PST

Nasjonal risikovurdering (NRA) terrorfinansiering 2026

Dokumentdato: 24. juni 2026

Innhold

Sammendrag

Aktører som muliggjør terror utgjør en sentral trussel mot internasjonal fred og sikkerhet. Terrorfinansiering er et globalt, komplekst fenomen, som bidrar til å understøtte trusselen om terror. Terrortrusselbildet preges av den aktuelle situasjonen i verden, som gir ulike mulighetsrom for ekstreme aktører. Geopolitiske forhold og den teknologiske utviklingen i samfunnet skaper nye arenaer for finansiell understøttelse av terrorvirksomhet. Denne utviklingen gjør det mer krevende for rapporteringspliktige så vel som sikkerhetsmyndigheter å forebygge og forhindre terrorfinansiering.

Bidragene fra norske ekstremister til internasjonal terror er begrenset i omfang og størrelse, og norske aktører har generelt lav kapasitet til å skaffe til veie store midler. På nasjonalt nivå skjer finansieringen hovedsakelig gjennom enkeltaktører med små midler, ofte rettet mot enkeltpersoner og konkrete formål og sjelden mot organiserte nettverk.

Rapporten viser at terrorfinansiering kan foregå gjennom ulike kanaler og ved bruk av ulike verdier som kontanter, kryptoeiendeler, forhåndsbetalte kort, gull og luksusvarer, samt ved uregulert virksomhet og digitale plattformer. Banker, betalingstjenester, kryptotilbydere, innsamlingsvirksomhet og profesjonelle tilretteleggere kan være særlig utsatt for å bli utnyttet. Påvirkbare unge og mindreårige, selskaper med skjult eierskap og koblinger til kriminelle miljøer har også økt sårbarhet.

Overordnet vurderes den samlede risikoen for terrorfinansiering som MODERAT. Det faktiske omfanget synes begrenset, men sårbarheter og muligheten for misbruk tilsier at risikoen ikke kan anses som LAV. Risikoen for finansiering av terror i Norge vurderes som lavere enn risikoen for finansiering fra Norge til utlandet.

1. Bakgrunn

Aktører som muliggjør terror utgjør en sentral trussel mot internasjonal fred og sikkerhet. Terrorfinansiering er et globalt, komplekst fenomen, som bidrar til å understøtte denne trusselen. Et fellestrekk ved terrorfinansiering er utnyttelsen av internasjonale overføringssystemer til å finansiere terrorangrep eller terrororganisasjoners virksomhet.

Å forhindre terrorfinansiering bidrar til å redusere trusselen og til å bekjempe terror. Bekjempelse av terrorfinansiering har på denne bakgrunn vedvarende høy prioritet internasjonalt, i samsvar med prioriteringen i Financial Action Task Force (FATF), FN og EU.

> «*Terroraktivitet er en særlig alvorlig form for kriminalitet, fordi den truer borgernes grunnleggende trygghet og frihet. […] Klarer man å forebygge og forhindre tilførselen av midler til terroraktivitet, kan man også hindre terrorangrep*».
>
> - Regjeringens strategi for bekjempelse av hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen[1]
> (juni 2020)

Nasjonal risikovurdering (NRA) for terrorfinansiering skal i likhet med NRA for hvitvasking være et sentralt kunnskapsgrunnlag for å skape en felles forståelse av risikoen for terrorfinansiering i Norge. Formålet med vurderingen er å bidra til en risikobasert tilnærming til arbeidet med å bekjempe terrorfinansiering.

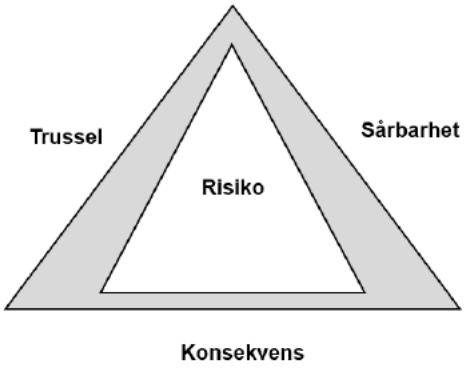
2. Metode og datagrunnlag

Utarbeidelsen av NRA 2026 er et oppdrag Justisdepartementet har gitt Politidirektoratet og Politiets sikkerhetstjeneste (PST). Økokrim har fått ansvar for å utarbeide hvitvaskingsdelen av den nasjonale risikovurderingen, mens PST har ansvar for delen om terrorfinansiering. Selv om NRA 2026 publiseres som to separate rapporter, må de ses i sammenheng. Flere momenter som knyttes til hvitvasking vil

[1] Regjeringen.no, *Regjeringens strategi for bekjempelse av hvitvasking, terrorfinansiering og finansiering av spredning av masseødeleggelsesvåpen*, juni 2020.

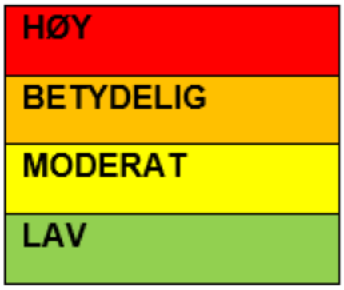
også være aktuelle å ta hensyn til når det gjelder terrorfinansiering, selv om de ikke nevnes eksplisitt her.

Metoden er basert på en analyse og vurdering av de tre elementene trussel, sårbarhet og konsekvens, som utledet av FATF.[2] Det er gjort enkelte tilpasninger for å ta høyde for forskjellene mellom hvitvasking og terrorfinansiering, samt særlige forhold knyttet til Norge. Rapporten vil eksempelvis i liten grad peke på geografiske risikomomenter. Disse risikoene er dynamiske og må forstås ut fra verdistrømmene[3] til de individuelle personene som ønsker å finansiere terror.



Figur 1: ØKOKRIM - modell for risikovurdering

Risikovurderingen søker å belyse hvilke aktiviteter som anses å innebære en risiko for terrorfinansiering. Det benyttes en firedelt skala for vurdering av risikonivå: lav, moderat, betydelig og høy.



Figur 2: Vurderingskala med fargekoder

I likhet med NRA for hvitvasking, vil PSTs vurdering bygge videre på NRA 2022 og dermed avgrenses til å gi et situasjonsbilde over de mest aktuelle og mest fremtredende risikoene. Vurderingen er derfor ikke uttømmende for risikoer det kan være aktuelt å ta hensyn til, men den rettes mot de områder som basert på nåværende kunnskapsgrunnlag er identifisert av PST gjennom referanseperioden 2022-2026.

[2] Metoden er nærmere beskrevet i NRA 2026 for hvitvasking, utarbeidet av Økokrim, samt ytterligere beskrevet i «FATF Terrorist Financing Risk Assessment Guide».
[3] En verdistrøm i terrorfinansieringssammenheng er forflytningen av økonomisk verdi fra en kilde til et formål, enten verdien flyttes som penger, varer, tjenester eller andre aktiva.

PSTs data- og informasjonsgrunnlag baserer seg blant annet på tilgjengeliggjort informasjon fra egen innhenting, eksternt fagmiljø og offentlige etater. Informasjonen som fremsettes i rapporten er dessuten påvirket av at deler av kunnskapsgrunnlaget er sikkerhetsgradert. Ytterligere sårbarheter er beskrevet i kapittel 8.

Terrorfinansiering tar ikke hensyn til landegrenser, og på bakgrunn av datagrunnlaget vil det være tilfeller hvor denne rapporten beskriver fenomener og modus som ikke er blitt direkte observert av PST i Norge. Disse vurderes likevel å være relevante og innenfor mulighetene for terrorfinansiering i og fra Norge. PST har de siste årene sett en økning i informasjonstilfanget knyttet til terrorfinansiering. Det har i rapporteringsperioden vært en jevn økning i rapporteringen om mistenkt terrorfinansiering fra publikum så vel som fra nasjonale og internasjonale samarbeidspartnere. Selv om det totale kildegrunnlaget kan anses som begrenset, underbygger økningen et forsterket fokus hos de rapporteringspliktige[4] så vel som hos myndighetene. Økt informasjonstilgang vil på sikt være en positiv bidragsyter til arbeidet med å bekjempe terrorfinansiering.

PSTs mandat og definisjoner

PSTs oppgaver og ansvar knyttet til terrorfinansiering fremgår av politiloven § 17 b. PST skal forebygge og etterforske blant annet overtredelser av straffeloven § 135 og 136 a. Videre fremgår det av politiloven § 17 g at sjef PST kan beslutte å båndlegge midler, dersom det er god grunn til å tro at noen har forsøkt eller antas å ha begått en nærmere angitt terrorhandling.

Med ***terrorfinansiering*** menes begrepet slik det er definert i straffeloven § 135. § 136a rammer også terrorfinansiering. Begrepet terrorfinansiering omfatter en lang rekke handlinger.

Med ***sannsynlighet*** menes et sett med standardiserte sannsynlighetsord som benyttes av PST[5]. Formålet med disse er å skape en mer ensartet beskrivelse av sannsynligheten i vurderingene og derigjennom redusere uklarhet og misforståelser.

[4] Advokater, banker, regnskapsførere, eiendomsmeglere og andre aktører defineres gjennomgående i denne risikovurderingen som «rapporteringspliktige». Med rapporteringspliktige menes aktører som er underlagt hvitvaskingsloven og som er pålagt å rapportere mistenkelige transaksjoner til Økokrim.
[5] Se beskrivelse av sannsynlighetsord i Nasjonal trusselvurdering 2026 (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)

Med ***terrortrussel*** menes terrortrusselsituasjonen. Mens sannsynlighetsordene representerer PSTs vurdering av sannsynligheten for at det vil skje forsøk på en terrorhandling, er terrortrusselen et uttrykk for graden av alvorlighet i situasjonen.[6]

Med ***ekstremisme*** menes aksept for eller støtte til bruk av vold for å nå politiske, religiøse eller ideologiske mål.[7]

Med ***sårbarhet*** menes de faktorene som kan utnyttes av trusselen, eller som kan støtte eller legge til rette for slik virksomhet. Sårbarheter kan omfatte trekk ved en bestemt sektor, et finansielt produkt eller en type tjeneste som gjør dem attraktive for terrorfinansiering. Sårbarheter kan også omfatte svakheter i tiltak som er spesielt rettet mot terrorfinansiering, eller særegenheter ved en jurisdiksjon som kan påvirke mulighetene til å skaffe eller flytte midler, eksempelvis en stor uformell økonomi eller manglende grensekontroll.[8]

Med ***konsekvens*** menes den skade eller påvirkning en terrorfinansiering kan føre til dersom den materialiserer seg. Dette omfatter både virkninger for finansielle systemer og institusjoner, samt videre konsekvenser for økonomi, samfunn og nasjonale interesser. Konsekvensene av terrorfinansiering vil normalt kunne anses som mer alvorlige enn ved hvitvasking og annen økonomisk kriminalitet.[9]

3. Overordnet situasjonsbilde

Trusselbilde terrorfinansiering

Organisert terrorvirksomhet krever ofte grenseoverskridende finansiering. Terrortrusselbildet preges av en rekke aktuelle forhold som skaper ulike muligheter. Enkelte av disse er blant annet fremhevet i PSTs trusselvurdering (NTV).

