvert mindreårige. Selv om vi forventer at mindreårige og unge voksne også vil ta del i angrepsaktivitet i 2025, forventes det også voksne gjerningspersoner.

Israelske, jødiske og kristne mål mer utsatt

Basert på propaganda og ideologiske føringer fra al-Qaida og IS forventer vi fortsatt at tilfeldige sivile, politi- og forsvarspersonell samt institusjoner eller personer som oppfattes å fornærme religionen islam, vil være aktuelle mål for ekstrem islamistisk angrepsaktivitet. I tillegg har samlingssteder for LHBT+-personer og religiøse samlingssteder de siste årene blitt mer aktuelle som mål.

Gjennom 2024 har ekstrem islamistisk propaganda i større grad enn tidligere rettet sitt fokus mot israelske og jødiske mål, men også kristne mål har vært fremhevet. I fjor så vi flere gjennomførte og avvergede angrep i Vesten mot nettopp disse målkategoriene. Vår vurdering er derfor at fokuset på jødiske og israelske mål har blitt markant forsterket, og at disse er blitt etablert som prioriterte målvalg innen ekstrem islamisme.

Terrortrusselen mot jødiske og israelske mål i Norge har over tid vært skjerpet. Denne utviklingen forventes å vedvare i 2025, fordi jødiske og israelske mål har fått økt betydning for ekstreme islamister, særlig som følge av israelsk krigføring i Gaza. Foto: Javad Parsa / NTB

TRUSSELEN FRA HØYREEKSTREMISME

Vi vurderer det fremdeles som mulig at høyreekstremister vil forsøke å gjennomføre terrorhandlinger i Norge i løpet av 2025.

Terrortrusselen fra høyreekstremister i Norge kommer primært fra høyreekstremister som deltar i transnasjonale voldsoppfordrende digitale nettverk. Vår erfaring er at enkeltpersoner i disse nettverkene kan utvikle evne og vilje til å begå terrorhandlinger.

Norske høyreekstremister forenes i ideen om at staten og folket skal være en homogen enhet basert på en forståelse om en felles «hvit rase» eller «hvite» kulturelle kjennetegn. De som ikke tilhører dette fellesskapet, anses av høyreekstremister å utgjøre en trussel. Videre bygger dagens høyreekstremisme på konspirasjonsteorier om at «den hvite rase» eller «hvite kultur» er i ferd med å bli utslettet. Denne opplevde eksistensielle frykten gjør at høyreekstremister mener at vold er legitimt for å forhindre utslettelse.

Transnasjonale nettverk påvirker trusselbildet negativt

Utviklingen og aktiviteten til transnasjonale digitale nettverk har vært en sentral drivkraft for terrortrusselen fra høyreekstremisme i Norge de siste årene. Særlig gjelder dette de nettverkene som er voldsoppfordrende. Her oppfordres deltagere til å begå terrorhandlinger. Målet er ofte massedrap eller målrettede drap på personer i det høyreekstreme fiendebildet. Vi er kjent med at nordmenn deltar i denne typen nettverk.

I de transnasjonale voldsoppfordrende nettverkene deles det grove voldsskildringer, propaganda og hyllester av tidligere terrorangrep. Deltagere i denne typen nettverk kan også knytte kontakt med likesinnede i andre vestlige land, og dermed bli en del av et internasjonalt nettverk av høyreekstremister. Dette gjør at personer langt utenfor våre grenser kan radikalisere og rekruttere til høyreekstremisme i Norge.

Vi er bekymret for at norske enkeltpersoner i disse nettverkene kan utvikle vilje og evne til selv å begå terrorhandlinger. At høyreekstremister i Norge deltar i slike nettverk har derfor en negativ effekt på det norske trusselbildet.

Enkelte transnasjonale voldsoppfordrende nettverk er også akselerasjonistiske. Høyreekstremister i slike nettverk utgjør fremdeles en særlig bekymring, ettersom det i disse nettverkene argumenteres for at det haster med å gjennomføre terrorangrep. Akselerasjonisme har vært en sentral ideologisk motivasjon ved flere høyreekstreme terrorangrep de siste årene.