Geopolitisk uro gir rom for økt terrorfinansieringsaktivitet

[6] PST, *Nasjonal trusselvurdering 2026* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)
[7] PST, *Nasjonal trusselvurdering 2026* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)
[8] FATF, *Terrorist Financing Risk Assessment Guidance*, 2019
[9] FATF, *Terrorist Financing Risk Assessment Guidance*, 2019

Geopolitisk uro, usikkerhet og destabilisering bidrar ofte til maktvakuum, svekkede statlige institusjoner og forsterkede sosiale spenninger. Slike forhold gir grobunn for opprørsgrupper, ikke-statlige væpnede aktører og voldelige ekstremister.

Flere regioner preges i dag av stormaktsrivalisering, uthuling av internasjonale normer og voksende ustabilitet. Konfliktene i Midtøsten og Afrika gir handlingsrom som terrorgrupper har utnyttet til å radikalisere og rekruttere, samt til å øke sin angreps- og finansieringsaktivitet både lokalt og i Vesten. Økonomisk og sosial uro i disse områdene gjør det lettere å rekruttere medlemmer til terrorvirksomhet, inkludert finansiell støttevirksomhet, og til å samle inn penger/midler fra befolkning og ressurser i områder de kontrollerer. Stormaktsrivalisering og stedfortrederkonflikter kan videre føre til ulike fraksjoner hvor opprørsgrupper kan få tilgang til ressurser og legitimitet de ellers ikke ville hatt. Kamp om naturressurser kan også øke terroraktørers handlingsrom ved at nød og ressursmangel skaper en desperat situasjon, som terrorgrupper utnytter til rekruttering, maktovertakelse og strategisk kontroll over ressurser.

Samtidig fører konflikter og humanitære kriser ofte til økt bruk av kontanter og uformelle pengeoverføringstjenester, noe som gjør pengestrømmer vanskeligere å spore. Geopolitisk uro kan også bidra til at bistand, veldedige innsamlinger og diasporaoverføringer misbrukes, mens digitale plattformer og sosiale medier gjør det enklere å samle inn støtte på tvers av landegrenser.

I tillegg kan sanksjoner, handelsforstyrrelser og internasjonal splittelse skape flere gråsoner, der ulovlige nettverk får større handlingsrom. Til sammen betyr dette at geopolitisk uro ikke bare øker risikoen for terror, men også styrker de økonomiske strukturene som gjør terrorvirksomhet mulig.

Gråsonevirksomhet problematiserer trusselbildet

Trusselbildet er videre preget av flere aktører med ulik motivasjon som i større grad synes å operere sammen, slik som statlige aktører, terrorgrupper og aktører som driver organisert kriminalitet[10]. Denne utviklingen visker ut tradisjonelle skillelinjer mellom ulike typer kriminalitet. I likhet med FATF og Europols observasjoner, erfarer vi også i Norge at flere ekstremister har tilknytning til statlige aktører, kriminelle nettverk og miljøer som driver annen organisert kriminalitet, inkludert hvitvasking og

[10] PST, *Nasjonal trusselvurdering 2026* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)

ulike primærforbrytelser. Dette bidrar til å gjøre trusselbildet mer uoversiktlig og komplekst, ettersom det kan være vanskelig å skille terrorfinansiering fra annen kriminalitet.

Det observeres en økende bruk av mellomledd, som har som mål å skjule overføringer eller omgå juridiske begrensninger. Dette gjør det mer krevende å avdekke både potensielle terrorhandlinger og terrorfinansiering, og bevise at finansiering av handlinger er gjort med forsett.

Bruk av kunstig intelligens skaper muligheter

Digital innovasjon og nye teknologiske løsninger for verdioverføringer, samt bruk av kunstig intelligens (KI), har videre bidratt til at dagens transaksjonsstrømmer er blitt mer komplekse. Dette har igjen utvidet trusselaktørenes muligheter til å opptre i det skjulte, særlig der transaksjoner beveger seg raskt og fragmentert over ulike finansielle systemer og landegrenser.

Europol fremhever at KI og andre nye teknologier skaper muligheter, ved at terrorfinansiering blir billigere, raskere og mer tilpasningsdyktig. KI kan også få ulovlige verdistrømmer til å fremstå som troverdige, dette gjelder falske identiteter, manipulerte dokumenter og misbruk av virtuelle eiendeler, samt bedre forfalsket dokumentasjon, tilsløring av avsendere og mottakere og sofistikerte betalingsinstrukser.[11]

KI senker videre terskelen for digital påvirkning og sosial manipulering. Det øker risikoen for mer målrettet innhold, billigere produksjon av propaganda og mer effektiv mobilisering av eventuelle støttespillere.[12] Slik kommunikasjon øker også risikoen for terrorfinansiering, eksempelvis ved oppfordring til pengeoverføringer i digitale fora.

De ovennevnte forholdene anses å kunne øke risikoen for at terrorfinansiering i og fra Norge vil kunne skje.

[11] FATF, *Horizon Scan: Artificial Intelligence and Deepfakes,* 2025.
[12] Europol, *European Union Terrorism Situation and Trend Report,* Publications Office of the European Union, Luxembourg, 2025.

Drivere for terrorfinansiering

Utviklingen globalt viser en tydelig geografisk og operativ forskyvning av terrorangrepene. Internasjonale analyser, blant annet fra Europol og IEP[13], peker på at de mest dødelige terrorvirksomhetene i økende grad er konsentrert til Sahel-regionen og deler av Sør-Asia, mens Europa og andre vestlige land i større grad preges av et fragmentert og mindre forutsigbart trusselbilde. I vestlige land er det særlig en økning i trusler fra enslige aktører og små, løst organiserte nettverk, ofte drevet av rask digital radikalisering gjennom lukkede nettfora og sosiale medier.

Samlet peker utviklingen på at den sentraliserte kapasiteten til tradisjonelle terrororganisasjoner flere steder er svekket, samtidig som trusselbildet i Europa og andre vestlige land er blitt mer desentralisert, digitalisert og krevende å avdekke på et tidlig stadium. Et mer fragmentert trusselbilde innebærer videre at finansiering i større grad kan skje gjennom små og mindre synlige overføringer, ofte ved hjelp av digitaliserte tjenester, kryptovaluta og grensekryssende overføringer.[14]

Terrorvirksomheten i Europa har de siste par årene vært høyere enn på mange år. De fleste angrepsplanene blir imidlertid avverget av sikkerhets- og etterretningstjenester. Ekstreme islamisters angrepsvirksomhet i Europa har økt markant etter Hamas' terrorangrep 7. oktober 2023 og Israels påfølgende militæroperasjon i Gaza. Den høye angrepsvirksomhet fortsatte i 2025 og forventes å vedvare i 2026. Den høyreekstreme angrepsvirksomheten i Europa har ligget på et stabilt nivå siden 2020.

Europol rapporterte at 449 personer ble arrestert for terrorisme-relaterte lovbrudd i Europa i 2024, som er en økning fra både 2023 og 2022. Den største andelen av arrestasjonene knytter seg til ekstrem islamisme (289), etterfulgt av høyreekstremisme (47).[15] Europols årlige TE-SAT-rapporter viser imidlertid at ekstremisme i Europa i økende grad kjennetegnes av hybride og ideologisk sammensatte virkemidler, der tradisjonelle skillelinjer mellom jihadistisk, høyreekstrem og annen ekstremisme blir mindre tydelige. Europol fremhever også en bekymringsfull økning i antall mindreårige involvert i terrorrelaterte saker, samt

[13] Institute for Economics & Peace, *Global Terrorism Index 2026: Measuring the impact of terrorism*, 2026
[14] For mer informasjon knyttet til utviklingstrekk og indikatorer vises det blant annet til JRC Indicators Explorer, utviklet at EU-kommisjonens Joint Research Centre, som sammenstiller informasjon fra en rekke kilder, herunder Global Terrorism Index.
[15] Europol, *European Union Terrorism Situation and Trend Report,* Publications Office of the European Union, Luxembourg, 2025.

hvordan digitale plattformer og krypterte kommunikasjonstjenester benyttes til propaganda, rekruttering og operativ planlegging. Problemstillinger tilknyttet mindreårige vil bli tatt opp senere i dette dokumentet.

I henhold til Nasjonal trusselvurdering 2026 vurderes terrortrusselnivået i Norge som MODERAT. Det betyr at etter PSTs vurdering har en eller flere personer en intensjon om å gjennomføre terrorangrep, men uten å ha tatt konkrete skritt eller ha realistiske planer, og/eller uten at noen forhold forsterker trusselen. Terrortrusselnivået er et uttrykk for den samlede trusselen fra alle typer ideologisk, politisk og religiøst motivert vold.

PST vurderer det som mulig at både ekstreme islamister og høyreekstreme fortsatt vil forsøke å gjennomføre terrorangrep i Norge i 2026, og disse vurderes å utgjøre den mest alvorlige terrortrusselen mot Norge.[16]

Alle trusselvurderinger er beheftet med usikkerhet, og trusselbildet påvirkes av flere faktorer. PSTs nasjonale trusselvurdering beskriver at selv om vi har et MODERAT terrortrusselnivå, er terrortrusselbildet mer komplekst og uforutsigbart enn tidligere, og skjerpet når det gjelder noen spesifikke trusselutsatte grupper.

Uforutsigbarhet og usikkerhet globalt, knyttet til potensielle enkelthendelser og mer langsiktige negative utviklingstrekk, fører også til raske endringer i situasjonsbildet. Som beskrevet i NTV 2026, er flere andre ekstremismeretninger blitt aktuelle, for eksempel antistatlig ekstremisme. PST er kjent med at det har vært tilfeller av terrorfinansiering knyttet til disse ekstremismeretningene i flere land, også europeiske.

Oppmerksomheten bør derfor rettes mot risikoen for terrorfinansiering innenfor de ulike ekstremismeretningene, også i Norge.

Omfanget av terrorfinansiering i og fra Norge

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

[16] PST, *Nasjonal trusselvurdering 2026* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)

norske myndigheter. I tillegg vil betalingstjenestene være i stadig endring. Vi forventer at denne utviklingen vil fortsette.»

- *Nasjonal trusselvurdering 2026 (PST)*

Trusselen fra ekstreme islamister vedvarer, til tross for at det fortsatt er identifisert få personer i Norge som støtter ekstrem islamisme. Tidligere etablerte grupper er lite aktive, men vi har få indikasjoner på at veletablerte ekstremister er blitt avradikalisert.[17]

I Norge er det få tydelig 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. Flere personer i Norge har også forbindelser til europeiske og andre internasjonale ekstreme islamistiske nettverk. Slike nettverk kan potensielt be personer i Norge om å tilrettelegge for eller utføre terror og således utgjøre en risiko for terrorfinansiering.[18]

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. Parallelt med de fysiske gruppene er det en rekke digitale arenaer der norske høyreekstreme deler ideologi og propaganda.[19] Fravær av etablerte høyreekstreme terrororganisasjoner vil likevel begrense høyreekstremisters evne til å planlegge, finansiere og koordinere komplekse angrep.[20]

På tross av det ovennevnte er PST gjennom referanseperioden blitt gjort kjent med tilfeller hvor det er blitt overført midler for å finansiere terror, både i og utenfor Norge. Basert på nåværende informasjonsgrunnlag vurderes terrorfinansiering å utgjøre en liten andel av den totale norske økonomien, både i antall transaksjoner og beløp. [21]

Transaksjonsdata PST besitter viser at midler i hovedsak tilflyter terrorgrupper i utlandet, slik som IS, al-Qaida, Hizbollah og al-Shabaab. Beløpene har vært av

[17] PST, *Nasjonal trusselvurdering 2026* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)
[18] PST, *Nasjonal trusselvurdering 2026* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)
[19] PST, *Nasjonal trusselvurdering 2026* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)
[20] Etterretningstjenesten, *Fokus*, 2026
[21] Økokrim, *Nasjonal risikovurdering*, 2026

beskjeden størrelse, og transaksjonene er spredt over lengre tidsperioder. Det er også observert en splitting av transaksjoner mellom ulike tjenestetilbydere, samt bruk av mellomledd i andre europeiske land.

PST erfarer at det gjerne er personer tilknyttet utenlandske terrororganisasjoner som mottar den største andelen av finansieringen fra Norge. Overføringene gjennomføres gjerne via tilretteleggere, som arbeider på tvers av europeiske land, og som deretter videreformidler midlene til andre ekstremistiske tilretteleggere i nærheten av terrororganisasjonenes hovedseter.

Basert på nåværende datagrunnlag erfarer PST at midler eller verdier som benyttes til terrorfinansiering ofte stammer fra legitime inntektskilder. Norske ekstremister er, på lik linje med ekstremister i andre europeiske land, i stor grad selvfinansierte og bruker egne midler til å betale reise, klær og utstyr i forkant av eventuelle utreiser til konfliktområder eller i forbindelse med angrepsvirksomhet i Norge.[22] Egne midler inkluderer også salg av egne eiendeler og verdigjenstander og penger fra familie eller låneopptak.

De siste årene er det blitt observert et lite antall ekstremister som har selvfinansiert relativt komplekse angrep, hovedsakelig i utlandet, men også i Norge. Denne selvfinansieringen og bruken av ressurser kan foregå over flere år. Nasjonale eksempler er Anders Behring Breivik, som brukte flere år på innkjøp av kapasitetsforbedrende materiell som kjemikalier, våpendeler og ammunisjon. Anskaffelsen av det nevnte materiellet krevde ikke noen betydelig kapital, og innkjøpene var spredt over flere år. Et annet eksempel er Arfan Bhattis bistand til Zaniar Matapour i planleggingen av terrorangrepet 25. juni 2022, hvor Bhatti bl.a. bidro med å skaffe Matapour våpen.

PST fremhever at mulighetene fremstår som flere enn det tjenesten så langt har observert faktisk gjennomføres, både nasjonalt og utenfor Norge. På grunnlag av identifiserte sårbarheter er det derfor en risiko for at det foreligger mørketall for omfanget av terrorfinansiering i og utenfor Norge, og når det gjelder i hvilken grad Norge benyttes som et «transittland» for overføringer knyttet til terrorfinansiering.

Etter PSTs vurdering er imidlertid risikoen størst knyttet til finansiering av terror fra Norge til utlandet. Dette har videre sammenheng med informasjonsgrunnlaget PST besitter om det nasjonale trusselbildet.

[22] Europol, *European Union Terrorism Situation and Trend Report*, Publications Office of the European Union, Luxembourg, 2025.

4. Utvalgte indikatorer og fremgangsmåter for terrorfinansiering

Denne delen fremhever utvalgte indikatorer og fremgangsmåter basert på PSTs erfaringer i referanseperioden. Utvalget er gjort på bakgrunn av en gjennomgang av PSTs informasjonsgrunnlag og observasjoner og er ikke uttømmende. Kapittelet er kun ment å peke på indikatorer og fremgangsmåter som det bør rettes særlig oppmerksomhet mot i dagens situasjonsbilde.

Ekstreme holdninger og tilknytning til ekstreme miljøer

Utvikling av ekstreme holdninger anses å øke risikoen for å gi støtte til terror. Ytterliggående tankesett eller radikalisering, hvor en person gradvis endrer sine holdninger og i økende grad aksepterer eller legitimerer bruk av vold, er derfor forbundet med økt risiko for at vedkommende vil støtte terrorhandlinger.

PST erfarer at personer med slike holdninger også ofte knytter seg til ekstreme nettverk, både nasjonalt og internasjonalt. PST har sett at støtte til terror ofte kanaliseres via disse nettverkene og ikke direkte til eventuelle terrorgrupper eller land hvor slike opererer.

Mottakere av offentlig støtte

Vi har observert en risiko for at personer med ekstreme holdninger, som samtidig mottar offentlige ytelser, senere benytter disse midlene til terrorfinansiering.

I flere saker har PST også erfart at personer som har misbrukt trygdeordninger ved å motta urettmessig støtte i form av statlige lån, barnebidrag, dagpenger, arbeidsavklaringspenger osv., har en høyere risiko for å benytte disse inntektene til å finansiere terror i utlandet. Dette erfares også andre steder i Europa, og FATFs medlemsland rapporterer en økende evne blant ekstremister til skatteunndragelse for å maksimere utbetalingen av sosiale stønader.[23]

[23] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

Tilknytning til kriminelle nettverk

FATF har gjennom flere år påpekt koblinger mellom kriminelle nettverk og terrorfinansiering. Disse nettverkene har blant annet støttet terrorgrupper på flere måter, eksempelvis ved å fremskaffe midler til våpen og annet utstyr, falske reise- og deklareringsdokumenter eller annet som bidrar til å øke terroristenes handlingsrom.[24]

PST erfarer at norske ekstremister til en viss grad utnytter samfunnets sårbarheter og engasjerer seg i kriminell virksomhet for å skaffe inntekter til ulike formål, også terrorfinansiering.

PST erfarer at ekstremister med risiko for å involvere seg i terrorfinansiering ofte har nær tilknytning til kriminelle personer og miljøer, som begår en rekke primærlovbrudd for å generere økonomisk utbytte, eksempelvis bedragerier. Aktuelle modus inkluderer bruk av mellommenn for å få innvilget lån, hvor pengene umiddelbart etterpå spres på ulike konti for å tilsløre pengestrømmen.

Internasjonale kilder bemerker at høyreekstreme i mindre grad deltar i innbringende kriminalitet sammenlignet med ekstreme islamister. PST har ikke nærmere informasjon om omfanget av ulike kriminelle handlinger fordelt på ekstremismeretninger i Norge, men det samme synes å gjelde her.

En tettere sammenblanding mellom kriminelle nettverk og ekstremister kan øke risikoen for terrorfinansiering, både med og uten hensikt. En slik sammenblanding gir ekstremister tilgang til etablerte inntektskilder, logistikk og mekanismer for å skjule midler fra organisert kriminalitet. Gjennom koblinger til smugling, narkotika, våpenhandel, utpressing og andre illegale markeder, kan terrorgrupper lettere skaffe midler, flytte verdier og skjule aktivitet i allerede etablerte kriminelle strukturer. FATF fremhever at sammenfallet mellom terrorfinansiering og organisert kriminalitet er en tydelig risikoutvikling. I tillegg påpeker Europol hvordan enkelte ekstremistmiljøer kombinerer lovlige og ulovlige inntektskilder, inkludert koblinger til organisert kriminalitet, noe som gjør finansieringen mer robust, diversifisert og vanskeligere å avdekke.

[24] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

Unge og mindreårige

«Utfordringen med mindreårige og unge voksne som radikaliseres, forventes å fortsette i 2026»

- *Nasjonal trusselvurdering 2026 (PST)*

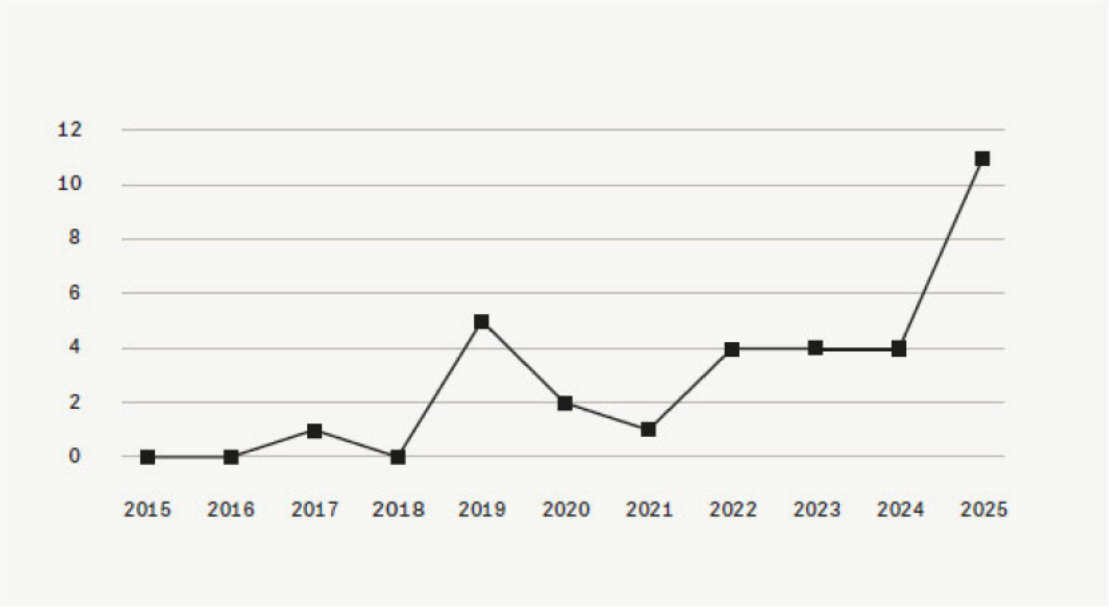
Radikalisering av unge og mindreårige er en økende bekymring i Norge. Psykisk uhelse og utenforskap er eksempler på særlige sårbarhetsfaktorer. Stadig flere barn og unge involverer seg i ekstremistiske miljøer og særlig gjennom digitale kanaler. Trusselbildet kompliseres ytterligere av at ideologi og voldsfascinasjon blandes sammen på en måte som gjør det vanskeligere å avdekke potensielle terrorhandlinger.[25]

Mindreårige utgjør en sårbar gruppe, særlig i det digitale rom hvor propaganda, sosial tilhørighet og økonomisk støtte lettere glir over i hverandre, noe som blir ytterligere forsterket av kunstig intelligens (KI). I et slikt miljø kan også terskelen for pengeinnsamling, mikrodonasjoner og annen finansiell støtte senkes og kamufleres som digital deltakelse.[26]

Europol rapporterer at antall mindreårige og unge som er involvert i terror og voldelig ekstremisme fortsetter å øke. Samme rapport viser også til hvordan ekstremister generelt tilpasser innholdet på plattformene de unge benytter og bruker algoritmestyrt innhold og spill til rekruttering og radikalisering.[27]

Økende bruk av kunstig intelligens gjør også mindreårige sårbare for påvirkning, rekruttering og digital mobilisering gjennom mer presis, personlig og kontinuerlig eksponering. I praksis betyr dette at KI ikke bare kan gjøre det lettere å påvirke de unge, men også lettere å bruke dem som givere, formidlere eller lavprofilerte mellomledd i små, digitale og tilslørte transaksjonsstrømmer.