Det er viktig å understreke at kun et fåtall av de som deltar i høyreekstreme nettverk vil forsøke å utføre terrorhandlinger. Til tross for at enkeltpersoner kan true med å begå terrorhandlinger, er vår erfaring at de færreste går fra ord til handling. Å identifisere og vurdere hvem som vil gå fra å konsumere og publisere voldsoppfordrende innhold til faktisk å forsøke å utføre en terrorhandling, vil fortsatt være krevende.

Et transnasjonalt nettverk består av personer og/eller grupper som oppholder seg i ulike land. Nettverkene opererer både på digitale og fysiske arenaer, og grad av lederstruktur kan variere. Deltagerne kan opptre anonymt eller med kjent identitet.

Akselerasjonisme er en høyreekstrem doktrine. Sentralt står ideen om at en «rasekrig» er nært forestående, og at det haster med å fremskynde en samfunnskollaps mens den «hvite rase» fortsatt er i demografisk flertall i Vesten. Terrorisme fremheves som et viktig verktøy for å destabilisere samfunnet og for å igangsette «rasekrigen».

Digitale plattformer er hovedarenaer for radikalisering og rekruttering

Store deler av den høyreekstreme aktiviteten foregår i dag på digitale arenaer. Vi forventer at digitale plattformer vil fortsette å være hovedarenaer for radikalisering og rekruttering til høyreekstremisme i Norge.

En radikaliseringsprosess er ulik fra person til person, og det er mange veier både inn og ut av en radikaliseringsprosess. I det digitale rom er imidlertid vår erfaring at et typisk radikaliseringsløp går fra åpne sosiale medier, som TikTok og Instagram, til digitale plattformer med mulighet for kryptert kommunikasjon. På krypterte digitale plattformer er innholdet ofte mer voldsforherligende og grenseoverskridende. For enkelte fungerer sosiale medier som digitale motorveier for radikalisering.

Høyreekstremt innhold er lett tilgjengelig på åpne digitale plattformer. Både algoritmer på sosiale medier, og dagens brukervennlige teknologi, gjør det enkelt å konsumere, dele og lage propaganda. Eksempelvis ser vi at TikTok for mange er en inngangsport til høyreekstremt innhold.

I tillegg til de transnasjonale nettverkene er også norske høyreekstreme digitale nettverk en kilde til bekymring for radikalisering. Også her kan man bli eksponert for høyreekstremt tankegods, dele propaganda og ikke minst knytte kontakt med likesinnede i Norge.

Selv om digitale nettverk er hovedarenaer for radikalisering og rekruttering, vil det fortsatt være aktivitet i det fysiske rom. Vi er kjent med at det høyreekstreme fenomenet Active Clubs har etablert seg i Norge. Active Clubs er et nettverk av mindre lokale grupper hvor det bygges fellesskap gjennom høyreekstrem ideologi og trening. Vi knytter i liten grad en terrorbekymring til Active Clubs i Norge, men vi er bekymret for at slike fysiske arenaer kan føre til at enkelte radikaliseres og bygger nettverk med likesinnede.

Vi forventer at norske høyreekstremister vil fortsette å hente ideer og inspirasjon fra ulike arenaer. Dette kan være fra andre ideologiske retninger, men også fra fellesskap og miljøer uten et tydelig ideologisk preg. Bruk av populærkulturelle referanser sammen med høyreekstrem symbolbruk er også en vedvarende trend. At høyreekstremister tar i bruk symboler og ideer fra ulike fellesskap og miljø, gjør at høyreekstremt tankegods kan appellere til flere enn tidligere. Denne utviklingen har de siste årene gjort trusselen fra høyreekstremisme mer uforutsigbar og uoversiktlig.

Bildet viser et hypotetisk, men realistisk eksempel på voldsoppfordringer og sjargong i høyreekstreme digitale nettverk. Bildet er illustrert av PST og viser en chattelogg på direktemeldingstjenesten Telegram. Brukeren er ikke ekte. Illustrasjon: Politiets sikkerhetstjeneste

Mange årsaker til radikalisering

De som radikaliseres til høyreekstremisme i Norge, har ulik bakgrunn og alder og kommer fra hele landet. Radikalisering og rekruttering til høyreekstremisme er med andre ord en landsomfattende utfordring.