[25] PST, *Nasjonal trusselvurdering 2026,* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)
[26] Europol, *European Union Terrorism Situation and Trend Report,* Publications Office of the European Union, Luxembourg, 2025.
[27] Europol, *European Union Terrorism Situation and Trend Report,* Publications Office of the European Union, Luxembourg, 2025.



Figur 3: Utviklingen i høyreekstrem angrepsaktivitet i Vesten der mindreårige har vært involvert i perioden 2015-2025 (Kilde: PST)

I likhet med politiet for øvrig opplever PST at mindreårige oftere er involvert i kriminalitet enn tidligere. Utviklingen sammenfaller med trenden som er rapportert av Økokrims Financial Intelligence Unit (FIU) om at gjennomsnittlig alder på person involvert i mistenkelige forhold (MF-rapporter med terrorfinansieringsmistanke) stadig blir lavere.[28]

PST opplever at terrorfinansiering knyttet til mindreårige er særlig utfordrende å avdekke, fordi de mindreårige ofte inngår i saker der finansielle spor er svake, indirekte eller skjult bak voksne personer og digitale mellomledd. Dette sammenfaller med det som blant annet er påpekt av FATF, om at når yngre personer blir involvert i terrorrelatert virksomhet, kan inntekter, kontoer og transaksjoner i mindre grad stå i deres eget navn, noe som gjør det vanskeligere å oppdage mønstre og gripe inn tidlig.

Selv om sikkerhets- og etterretningstjenestene avverger en stor andel angrep, oppleves det fortsatt utfordrende å avdekke soloaktørers planer.[29] Radikalisering av mindreårige og unge voksne forblir dermed en utfordring, både for offentlige

[28] Økokrim, *Financial Intelligence Unit Årsrapport*, 2025
[29] PST, *Nasjonal trusselvurdering 2026,* (https://www.pst.no/trusselbilde/norsk-trusselvurdering/nasjonal-trusselvurdering-2026/)

myndigheter og rapporteringspliktige. PST har derfor grunn til å anta at det foreligger mørketall.

Skjult eierskap og reelle rettighetshavere

Ekstremister observeres i økende grad å tilegne seg kunnskap om hvordan legale strukturer, slik som ulike bedrifter, foreninger og stiftelser, kan benyttes til å generere midler eller skjule at disse skal gå til terrorfinansiering.

PST har sett tilfeller der mer kompliserte selskapsstrukturer er benyttet for å tilsløre transaksjoner og mottakere, og til å skjule eiere og reelle rettighetshavere. Selskapsstrukturene er ofte grensekryssende og involverer skatteparadiser, land med svakere etterlevelse av internasjonale standarder og regelverk, bruk av stråpersoner og -selskaper, samt uoversiktlige, fragmenterte eller lite transparente forsynings- eller verdikjeder.

Blant annet anses eiendom som egnet til å tilsløre bakenforliggende eierskap og reelle rettighetshavere, gjennom komplekse eierstrukturer og mulighet for bruk av blanko-skjøter.

Likeså kan investeringer i verdipapirer, fond, selskaper eller opprettelse av selskapsstrukturer via forvaltningssteder med mindre kontroll og transparens benyttes til å skjule reelle investorer og dermed generere tilsynelatende legitime inntekter for tilslørte formål.

Utnyttelse av virksomhetsstrukturer

Ekstremister observeres i større grad å være knyttet til annen profittgenererende kriminalitet, som igjen er egnet til å generere midler for terrorfinansiering. Det vises for øvrig til avsnittet om bruk av kontanter under kapittel 5, samt kapittelet «Utnyttelse av virksomhetsstrukturer» i Økokrims NRA.

Bransjer med risiko for betydelig kontantgenererende virksomhet, slik som bygg- og anlegg, varehandel osv., anses særlig egnet, basert på den høye risikoen for utnyttelse til kriminalitet, som i neste omgang kan inngå i terrorfinansiering. Hvor egnet bransjen er, har blant annet sammenheng med virksomhetens kompleksitet, mulighet for «svart arbeid» og underslag som kan generere store kontantstrømmer og

bruk av eksempelvis underleverandører eller komplekse verdikjeder, samt geografisk eksponering på tvers av landegrenser.

Særlig om eksport av varer og tjenester

Anskaffelse av varer og tjenester, inkludert teknologi, våpen og annet utstyr, er en forutsetning for at terrorgrupper skal kunne fortsette å operere. Vi har sett at terrorgrupper tilegner seg både informasjon, midler og nødvendig utstyr ved å skjule støtte til sin aktivitet ved å utnytte virksomheter som kan knyttes til eksport av varer og tjenester. Dette kan eksempelvis skje gjennom:

- bruk av frontselskaper og stråpersoner for å skjule formål
- over- og underfakturering i forbindelse med handel
- fiktiv eksport
- handel med såkalte «flerbruksvarer[30]»
- omdirigering av varer via jurisdiksjoner med svakere kontroll og svakere etterlevelse av regelverket

Sjøfart, shipping, fiskeri og andre eksportaktører er blant industriene som anses egnet til å skjule både transaksjoner og andre verdier som kan gå til terrorfinansiering. Sjøfart og shipping innebærer ofte svært kompliserte handelsmønstre og verdikjeder. Aktørene preges dessuten av kompliserte eierstrukturer, etableringer i jurisdiksjoner med lav grad av statlig styring, samt virksomhet som går ut på at verdier transporteres, også til områder med høyere risiko.

Det er også kjent at terrororganisasjonen IS historisk har oppnådd betydelige inntekter fra produksjon og handel med olje og gass. Terrororganisasjonen al-Qaida forsøker fortsatt aktivt å etablere kontroll over havner langs Adenbukta. Den jemenittiske Houthi-bevegelsen har også forsøkt å ta kontroll over viktige olje- og gassfelt.[31]

De ovennevnte terrororganisasjonene er avhengige av samarbeidspartnere for å selge og frakte varene, for eksempel logistikkselskaper og mellommenn. Norge er et land med en stor sektor innenfor olje, gass og tilknyttet logistikk. Til tross for at olje- og gassindustrien på norsk sokkel er strengt regulert, er det likevel en risiko for at

[30] Flerbruksvarer er ordinære, sivile varer, teknologier eller tjenester som opprinnelig er utviklet for kommersielle formål, men som også har egenskaper som gjør at de kan brukes til militære formål.
[31] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

norske aktører, enten direkte eller indirekte, eksponeres for pengestrømmer som benyttes til terrorfinansiering.

Særlig om sanksjonsomgåelser og risiko for terrorfinansiering

Sanksjoner fra FN eller restriktive tiltak iverksatt av EU er i mange tilfeller rettet mot terrororganisasjoner, tilknyttede enkeltpersoner, eller stater som støtter slike organisasjoner. Omgåelse av sanksjoner innebærer derfor en risiko for at midler flyttes til aktører som utfører terror. Vi ser at metodene som benyttes for å omgå sanksjoner ofte sammenfaller med metodene som benyttes for å skjule at midler skal gå til terrorfinansiering, slik som bruk av komplekse selskapsstrukturer, bruk av mellomledd og komplekse verdikjeder. Medvirkning til sanksjonsomgåelser kan dermed også i praksis risikere å være medvirkning til terrorfinansiering.

Veldedige organisasjoner

Frivillige organisasjoner (NPO) overfører betydelige beløp fra Norge til utenlandske organisasjoner og virksomheter hvert eneste år. Selv om mange bidrag er ment for humanitære formål, kan enkelte giveres intensjon bli manipulert, og midlene i praksis kanaliseres til kriminell virksomhet, inkludert finansiering av terrorisme.

Terrornettverk utnytter ofte veldedige organisasjoner eller oppretter falske organisasjoner for å samle inn penger under dekke av eksempelvis humanitære formål, som tidligere sett ved blant annet *Holy Land Foundation* og *Global Relief Foundation*, som begge bedrev terrorfinansiering og ble stengt ned i kjølvannet av angrepet i New York i 2001. Det er også kjent at terrorister i enkelte tilfeller har benyttet slike organisasjoner til å flytte midler, gi logistikkstøtte, rekruttere medlemmer, tilføre legitimitet eller på andre måter støtte terrorvirksomhet. PST er kjent med at ekstremister har opprettet organisasjoner nasjonalt med uklare formål, hvor det er uklart hva penger eller andre innsamlede formuesgoder har blitt brukt til.

Kontrollen av NPO-sektoren er i stor grad avhengig av i hvilken grad organisasjonene er registrert, og manglende tilknytning til offentlige registre gir færre kontrollmekanismer. Organisasjoner som aktivt unngår flere registre og rapporteringskrav, kan ha et underliggende motiv om å redusere myndighetsinnsyn.

Data viser at NPO-er med begrenset registrering, for eksempel kun i Enhetsregisteret, som hovedsakelig samler inn penger til konfliktområder, utgjør den høyeste risikoen for at midler blir misbrukt til kriminelle formål. Disse organisasjonene

har ofte lavere grad av krav og tilsyn, og er derfor attraktive for aktører som ønsker å skjule terrorfinansiering.

5. Utvalgte verdier benyttet til terrorfinansiering

Det er flere verdistrømmer som er særlig utsatt for bruk til terrorfinansiering i og fra Norge. Kontanter er fortsatt sentrale og flyttes gjerne via uformelle kanaler og kriminelle nettverk, mens kryptovaluta i økende grad benyttes til å sende og skjule midler. Forhåndsbetalte kort og handel med gull og luksusvarer fungerer som alternative kanaler, ettersom de er lette å transportere, omsette og vanskelige å spore. Disse midlene brukes til å dekke operative kostnader, støtte medlemmer og deres familier, samt opprettholde ekstreme organisasjoners virksomhet.

I dette kapittelet presenteres utvalgte verdistrømmer som vurderes av PST å ha en forhøyet risiko for terrorfinansiering. Listen er ikke uttømmende, men beskriver utvalgte muligheter nasjonalt, basert på tilgjengelig informasjonsgrunnlag i referanseperioden. For øvrig viser vi til Tolletatens analyser av betalingsstrømmer og økonomisk aktivitet i perioden 2022-2025 i NRA om hvitvasking, inkludert skjulte pengestrømmer, som også er relevant for terrorfinansieringsrisikoen.[32]

Kontanter

Kontanter anses fortsatt å være en av de foretrukne måtene for ekstremister å anonymt anskaffe, flytte, lagre og anvende midler på[33]. I de fleste tilfeller tilgjengeliggjøres midler som skal benyttes til å finansiere terror til slutt i kontanter, for å muliggjøre anonyme betalinger av logistiske og operative utgifter, slik som lønn, innkjøp av utstyr eller økonomisk støtte til familier.

Kontanter spiller en sentral rolle i uformelle økonomier og i organiserte kriminelle nettverk. Vi har sett at noen terrorgrupper deler transportruter med organiserte kriminelle grupper, fordi kanalene er ideelle for å skjule både midlenes opprinnelse og

[32] Økokrim, *Nasjonal risikovurdering*, 2026
[33] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

destinasjon. Kriminelle migrasjonsruter og godstransportnettverk kan brukes til diskrete transaksjoner i bytte mot kontanter.[34]

I motsetning til NRAs del om hvitvasking, hvor kontanter til dels anses å være upraktisk, gjelder ikke dette terrorfinansiering, hvor det ofte dreier seg om mindre beløp som er enklere å transportere og omsette. Kontanter er også foretrukket av flere internasjonale terrororganisasjoner.

Data PST besitter tilsier at kontanter fortsatt dominerer i finansieringen av terror, også på grunn av at organisasjoner ofte opererer i og fra områder med mindre grad av etablert finansiell og digital infrastruktur. Vi har dessuten sett at overføringer skjer ved bruk av ulovlige pengeoverføringstjenester, eller ved lovlige pengeoverføringer ut av landet, før midlene introduseres til den ulovlige økonomien.

Kryptoeiendeler

På grunn av kryptoeiendelenes kompleksitet og raske globale rekkevidde, erfarer PST at slike verdier i økende grad benyttes av ekstremister, både til å sende og tilegne seg midler som skal gå til terror. Enkelte eiendeler tilbyr også en større eller mindre grad av anonymitet, som gjør verdistrømmene vanskelig å spore.

Ekstreme islamister har i mer enn ti år eksperimentert med ulike typer kryptovalutaer, og enkelte IS-grener har gjennom sin propaganda oppfordret tilhengerne til å donere midler til deres virksomhet ved bruk av kryptovalutaer som Bitcoin[35] og Monero[36].

Siden 2022 har bruken av kryptovalutaer, FinTech-selskaper[37] og andre digitale betalingsmetoder økt markant blant ekstreme islamistiske grupper. Også grupper med et mer regionalt fokus, slik som Hamas, ligger i front når det gjelder anvendelsen av kryptovaluta. Hamas har i flere år bedt om at donasjoner skal skje via kryptovaluta og har etablert flere kryptovalutavekslingskontorer i eller i nærheten av områder der de opererer. Dette gir Hamas muligheten til enkelt å konvertere kryptovaluta til kontanter, noe som er essensielt for å kunne utnytte donasjonene i stor skala.[38]

---

[34] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[35] Bitcoin er en desentralisert digital valuta lansert i 2009 som fungerer uten sentralbanker eller mellomledd.
[36] Monero (XMR) er en desentralisert kryptovaluta med åpen kildekode, som fokuserer sterkt på privatliv, anonymitet og sporbarhet. I motsetning til Bitcoin, skjuler Monero automatisk avsender, mottaker og beløp i alle transaksjoner ved hjelp av avansert teknologi.
[37] FinTech (finansteknologi) er et paraplybegrep for teknologi som brukes i finansielle produkter og tjenester. Dette kan eksempelvis være innenfor betaling, sparing, finansiering, aksjehandel og forsikring.
[38] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

Kryptovaluta har også blitt et sentralt element i IS' overordnede finansieringsstrategi, og det er rapportert om donasjoner til ISKPs[39] medieenhet i Bitcoin, Ethereum[40] og USDT[41], som fremstår som en respons på aktiv propaganda og aktive rekrutteringskampanjer. Et konkret eksempel er en rekrutteringsoperasjon i Tadsjikistan, hvor ISKP samlet inn 2 millioner dollar i USDT fra globale sympatisører. Når disse midlene konverteres til kontanter, kan ISKP bruke kurerer til å distribuere pengene etter behov, betale for varer og tjenester eller dekke andre kostnader som for eksempel lønn.[42]

Avdekkede transaksjonsstrømmer involverer ofte bruk av ulike kryptoeiendeler, flere blokkjeder[43], delte kryptoadresser[44], lommebokleverandører[45] og utbetalingsmekanismer. Transaksjonsstrømmene blir vanskelige å spore når de på denne måten tilrettelegger for lettere tilsløring av både avsender og endelig mottaker.

Det er utfordrende å kvantifisere omfanget av kryptovalutamisbruk i forbindelse med finansiering av terrorhandlinger i og fra Norge. Økt tilgjengelighet, bredere aksept hos terrororganisasjoner og utviklingen av flere nisjeprodukter for å styrke anonymiteten, gjør det svært krevende å kartlegge og agere mot terrorfinansieringsoverføringer i kryptovaluta. PST ser likevel at bruken av kryptovaluta blant terrorgrupper og enkeltpersoner øker generelt, også i kombinasjon med andre metoder.

Det har forekommet terrorangrep i Vesten hvor det er avdekket at kryptovaluta er blitt benyttet i et forsøk på å tilsløre finansieringsstrømmene. Det finnes også flere tilfeller hvor ekstreme islamister i Norden har benyttet kryptovaluta i forbindelse med ulovlige pengeoverføringstjenester og terrorfinansiering. Det er dokumentert at ekstremister har brukt kryptovaluta for å flytte midler til ulike innsamlingstiltak som omtales i IS' propaganda, med mål om å støtte IS-operatører og deres familier som er fengslet i leirer i Nord Syria og Irak.

---

[39] ISKP (Islamic State Khorasan Province) er en del av den såkalte Islamske Stat og holder primært til i Afghanistan.
[40] Ethereum er en desentralisert, åpen blokkjedeplattform, primært kjent for å muliggjøre smarte kontrakter og desentraliserte applikasjoner. I motsetning til Bitcoin fungerer Ethereum som en programmerbar plattform som brukes som «drivstoff» for nettverkstransaksjoner.
[41] USDT eller «Tether» er en «stablecoin», en type kryptovaluta designet for å ha en stabil verdi som alltid er tilnærmet lik én amerikansk dollar. Den fungerer som en bro mellom tradisjonell valuta og kryptomarkedet og brukes mye for å sikre verdier, handle krypto uten store svingninger og for raske overføringer.
[42] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[43] En blokkjede er en desentralisert og distribuert digital «regnskapsbok», som gjør det mulig å registrere, spore og synliggjøre alle digitale transaksjoner. En blokkjede lagrer data i blokker, som linkes til hverandre ved bruk av kryptografi. Den mest velkjente bruken av blokkjeder er kryptovaluta, for eksempel Bitcoin.
[44] En kryptoadresse er en unik identifikator, bestående av en rekke bokstaver og tall, som brukes til å sende og motta kryptovaluta, tilsvarende et bankkontonummer.
[45] En kryptolommebok er et digitalt verktøy som lar en oppbevare, sende og motta kryptovaluta. Den fungerer som et grensesnitt mellom bruker og blokkjeden, hvor eventuelle digitale eiendeler er lagret.

Forhåndsbetalte kort

Kjøp av forhåndsbetalte kort som er lastet med et fast beløp av elektronisk valuta, er sett benyttet som et alternativ til overføring via tradisjonelle bankkontoer, kredittkort og kontanter. Disse betalingskortene er lette å frakte og muliggjør transaksjoner med et bredt spekter av tjenesteleverandører, som for eksempel Visa og MasterCard. Kjøp av såkalte «open loop[46]»-kort ser ut til å være mer attraktive, fordi de er lette å bruke i butikker og minibanker over hele verden.[47]

For øvrig viser vi til Økokrims omtale av gavekort i NRA 2026.

Gull og luksusvarer

Handel med luksusvarer, inkludert biler og kunst, kan også benyttes til å finansiere terror. Det samme gjelder handel med råvarer, slik som gull og diamanter. Slike varer representerer fysiske verdibærere, som er lette å forflytte og omsette i utlandet. Varene kan benyttes direkte eller senere omsettes til andre nødvendige goder for å opprettholde terrorvirksomheten.

Gull er en globalt akseptert handelsvare med liten sporbarhet og høy verdi. I Norge kan gull handles forholdsvis anonymt og lar seg lett smugle på tvers av landegrenser. PST er kjent med at det forekommer utstrakt kjøp og salg av gull i Norge, og at det også transporteres gull på tvers av landegrenser.

For øvrig henviser vi til kapittelet «Verdier utover penger: fysiske og digitale verdigoder» i Økokrims NRA, samt til omtalen av indikasjoner på skjulte pengestrømmer.[48]

[46] "Open loop"-kort er forhåndsbetalte kort som kan benyttes på lik måte som vanlige bankkort.
[47] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[48] Økokrim, *Nasjonal risikovurdering*, 2026

6. Utvalgte rapporteringspliktige med særlig risiko for å bli utnyttet til terrorfinansiering

Banker, betalingstjenester og tilbydere av kryptoeiendelstjenester er særlig utsatt for å bli utnyttet til terrorfinansiering. Tradisjonelle banktjenester brukes fortsatt til å plassere, oppbevare og overføre midler, ofte ved bruk av stråpersoner, familiemedlemmer, «neobanker» eller virtuelle IBAN-løsninger, som kan bidra til å skjule transaksjonens reelle formål og mottakere. Nye betalingstjenester og grensekryssende betalingsformidlere øker mulighetene for terrorfinansiering. Kryptoeiendelstjenester anses som særlig utsatt for å bli utnyttet til terrorfinansiering, ettersom disse fungerer som en inngangs- og utgangsport til den ordinære økonomien.

De nevnte indikatorer, fremgangsmåter og verdier tatt i betraktning, mener PST at det foreligger en særlig risiko for at banker, betalingstjenester og tilbydere av kryptoeiendelstjenester kan bli utnyttet av personer som ønsker å finansiere terror. Det understrekes at utvalget ikke skal tolkes slik at øvrige rapporteringspliktige ikke kan bli utnyttet for formålet. Det forutsettes at alle foretar selvstendige vurderinger av risikoen for terrorfinansiering ved egen virksomhet og eksponering.

Banker

Basert på datagrunnlaget som PST besitter, er det holdepunkter for at finansielle tjenester tilbudt av banker fortsatt utnyttes til terrorfinansiering. Dette til tross for det økte fokuset på tiltak som regulerer sektoren, inkludert identifisering av reelle rettighetshavere, åpenhet, styrkede identitetskontroller og tilsyn.

Banker anses internasjonalt å ha en høy risiko for å bli utnyttet til terrorfinansiering. Globalt rapporteres det at tradisjonelle bankkontoer fortsatt blir benyttet av transnasjonale terrorgrupper til plassering og oppbevaring av midler. Dette gjøres også ved bruk av strå- eller mellommenn, frontselskaper, grensekryssende etablering av selskaper og bankkontoer for å skjule identitet osv. Bruk av tradisjonelle

bankkontoer forekommer også hyppigere i områder under kontroll av terrororganisasjoner.[49]

PST har sett at såkalte neobanker[50] hjemmehørende i utlandet med sin grensekryssende virksomhet er nevnt i stadig flere saker hvor det også er indikasjoner på eller mistanke om terrorfinansiering. Disse har ofte en svakere etterlevelse av regelverk, eller opererer fra land med mindre eller lav grad av regulering og kontroll.

Virtuelle IBAN (vIBAN) er et fenomen som har fått økt oppmerksomhet i løpet av rapporteringsperioden. En virtuell IBAN er et digitalt bankkontonummer som ikke er direkte knyttet til en fysisk bankkonto, men som fungerer som et alias eller underkonto av en hovedkonto. Virtuelle IBAN utgjør en risiko for terrorfinansiering, fordi de kan brukes til å skjule midlenes opprinnelse og vanskeliggjøre de rapporteringspliktiges kontroll. PST har sett at bruken av virtuelle IBAN-numre er blitt mer vanlig i forsøk på terrorfinansiering, og er noe rapporteringspliktige bør være spesielt oppmerksomme på.