Det er mange ulike årsaker til at personer oppsøker og deltar i høyreekstreme nettverk. Vi ser at den høyreekstreme propagandaens visuelle og estetiske utrykk fortsetter å appellere til de som rekrutteres til høyreekstremisme. Noen deltar i høyreekstreme nettverk som følge av ulike sårbarheter, eksempelvis psykisk uhelse, ensomhet eller søken etter sosiale fellesskap. Andre er ideologisk nysgjerrige, mens enkelte er på jakt etter underholdning eller har en fascinasjon for vold. Noen personer vil tiltrekkes av høyreekstreme nettverk for å tøye grenser gjennom politisk ukorrekt kommunikasjon.

Vi har over tid registrert at en andel av de som i dag radikaliseres til høyreekstremisme, er mindreårige og unge menn. I radikaliseringsprosessen til denne aldersgruppen ser vi at bruk av digitale plattformer ofte er særlig sentralt. Vi forventer at utviklingen og utfordringene ved at mindreårige blir radikalisert vil fortsette.

Selv om det i utgangspunktet er ulike årsaker til at personer deltar i høyreekstreme nettverk, kan gjentagende eksponering for dehumaniserende og ensidig tankegods føre til at det høyreekstreme budskapet får fotfeste. Vår erfaring er at en radikaliseringsprosess kan gå raskt. Bekymringen vår er at enkelte vil omsette høyreekstreme holdninger i høyreekstreme terrorhandlinger.

Høyreekstremisme fortsetter å inspirere til angrepsplanlegging i Vesten

Vår erfaring er at det er et mangfold av hendelser og drivkrefter som kan radikalisere og i ytterste konsekvens mobilisere høyreekstremister til å forsøke å begå terrorhandlinger. Det kan være samfunnsutvikling og dagsaktuelle hendelser på lokalt, nasjonalt og internasjonalt plan. I tillegg kan personlige forhold være mobiliserende. Hvilke samfunnshendelser som oppleves som drivkrefter for radikalisering og terrorplanlegging, er svært individuelt.

Det er imidlertid noen overordnede utviklingstrekk og hendelser som kan påvirke terrortrusselen fra høyreekstremisme i Norge. Dette er særlig utvikling som kan underbygge høyreekstremisters konspirasjonsteorier om at «den hvite rase» er truet. For mange høyreekstremister vil faktisk eller opplevd økt ikke-vestlig innvandring til Vesten være en slik mobiliserende faktor. Økt innvandring til Norge fra land i Midtøsten og Afrika som følge av pågående kriger og humanitære kriser er et slikt eksempel. For andre vil opplevelsen av at det norske samfunnet er i moralsk forfall være mobiliserende. For høyreekstremister kan dette være det norske samfunnets aksept for liberale kjønnsidentiteter og vedvarende normalisering av LHBT+-rettigheter.

Vi ser også at gjennomførte høyreekstreme terrorangrep fortsetter å være en viktig inspirasjonskilde og drivkraft for høyreekstremister. Dette gjelder både angrep som skjedde for flere år siden, og nye høyreekstreme terrorangrep. Sammenlignet med 2019 har det siden 2020 vært et lavere antall gjennomførte terrorangrep i Vesten. Men fremdeles avverges det et betydelig antall høyreekstreme angrep. At den største andelen av høyreekstreme terrorangrep i Vesten avverges, er med på å forhindre at nye gjennomførte terrorangrep inspirerer til ny terrorplanlegging. Samtidig viser dette at terrortrusselen fra høyreekstremister i Vesten og Norge er reell.

Av internasjonale hendelser har hverken krigen i Ukraina eller konflikter i Midtøsten ført til økt høyreekstrem radikalisering eller angrepsaktivitet. Årsaken er blant annet at krigene ikke har en tydelig ideologisk betydning for norske høyreekstremister. I Ukraina har imidlertid enkelte nordmenn med tilknytning til høyreekstremisme deltatt i krigen. Vi er fortsatt bekymret for at disse personene tilegner seg kunnskap og erfaring om angrepsmidler, får lavere voldsterskel, utvikler sine ekstremistiske kontaktnett og blir mer sårbare på grunn av krigstraumer.