I det internasjonale samarbeidet rapporteres det at penger som stammer fra usikret og sikret kreditt[51] fortsatt benyttes til å finansiere terror, inkludert fremmedkrigere og lokale angrep. Midlene er i mange tilfeller fremskaffet ved dokumentforfalskning, eller ved hjelp av nær familie for å skjule endelig mottaker. PST har erfart at kjente norske ekstremister gjerne benytter kontoer tilhørende familiemedlemmer eller kontoer som kan knyttes til terrororganisasjoner, dersom de skal overføre penger til andre kjente ekstremister.

Transaksjoner fra ekstremister og overføringer til terrorrelatert formål er ofte av mindre størrelse. Dette gjør transaksjonene vanskelige å avdekke, spesielt dersom det benyttes metoder som nevnt ovenfor.

For øvrig henviser vi til Økokrims beskrivelse av relevante risikoer for banksektoren i deres NRA om hvitvasking.

[49] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[50] I denne sammenheng menes heldigitale banker uten fysisk lokasjon
[51] Eksempelvis forbrukslån, boliglån etc.

Betalingstjenester

Fremveksten av nye betalingstjenester har økt de siste årene. Flere av disse tilbyr pengeoverføringer og betalinger både fysisk og på nett. Mange opererer som mellomliggende aktører i betalingskjeder, noe som bidrar til å komplisere transaksjonsstrømmene ved at midler går via flere ledd, også grensekryssende, før de ender opp hos den endelige mottakeren. Sektoren er videre preget av innovasjon, som bidrar til at midler flyttes raskere over landegrenser. Mange slike tjenesteleverandører tilbyr også tjenestene fra utlandet, også jurisdiksjoner med mindre åpenhet eller kontroll.

Det fremgår av PSTs datagrunnlag at det i stadig større grad benyttes betalingstjenester til å flytte penger raskt over landegrenser, som et ledd i å tilsløre transaksjonsstrømmer. PST har erfart at digitale pengeoverføringstjenester[52] benyttes aktivt av norske ekstremister. Slike benyttes både til transaksjoner mellom ekstremister i Norge, men kanskje spesielt for overføringer ut av landet som kanaliseres videre til terrorformål. Vi ser at svakheter i enhetlig regulering og etterlevelse på tvers av jurisdiksjoner i større grad blir utnyttet til å skjule den endelige mottakeren og avsenderen av midler.

PST ser særlig en risiko forbundet med agenter for utenlandske betalingsforetak, som kan utføre betalingsformidlingstjenester for norske kunder på bakgrunn av konsesjon i et annet EØS-land. Agentene opererer raskt og befatter seg primært med små og grensekryssende transaksjoner, ofte til høyrisikoområder. Hvitvaskingsloven kan kun i begrenset grad anvendes for disse, noe som fører til mindre mulighet for nasjonal kontroll. Dette gjør metoden attraktiv for terroraktører, fordi hurtighet, manglende tiltak og enhetlig kontroll kan føre til at tiltenkt formål og destinasjon blir tilstrekkelig tilslørt. Flere av transaksjonene som gjennomføres i sektoren kan også anses som enkeltstående transaksjoner uten etablering av kundeforhold, noe som reduserer kravene til kundetiltak etter regelverket. Tjenestene ser i større grad ut til å bli benyttet av sårbare personer eller personer forbundet med høyere risiko, inkludert personer som står på utsiden av samfunnet og har begrenset tilgang til tradisjonelle banktjenester for overføringer til utlandet. Tjenestene er også svært utsatt for misbruk av kriminelle, som utnytter eksisterende svakheter i regulering, rutiner og kontroll. Dette har gjort sektoren mer utsatt for terrorfinansiering.

[52] Eksempler på digitale pengeoverføringstjenestetilbydere er PayPal, Wise, Revolut osv. Det bemerkes at Revolut og PayPal også har bankkonsesjon.

For øvrig henviser vi til Økokrims beskrivelse av relevante risikoer ved sektoren i deres NRA om hvitvasking. Mange av beskrivelsene som gjør sektoren utsatt for hvitvasking, gjør den også attraktiv for aktører som ønsker å finansiere terror.

Tilbydere av kryptoeiendelstjenester

Vi ser at kryptoeiendeler blir et stadig mer attraktivt middel for å finansiere terror. Dette skyldes mulighetene for rask flytting av store verdier over landegrenser. Kryptoeiendelstjenester anses som særlig utsatt for å bli utnyttet til terrorfinansiering, ettersom disse fungerer som en inngangs- og utgangsport til den ordinære økonomien. Selv om krypto forenkler forflytting og tilsløring av midler, forblir fiat-valutaer[53] det primære endemålet for terroraktører. Dettes skyldes graden av omsettelighet og verdi i markedet. Kryptoeiendelstjenester er derfor et kritisk kontrollpunkt for å hindre at terrorfinansiering får skje.

Det fremgår av PSTs datagrunnlag at kryptoeiendeler ofte benyttes til å flytte verdier ut av Norge. Vi har blant annet observert overføringer fra Norge til utenlandske aktører, eksempelvis i jurisdiksjoner med mindre grad av kontroll, eller til aktører som tillater handel i kryptoeiendeler som er anonyme eller mindre sporbare. Disse midlene er senere blitt overført til adresser knyttet til terrororganisasjoner. PST opplever det imidlertid utfordrende å kartlegge i hvor stor grad det er overført midler i den hensikt å finansiere terrorisme.

For øvrig viser vi til omtalen av krypto i NRAs del om hvitvasking, også om mulighetene for misbruk av nasjonale tilbydere av kryptoeiendelstjenester, spesielt når utenlandske aktører er involvert.[54]

[53] Med «fiat-valuta» menes valuta utstedt av en statlig enhet, gjerne en sentralbank, som fungerer som gyldig betalingsmiddel i en gitt jurisdiksjon. Eksempler er norske kroner, amerikanske dollar og euro.
[54] Økokrim, *Nasjonal risikovurdering*, 2026

7. Ulovlig og uregulert virksomhet

Ulovlig og uregulert virksomhet utgjør et stort mulighetsrom for terrorfinansiering. Ulovlig betalingsformidling tilbyr internasjonale kanaler til å formidle økonomiske bidrag og ses ofte i forbindelse med kriminelle aktører. Kriminelle aktører søker også å utnytte profesjonelle tilretteleggere for å tilsløre egen virksomhet, både ved misbruk av profesjonelle aktører, men også med direkte bistand fra eksempelvis advokater og regnskapsførere.

Mulighetene for innsamlingsvirksomhet har økt betraktelig i tråd med den teknologiske utviklingen, og terroraktører kan misbruke den geopolitiske situasjonen til å skjule terrorfinansiering som humanitær støtte.

Annen teknologisk utvikling, slik som digitale plattformer, gir ytterligere muligheter til fordekte transaksjoner med liten eller ingen sporbarhet, noe internasjonale terrororganisasjoner i økende grad utnytter. Alternative formuesgoder som gull og spillvirksomhet fortsetter å være foretrukne alternativer for overføring av verdier med terrorhensikt, gitt deres høye verdi og reduserte sporbarhet.

Ulovlig betalingsformidling

Ifølge internasjonale rapporter benyttes ulovlig betalingsformidling, inkludert ulovlige pengeoverføringstjenester, i utstrakt grad for å flytte midler som skal understøtte terrorrelatert virksomhet. Blant annet benytter ekstremister egne nettverk for å motta og overføre midler over landegrenser og lagre verdier på vegne av gruppen. Disse nettverkene, som for eksempel ISKP i Afghanistan, er integrert i andre IS-relaterte finansielle strukturer som støtter IS' finansielle operasjoner globalt.[55]

Det rapporteres også at nesten alle terrorgrupper kan knyttes til bruk av ulovlige eller uregulerte betalingstjenester. Slike benyttes også internt for å flytte penger innenfor organisasjonen og til å betale fremmedkrigere og til å dekke kostnader knyttet til rekruttering, reise, opphold og operative handlinger. Det samme gjelder økonomiske bidrag fra diasporaer, som ofte kanaliseres til terrororganisasjoner i andre land gjennom slike ulovlige pengeoverføringer.[56]

[55] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[56] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

Ulovlige tjenester benyttes også til å skjule inntekter fra kriminell virksomhet som involverer grensekryssende transaksjoner, for eksempel narkotikahandel og smugling. PST har i den sammenheng også sett indikasjoner på at midler som er flyttet som del av annen kriminell virksomhet ved hjelp av slike nettverk, til slutt kan ha gått til både tilsiktet og utilsiktet terrorfinansiering. Dette beskrives nærmere i kapittel 4, «Tilknytning til kriminelle nettverk».

PST har data som underbygger at midler overføres fra Norge ved hjelp av personer og foretak som tilbyr ulovlige pengeoverføringstjenester i markedet. Sammenblanding gjør det imidlertid utfordrende å kartlegge i hvor stor grad midlene er overført for å finansiere terrorisme. Risikoen øker på grunn av et stort handlingsrom og enkel tilgjengelighet.

Profesjonelle tilretteleggere

Økokrim definerer profesjonelle tilretteleggere og innsidere som for eksempel regnskapsførere, bankrådgivere og advokater. Disse kan muliggjøre hvitvasking og/eller terrorfinansiering ved å bistå med åpning av kontoer, tilby klientkonto, skjule reelle rettighetshavere og pengestrømmer, tilrettelegge for lån eller «lukke øynene» i sentrale portvokterroller.[57]

For å overføre og skjule sporbarheten til midler som er tiltenkt terrorfinansiering, kan ekstremister benytte såkalte profesjonelle tilretteleggere. Til tross for en tilsynelatende stor etterspørsel etter slike tilretteleggere, er det PSTs vurdering at slike i større grad benyttes til hvitvasking av utbytte heller enn terrorfinansiering.

Transaksjoner utført av ekstremister er ofte små og totalbeløpet sjelden omfattende, sammenlignet med midler som ønskes hvitvasket. Vi har likevel sett at en viss grad av tilrettelegging kan være nødvendig for å kanalisere midler til de rette mottakerne. Eksempelvis har terrororganisasjoner som al-Qaida og IS hatt behov for mellommenn, som fungerer som bindeledd mellom givere og de operative gruppene.[58] Det er derfor en risiko for at slike også kan eksistere i Norge. Dette fører til at rapporteringspliktige bør rette sin oppmerksomhet særlig mot å avdekke profesjonelle tilretteleggere.

[57] Økokrim, *Nasjonal risikovurdering*, 2026
[58] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

Det kan også forekomme tilfeller der ekstremister aktivt forsøker å villede profesjonelle tilretteleggere. Det er ofte krevende for rapporteringspliktige å oppdage mistenkelige transaksjoner, på grunn av deres store antall kunder og høye arbeidstempo. Regnskapsførere, som er mer involvert i behandlingen av kundenes regnskapsmateriale, anses som en mer risikoutsatt gruppe enn revisorer, ettersom revisorer gjennomgår materialet med tilbakevirkende virkning. For advokater viser datagrunnlaget at antall innsendte MF-rapporter fra advokater har vært lavt sammenlignet med det som er sendt inn av regnskapsførere og revisorer. Dette kan indikere et behov for økt kompetanse om terrorfinansiering i sektoren, for å redusere risikoen for at den kan bli misbrukt.

Fra et terrorfinansieringsperspektiv er også bruken av falske fakturaer og kvitteringer en potensiell risiko, spesielt sett i lys av generativ KIs mulighet til å fabrikkere kvitteringer. Ekstremister kan forsøke å inkludere tilsynelatende legitime fakturaer og kvitteringer i regnskapsmaterialet for å villede regnskapsførere og revisorer, og på denne måten skjule terrorfinansieringsvirksomhet.

PST er så langt ikke kjent med at norske ekstremister har benyttet seg av profesjonelle tilretteleggere i noen utstrakt grad. Det finnes likevel muligheter, og det er således en risiko for at disse vil kunne benyttes til å understøtte terrorfinansiering i og fra Norge.

Generell risiko knyttet til profesjonelle tilretteleggere er ytterligere beskrevet i kapittel 6 av Økokrims NRA.[59]

Innsamling av penger og formuesgoder

Innsamling av penger eller andre formuesgoder i Norge er ikke lovregulert. Det er heller ingen krav til registrering eller underretning. Dette betyr at enkeltpersoner og lukkede miljøer kan samle inn penger uten å måtte opprette en organisasjon.

PST har sett at norske ekstremister i noen grad leder, men i større grad deltar i, innsamlingsvirksomhet hvor formålet med innsamlingen ofte er uklar. Ekstreme islamister benytter for eksempel religiøse arenaer, som moskeer, til å samle inn penger via zakat[60] og lignende. Denne metoden er egnet til å generere større beløp

[59] Økokrim, *Nasjonal risikovurdering*, 2026
[60] Å gi zakat, som betyr "å gi til de fattige", er en av islams fem søyler. De andre er bønn (adhan), haj (pilgrimsreise), shahada (martyrdom) og faste i Ramadan.

ved å utnytte givernes religiøse overbevisning, og det er en risiko for at midlene som samles inn kan bli benyttet til å finansiere terror. Det er avdekket flere tilfeller hvor innsamlinger med norske givere har blitt gjort for å understøtte terrorformål.

Vi har også sett at enkeltpersoner, som ikke er tilknyttet en veldedig organisasjon, kan starte innsamlingskampanjer under dekke av humanitære eller sosiale årsaker, mens de innsamlede midlene i siste instans potensielt støtter terrorrelaterte aktiviteter eller ekstremister. Humanitære og veldedige saker tjener som effektive skalkeskjul og er derfor egnet til å utnyttes for terrorfinansieringsformål. Eksempler på veldedige formål som kan bli misbrukt er konfliktene i Gaza, Syria og på Afrikas horn.[61]

De seneste årene har ny teknologi muliggjort mer effektiv pengeinnsamling. PST er kjent med at enkeltpersoner og organisasjoner i Norge har iverksatt innsamlinger til norgestilknyttede fremmedkrigere og internasjonale terrororganisasjoner, uten at disse personene eller organisasjonen er registrert av for eksempel Innsamlingskontrollen[62].

Det er observert en trend blant norske ekstreme islamister hvor midler samles inn for å støtte eller smugle ut IS-tilknyttede fremmedkrigere, samt deres familiemedlemmer, fra leirer og fengsler i Syria. Flere nettverk har samlet inn penger, som deretter er overført via ulovlige pengeoverføringstjenester eksempelvis til fangeleiren al-Hol[63] i Syria. De ansvarlige for de ulike innsamlingskampanjene aksepterer et bredt spekter av midler, inkludert kryptovaluta. På sine nettkanaler, i grupper og på kontoer oppgir innsamlerne at midlene skal brukes til å forbedre fangenes forhold eller sikre deres løslatelse.[64]

For norske høyreekstremister er det mindre vanlig å engasjere seg i innsamlingsvirksomhet for å finansiere terrorrelaterte aktiviteter i utlandet. Historisk har det heller vært en tendens til å benytte innsamlingsaktiviteter hovedsakelig for å støtte andre høyreekstremister personlig. Eksempelvis har det innenfor de mer hierarkisk organiserte gruppene i Norden blitt samlet inn penger for å betale bøter, støtte medlemmer som har avtjent fengselsstraff, eller på andre måter støtte medlemmer ved behov.

PSTs datagrunnlag tilsier at risikoen for innsamlingstiltak som understøtter terrorfinansiering til en viss grad vil gjenspeile den generelle geopolitiske situasjonen,

[61] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[62] Innsamlingskontrollen er en norsk stiftelse som har som formål å påse at innsamlinger gjennomføres på en forsvarlig måte.
[63] Al-Hol er en flyktningleir i Syria som huser en stor andel kvinner fra områder tidligere kontrollert av IS.
[64] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

og det vil være en større risiko for slik terrorfinansiering i perioder med geopolitisk usikkerhet og humanitære kriser.

Sosiale medier, digitale plattformer og gavekort

«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.»

- *Nasjonal trusselvurdering 2026 (PST)*

PST erfarer at ulike digitale plattformer i større grad aktivt benyttes som supplerende verktøy i prosesser for å tilsløre eller skjule pengeoverføringer.

Digitale innsamlingskampanjer annonseres typisk åpent via sosiale medier, men også maskert som oppfordringer til humanitær hjelp eller andre veldedige formål. Det er dokumentert økt bruk av QR-koder blant diverse terrorgrupper for å be om donasjoner eller for å formidle adresser til kryptolommebøker. I tillegg anvendes krypterte kommunikasjonsapplikasjoner i stor grad, fordi de muliggjør sikre samtaler om betalingsmetoder og den faktiske bruken av de innsamlede midlene.[65]

Terrororganisasjoner og enkeltpersoner rapporteres i økende grad å benytte krypterte meldingsapplikasjoner som WhatsApp, Telegram, Viber, Signal og lignende. Disse plattformene tilbyr private samtaler som garanterer brukernes anonymitet. Ekstremister utnytter tjenestene til å overføre finansielle data (f.eks. IBAN-numre, lommebokadresser eller andre betalingsmidler) og til å gi instruksjoner om donasjoner på en sikker måte. Funksjoner som «selvdestruerende» meldinger, som automatisk slettes etter et forhåndsdefinert tidsintervall, gjør sporing vanskeligere.[66]

Tilrettelegging for fordekte transaksjoner gjennom meldingstjenester kan gi betydelige utfordringer knyttet til sporbarhet. Når midler innføres i betalingssystemet, er detaljnivået om den endelige mottakeren svært begrenset. Det er kun sammenholdt med informasjonen som den aktuelle sosiale medieplattformen besitter, at det er mulig å fullstendig belyse transaksjonenes egentlige formål. Ved utgående overføringer fra den interne plattformen kan transaksjonsinformasjonen avdekke noe

[65] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[66] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025

om den opprinnelige sosiale plattformen, men i mange tilfeller vil den kun identifisere finansielle formidlere, noe som gjør kildeidentifikasjon av midlene vanskelig.[67]

Etter hvert som slike verktøy blir mer populære, lett tilgjengelige og lønnsomme, har terrororganisasjoner og enkeltpersoner tilpasset seg for å utnytte dem til å skaffe finansielle midler. Det er rapportert at enkelte terrorgrupper har benyttet innsamlingskampanjer på TikTok, hvor de har brukt aktuelle funksjoner som filtre og spill til å generere penger. I Sverige ble en 24-åring dømt til fengselsstraff for terrorfinansiering etter at han i perioden juli 2022 til juli 2023 samlet inn omkring en halv million svenske kroner via TikTok, som han sendte videre til personer knyttet til IS.[68]

Det er viktig å påpeke at det også i Norge er et stort handlingsrom for å støtte slike initiativer som ledes fra utlandet. Dette skyldes at det er krevende å få innsikt i de integrerte betalingsfunksjonene som tilbys av de ulike sosiale mediene.

PST er kjent med at ekstremister har begynt å benytte E-handelsplattformer[69] for operative innkjøp av utstyr, våpen, kjemikalier og materiell til 3D-printing. Dette er mer diskret enn fysiske anskaffelser. Slike plattformer kan også brukes til å selge varer for å finansiere terrorhandlinger, og til å flytte midler på måter som ligner handelsbaserte hvitvaskingsmetoder. De omsettelige varene kan dermed fungere som forkledning for verdier som overføres mellom nettverksmedlemmer.

Gullforhandlere

Gull er en universell valuta som kan anvendes verden over og er særlig attraktiv i land der finansielle systemer i mindre grad fungerer.

Per i dag er ikke norske forhandlere av gullvarer pliktig til å sende inn rapporter om mistenkelige forhold til FIU Økokrim. Det er imidlertid flere indikasjoner på at gullforhandlere utnyttes som ledd i terrorfinansiering. PST er kjent med betydelig aktivitet i sektoren og at flere ekstremister, i Norge så vel som i utlandet, kan knyttes til omfattende handel med gull.

[67] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[68] Misstanken: 24-åring finansierade terrorgrupp via Tiktok och kryptovaluta – döms | SVT Nyheter
[69] En e-handelsplattform er en programvareløsning som lar bedrifter og privatpersoner selge produkter og tjenester på nett.

Spillvirksomhet

Ulovlig pengespill

Ulovlige og uregulerte pengespill er identifisert som en betydelig og voksende terrorfinansieringsrisiko globalt, også av FATF[70]. Terrorfinansiering muliggjøres blant annet gjennom generering av inntekter, rigging, bruk av stråmenn, mellomledd, en kombinasjon av ulovlig spillvirksomhet og kryptoeiendeler, uklare utbetalingsstrukturer osv.

Som nevnt i NRA om hvitvasking, estimerer Lotteritilsynet at det uregulerte pengespillmarkedet i Norge utgjorde mellom 1,7 og 2,0 milliarder kroner i 2025.[71] Utenlandske pengespill har ikke de samme taps- og innsatsbegrensningene som norske spillselskap, og vil dermed være mer attraktive å benytte til hvitvaskingsformål så vel som terrorfinansiering. Det er et stort marked av utenlandske pengespill som kasino, poker og oddsspill på internett. Disse har ikke lov til å tilby pengespill i Norge, men er likevel tilgjengelige og rettet mot norske borgere. Det er videre uklart hvem som faktisk står bak flere av disse spilltjenestene.

Transaksjoner via utenlandske spillplattformer er også sett brukt som et fordekt dekke. Overføringer til spillkontoer fremstår som de er tiltenkt brukt til spill, men i realiteten blir midlene videreført derfra til den reelle mottakeren via spillkontoen, uten at midlene benyttes til spilling overhodet.

Pyramide- og ponzi-opplegg[72] har en forhøyet risiko for å bli misbrukt til terrorfinansiering. PST har observert at terrorgrupper har benyttet ponzi-opplegg for å generere midler som, enten direkte eller indirekte, går til å understøtte terrorvirksomhet. Midlene blir ofte hvitvasket for å skjule deres reelle destinasjon.