Mål om massedrap på personer som inngår i fiendebildet

Et høyreekstremt terrorangrep i Norge vil mest sannsynlig være et masseskadeangrep eller et målrettet drap. Angrepet vil rettes mot personer, grupper eller institusjoner som inngår i det høyreekstreme fiendebildet. Vi forventer fremdeles at et høyreekstremt terrorangrep utføres av én gjerningsperson, og gjerningspersonen vil ofte være del av et høyreekstremt nettverk.

Fiendebildet til norske høyreekstremister vil fortsatt være mangfoldig, og omfatter personer med ikke-vestlig utseende, muslimer, jøder, ikke-vestlige innvandrere, politikere og representanter for norske myndigheter, LHBT+, tradisjonelle medier og venstreekstremister. Høyreekstremister anser disse for å true overlevelsen av den «hvite rase» eller «hvite kultur».

Valg av mål for et eventuelt terrorangrep vil kunne påvirkes av hvor tilgjengelig målet er, graden av symbolverdi og i hvilken grad et mål er omfattet av sikringstiltak. Angrepsmål med få eller ingen sikringstiltak og høy tetthet av personer de anser som fiender, vil gjerne foretrekkes av høyreekstremister. Dette er fordi høyreekstremister ofte har som målsetting å gjennomføre angrep med høye drapstall. Denne typen angrep er en av forutsetningene for å få en høy status i høyreekstreme kretser.

Ettersom massedrap ofte er et mål for høyreekstremister, vil skytevåpen og enkle improviserte eksplosive innretninger (IED-er) ofte foretrekkes av høyreekstremistiske gjerningspersoner. Samtidig påvirkes valg av angrepsmidler av blant annet aktørens målsetting, ferdigheter, nettverk og ikke minst hvor tilgjengelige angrepsmidlene er. Dette gjør at en rekke ulike angrepsmidler er aktuelle, blant annet kniv, hugg- og stikkvåpen, kjøretøy og brannstiftende midler.

Tilgang på ny teknologi kan også påvirke valg av angrepsmidler, eksempelvis ved bruk av droner eller 3D-printteknologi. Blant høyreekstremister ser vi blant annet at interessen for 3D-printede skytevåpen er økende. Det er imidlertid fremdeles krevende å lage funksjonelle og effektive 3D-printede skytevåpen med høy kapasitet. Vi forventer likevel at utviklingen innen, og tilgjengeligheten på, 3D-teknologi vil kunne bidra til at interessen for slike skytevåpen vil øke.

Trusselen mot myndighetspersoner i Norge

Myndighetspersoner er medlemmer av kongehuset, Stortinget, regjeringen og Høyesterett, samt representanter for tilsvarende organer i andre stater som oppholder seg i Norge.

Vi vurderer det som **lite sannsynlig** at noen vil forsøke å gjennomføre alvorlige voldelige handlinger mot myndighetspersoner i Norge i 2025. PST forventer at myndighetspersoner vil utsettes for hets, og i noen tilfeller trusler.

Vi venter mer hets og trusler når kontroversielle saker og politiske motsetninger får mye oppmerksomhet – spesielt i forbindelse med stortings- og sametingsvalget. Hets og trusler mot myndighetspersoner er en vedvarende utfordring for vårt demokrati.

Myndighetspersoner vil fortsatt være utsatte mål for fremmede staters etterretningsvirksomhet.

Økning i trusler og hets mot myndighetspersoner over tid

PST vurderer det som **lite sannsynlig** at noen vil forsøke å gjennomføre alvorlige voldelige handlinger mot myndighetspersoner i Norge i 2025. Vi forventer hets og trusler mot myndighetspersoner som får mye medieoppmerksomhet og knyttes til kontroversielle saker. Enkelte vil utsettes for konfrontasjoner som kan oppfattes truende.

Store mengder hets og trusler kan oppleves truende og legge begrensninger på hvordan enkelte myndighetspersoner vil utøve sitt demokratiske virke. Enkelte vil velge å moderere sine standpunkter, avstå fra å uttale seg eller trekke seg fra sine verv på grunn av belastningen. Derfor er trusler og hets mot myndighetspersoner en alvorlig utfordring for demokratiet.

Vi har over tid erfart en økning i omfanget av trusler mot norske myndighetspersoner. Antall personer som kommer med trusler, har også økt.

Selv om de færreste som fremsetter trusler, har en reell voldsintensjon, må vi ta høyde for at enkeltpersoner vil forsøke å gjøre alvor av truslene. Store mengder truende ytringer på nett kan dessuten bidra til å alminneliggjøre og legitimere vold mot myndighetspersoner. Dette kan påvirke og inspirere enkelte til å utføre voldelige handlinger.

I høst er det stortings- og sametingsvalg i Norge. PST forventer at myndighetspersoner vil motta mer hets og trusler når kontroversielle saker og politiske motsetninger får mer oppmerksomhet. Dette bildet er fra mars 2023, da stortingspresident Masud Gharahkhani møtte kvinnelige politikere som har opplevd hets og trusler.

F.v. Hanne Tollerud, Anita Ihle, Masud Gharahkhani og Lan Marie Berg. Foto: Javad Parsa / NTB

Posisjon og individuelle faktorer påvirker trusselen

Alle myndighetspersoner har et sammensatt og ulikt trusselbilde. Trusselen påvirkes av myndighetspersonens posisjon, individuelle faktorer, medieeksponering og i hvilken grad vedkommende assosieres med kontroversielle saker.

Regjeringsmedlemmer og partiledere vil være mer trusselutsatte enn mindre profilerte politikere på grunn av deres nasjonale saksansvar og synlighet i media. Tilhørighet til partier på ytterfløyene og minoritetsbakgrunn kan øke omfanget av hets og trusler. Kvinnelige myndighetspersoner vil oftere motta seksualiserte trusler enn menn.

Kontroversielle saker som knyttes til kongehuset, vil tidvis føre til mer uønsket oppmerksomhet, hets og potensielle trusler mot medlemmer av kongehuset.

Trusselbildet for utenlandske myndighetspersoner i Norge vil i større grad påvirkes av internasjonale forhold. Noen er mer utsatt for trusler på grunn av konflikter i hjemlandet. Et eksempel er den skjerpede trusselen mot israelske og jødiske mål i Norge som følge av krigføringen mellom Israel og Hamas i Gaza.

Trusselaktører motivert av personlige årsaker har sjelden reell voldsintensjon

Aktører motivert av personlige årsaker forventes å stå for den største andelen av hets og trusler mot myndighetspersoner. Disse vil primært være drevet av misnøye knyttet til egen livssituasjon eller av et spesielt saksforhold, og i enkelte tilfeller en fiksering på myndighetspersoner. Ofte vil det også være et betydelig innslag av sårbarhetsfaktorer, særlig psykisk uhelse og rusbruk. Den nasjonale kapasiteten til å håndtere personer med psykiatri- og rusutfordringer vil derfor ha innvirkning på omfanget av trusler mot myndighetspersoner.

Personlig motiverte aktører vil gjerne fremme trusler, hets og uønsket oppmerksomhet på internett eller via telefon. I 2024 ble for eksempel en person dømt for å ha fremsatt trusler om et væpnet «live-streamet» angrep mot Stortinget på Facebook.

Personlig oppmøte og konfrontasjoner kan også forekomme. Motivet vil sjelden være å skade en myndighetsperson, men snarere å oppnå endring eller hjelp til å bedre egen livssituasjon. Det kan også være å få utløp for frustrasjon eller sinne ved å henvende seg direkte til dem de anser som ansvarlige.

Myndighetspersoner i ekstremisters fiendebilde

Norske myndigheter vil fortsatt stå sentralt i fiendebildet til ekstremister. Ekstremisters forventninger om sikringstiltak rundt myndighetspersoner kan imidlertid bidra til at andre, lettere tilgjengelige mål blir valgt.

Høyreekstremister ser på myndighetene som landssvikere, og anklager dem for å legge til rette for utsletting av «den hvite rase». Samtlige politikere blir sett på som representanter for eliten og den korrupte staten. For norske høyreekstremister har den politiske venstresiden, og særlig Arbeiderpartiet, en sentral plass i disse konspirasjonsteoriene. Oppfattet tilrettelegging for ikke-vestlig innvandring og opplevde negative konsekvenser av innvandring vil fortsatt virke mobiliserende på myndighetshatet i høyreekstreme miljøer.

Ekstreme islamister forfekter et verdenssyn som går ut på at vestlige land undertrykker muslimer og er i krig med islam. Derfor vil ekstremister også kunne anse norske myndigheter som sine fiender. Per i dag fremstår imidlertid andre mål som mer fremtredende i Norge. Dette kan endres raskt, for eksempel dersom representanter for norske myndigheter oppfattes å krenke islam, støtte militær krigføring mot muslimer eller om Norge nevnes i offisielle terroroppfordringer fra terrororganisasjoner.

Myndighetspersoner kan utsettes for etterretningsvirksomhet og påvirkningsforsøk fra fremmede stater

Fremmede stater vil også i 2025 søke informasjon om norske politiske prosesser som kan påvirke deres interesser. Dette gjelder særlig Russland og Kina. Norske politikere, og personer som jobber i apparatet rundt disse, kan derfor være mål for fremmede staters etterretningsaktivitet.

Vi forventer at myndighetspersoner vil utsettes for cyberoperasjoner, særlig i form av phishing. Ofte initieres phishing-forsøk via epost, sosiale medier, SMS eller på andre kommunikasjonsplattformer. Formålet er å lure mottakeren til å laste ned skadevare eller oppgi innloggingsdetaljer som kan brukes til å kompromittere målet. Konsekvensen kan være at en fremmed statlig aktør får tilgang til myndighetspersonens private og profesjonelle korrespondanse, kalender og kontaktnettverk. Slik sensitiv informasjon kan potensielt benyttes i både etterretnings- og påvirkningsoperasjoner.

Myndighetspersoner har en symbolsk verdi i fremmede staters påvirkningsoperasjoner, fordi de representerer norsk politikk eller den norske opinionen. Statlige aktører kan forsøke å påvirke befolkningens tillit til politikere og politiske prosesser i Norge, for eksempel gjennom svertekampanjer eller desinformasjon. Påvirkning fra fremmede stater kan i ytterste konsekvens føre til økt polarisering og øke mengden trusler og hets mot politikere.

Trusler i forbindelse med stortings- og sametingsvalget 2025

Flere land i Europa registrerer en økning i antall truende handlinger og direkte angrep mot politikere, særlig i forbindelse med valg.

I perioden før, under og etter stortings- og sametingsvalget i 2025 vil landets politikere og sakene de fronter få betydelig mediedekning. Vi forventer mer hets og trusler når kontroversielle saker og politiske motsetninger får mye oppmerksomhet. Hyppige offentlige opptredener og annen valgkampaktivitet vil gjøre politikere mer tilgjengelige og dermed mer sårbare for konfrontasjoner.

Hvilke saker som bidrar til økt trusselaktivitet mot myndighetspersoner, vil påvirkes av økonomiske konjunkturer, internasjonale utviklingstrekk og politiske beslutninger. Det kan være saker som oppleves som begrensende på folks personlige økonomi og frihet, opplevd urettferdighet eller konflikter i møte med det offentlige. Saker der myndighetspersoner fremstilles i et negativt lys, kan også utløse myndighetsforakt, mistillit og konspirasjonstanker. Dette kan ha en negativ innvirkning på trusselen mot myndighetspersoner.

Politikere og andre mål knyttet til stortingsvalget kan potensielt utgjøre terrormål for ekstremister som har myndighetspersoner og politikere i sitt fiendebilde.

Enkelte statlige aktører kan også bruke perioden opp mot valget som en anledning til å påvirke politikere og befolkningen i en retning som tjener deres interesser.

Politiets sikkerhetstjeneste
pst.no