Interpol har rapportert om et transnasjonalt eksempel som inkluderer 17 land over hele verden. Saken hadde sitt utgangspunkt i et ponzi-opplegg basert på kryptovaluta. Virksomheten hadde mer enn 100 000 ofre og et estimert tap på over

[70] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[71] Lotteri- og Stiftelsestilsynet, *Ansvarligheit og kanalisering hos Norsk Tipping og Norsk Rikstoto, mars 2026. Netto omsetning er innsats minus gevinst til spillerne*, 2026
[72] En ponzi-svindel (eller ponzi-opplegg) er en form for investeringsbedrageri der avkastningen utbetales til tidligere investorer ved hjelp av penger fra nye investorer, istedenfor reell profitt.

500 millioner USD. Interpols etterforskning fant at flere av de benyttede krypto-lommebøkene potensielt kunne være knyttet til terrorfinansiering.[73]

Det er uavklart hvorvidt terror er blitt finansiert på denne måten i og fra Norge. Basert på omfanget av den ulovlige virksomheten, samt potensielle mørketall, er det PSTs vurdering at det ikke kan utelukkes at slike verdier har blitt kanalisert til terrorfinansiering, særlig i utlandet.

Videospill og spillobjekter

Vi har sett at noen terrorgrupper, eksempelvis høyreekstreme grupper og Hizbollah, utvikler og selger egne videospill både som propagandaverktøy og finansieringskilde. Slike spill er tilgjengelige på det åpne nettet. I tillegg forekommer transaksjoner via såkalte «spillobjekter», som er dokumentert brukt av enkelte høyreekstreme grupper. Disse spillobjektene kan kjøpes og doneres til andre spillere med svært begrenset sporbarhet.[74]

PST har ikke konkrete data på hvorvidt spillplattformer benyttes til terrorfinansiering i Norge, men er likevel kjent med at flere norske banker opplever en økning i antall kunder som overfører små eller mellomstore beløp til spillplattformer. Det rapporteres tidvis om overføring av større beløp, og det finnes også eksempler på gutter og unge menn som foretar store månedlige overføringer til spillplattformer.[75] Så langt har vi imidlertid ikke kunnet fastslå at transaksjoner er knyttet til terrorfinansiering, men utviklingen og omfanget taler for en økt risiko for tilsløring gjennom spill. Vi viser i denne sammenheng til det som tidligere er nevnt om radikalisering av mindreårige.

Det er en risiko for at den økende bruken av videospill vil kunne fungere som et verktøy for å påvirke barn og unge til å engasjere seg i finansiering av terrorrelatert virksomhet.

[73] Interpol, *83 arrests in landmark African operation against terrorism financing*, 2025
[74] FATF, *Comprehensive Update on Terrorist Financing Risks*, 2025
[75] Økokrim, *Financial Intelligence Unit Årsrapport*, 2025

8. Sårbarhetsbilde

Å avdekke terrorfinansiering er komplisert. Stadig flere aktører er involvert i transaksjonsstrømmer på tvers av landegrenser og jurisdiksjoner. Dette øker handlingsrommet for å tilsløre både avsendere og mottakere av midler.

Grensekryssende transaksjonsstrømmer som involverer flere aktører gjør det i tillegg vanskelig å følge midlene, men enda vanskeligere å fastslå at midler er blitt overført av en avsender for at de skal gå til terrorvirksomhet. Det enkelte bidrag er ofte av mindre størrelse, og dersom det er overført gjennom legitime overføringsmetoder, blir det desto mer krevende å skille dette fra andre, lovlige pengestrømmer.

Den økende sammensmeltingen av konvensjonelle og digitale innsamlings- og overføringsmetoder kompliserer bildet ytterligere.

Kompleksiteten i dagens verdi-/transaksjonsstrømmer forutsetter tilstrekkelig kunnskap og fenomenforståelse, og ofte tilgang til flere informasjonskilder for å kunne fastslå at et konkret tilfelle gjelder terrorfinansiering. Saker om terrorfinansiering er derfor krevende både å forbygge og etterforske. Usikkerheten knytter seg både til om transaksjonen lar seg spore, og til å avgjøre om transaksjonen er foretatt med tilstrekkelig forsett.

Tilgjengelige virkemidler og kapasitet

PST har i referanseperioden sett at en økende del av overføringene knyttet til terrorfinansiering dreies bort fra regulerte tjenester og over i det ulovlige og uregulerte markedet.[76] Dette inkluderer men er ikke begrenset til såkalte P2P-transaksjoner, eller transaksjoner tilrettelagt av personer og nettverk som tilbyr betalingsformidlingstjenester utenfor den lovlige økonomien. Dette skjer også i større grad ved bruk av supplerende teknologi som krypterte meldingstjenester i kombinasjon med kunstig intelligens og bruk av kryptoeiendeler på ulike blokkjeder.

På bakgrunn av dagens regulatoriske rammeverk, rollefordeling og myndighet innenfor forebygging av terrorfinansiering, fører denne nevnte dreiningen til et behov for økt samarbeid mellom alle relevante aktører, inkludert rapporteringspliktige, for å identifisere, forebygge og straffeforfølge terrorfinansieringsaktivitet.

[76] Det understrekes at det på tross av observert dreining mot ulovlig og uregulert virksomhet, fortsatt gjennomføres verdistrømmer med mål om å finansiere terror gjennom å utnytte regulerte tjenester.

Manglende analyse- og etterforskningskapasitet hos myndighetsaktører utgjør dermed en sårbarhet for i tilstrekkelig grad å kunne identifisere indikasjoner på terrorfinansiering og handle forebyggende og strafferettslig.

Det har vært få saker som har ledet til domfellelser for terrorfinansiering i Norge. Det er likevel viktig å påpeke at finansielle spor, analyse av transaksjonsstrømmer og oversikt over finansielle disposisjoner er viktige informasjonskilder for PST, også i de sakene som ikke eksplisitt omhandler terrorfinansiering.

Øvrige sårbarheter ved det norske regimet

På tross av en økning i antall innsendte MF-rapporter, er det vedvarende sårbarheter i etterlevelsen av gjeldende regelverk. I flere evalueringer av Norges innsats mot terrorfinansiering er det blitt avdekket flere sårbarheter som påvirker effektiviteten av det norske kontrollregimet.[77]

En sårbarhet er knyttet til at det generelt er en lav forståelse av fenomenet terrorfinansiering i Norge. Det er krevende å gjenkjenne aktuelle modus og hvilke potensielle aktører som kan stå bak. Dette får følger for det videre datagrunnlaget. En sentral sårbarhet er datagrunnlaget for å vurdere om mulighetene for terrorfinansiering faktisk blir utnyttet nasjonalt. Samtidig deles det generelt lite systematiske data på tvers av offentlige myndigheter om omfang, trender og effekten av iverksatte tiltak. Eksisterende kunnskapsgrunnlag bygger i stor grad på generelle trusselvurderinger, internasjonalt observerte modusbeskrivelser og enkeltsaker.

Dette betyr at det i dag er mer kunnskap om potensielle sårbarheter og mulige modus enn om det faktiske omfanget, utviklingen og effekten av tiltakene. Dette gjør at mangel på funn ikke uten videre kan tolkes som at terrorfinansieringsvirksomhet ikke forekommer.

Som nevnt i NRA om hvitvasking, preges også mange offentlige aktører innenfor terrorfinanseringsarbeidet av silotenkning og fokus på avgrensinger av eget mandat. Dette går igjen ut over informasjonsdelingen mellom ulike etater, men også med privat sektor og øvrige aktører som bidrar i den totale innsatsen mot terrorfinansiering. Et manglende fokus på sårbarheter utfordrer videre den nasjonale implementeringen av et effektivt motstandsregime.

[77] Se blant annet FATFs oppfølgende rapport etter evalueringen av Norge (2023) og IMFs rapport om antihvitvaskingsarbeidet i Norden og Baltikum (2023).

Videre benytter både myndigheter og rapporteringspliktige ofte lang tid på å utvikle tilstrekkelig kompetanse, verktøy, tilsyn og regelverk som står i forhold til den faktiske risikoen. Dette gjelder også regler for informasjonsdeling og systemer som muliggjør slik deling raskt og effektivt, også på tvers av landegrenser. Resultatet er at ekstremister kan ta i bruk nye digitale verktøy raskere enn myndigheter og plattformer klarer å tilpasse seg og således får operere uten hindringer.

Vi viser for øvrig til sårbarhetene som er beskrevet i NRAs del om hvitvasking, hvorav flere også er relevante for arbeidet med terrorfinansiering.

Statlige aktører

«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.»

- *Nasjonal trusselvurdering 2026 (PST)*

PSTs datagrunnlag underbygger at noen terrororganisasjoner i utlandet har mottatt og fortsatt mottar økonomisk og annen støtte fra statlige aktører. Statlig støtte til terror kan ta flere former, og kan inkludere direkte økonomisk støtte, logistisk bistand og materiell støtte eller opplæring. Statlig støtte kombinert med teknikker for omgåelse av sanksjoner gjennom handel eller smugling av råvarer, gjør det mer komplisert for både rapporteringspliktige og sikkerhetstjenester å avdekke en eventuell finansiering.

Norske rapporteringspliktige bør være oppmerksomme på denne typen finansiering. Risikoen er ofte indirekte og skjult i geografisk eksponering, bruk av mellomledd, komplekse eierskapsstrukturer og grensekryssende transaksjoner. Dette gjør det nødvendig med forsterkede kundetiltak, god forståelse av reelle rettighetshavere og økt oppmerksomhet rundt hvorvidt tilsynelatende ordinære kundeforhold eller betalingsstrømmer kan inngå i et bredere terrorfinansieringsbilde.

9. Konsekvenser

Terrorfinansiering få konsekvenser både internt i Norge og fra Norge til utlandet. I Norge kan terrorfinansiering bidra til å opprettholde og styrke ekstremistiske nettverk, legge til rette for rekruttering, propaganda, logistikk og i verste fall planlegging eller gjennomføring av terrorangrep. Konsekvensen er derfor ikke bare økonomisk kriminalitet i snever forstand, men en potensiell styrking av aktører som truer liv og helse, så vel som nasjonal sikkerhet og trygghetsfølelse.

Terrorfinansiering fra Norge til utlandet kan også ha alvorlige konsekvenser, selv om den aktuelle voldshandlingen skjer i et annet land. Slike midler kan bidra til å opprettholde terrorgrupper, finansiere angrep, forlenge konflikter og svekke den internasjonale sikkerheten. For Norge innebærer dette også en risiko for at landet brukes som en plattform eller et mellomledd i internasjonale finansieringskjeder, noe som vil få konsekvenser for Norges sikkerhetspolitiske ansvar og internasjonale forpliktelser.

10. Samlet risikovurdering

Overordnet vurderes den samlede risikoen for terrorfinansiering som MODERAT. Det faktiske omfanget synes begrenset, men sårbarheter og muligheter for misbruk tilsier at risikoen ikke kan anses som LAV. Risikoen for terrorfinansiering internt i Norge vurderes som lavere enn risikoen fra Norge til utlandet.

Vurderingen av risikonivå har blant annet sammenheng med at norske ekstremisters internasjonale bidrag til terrorfinansiering generelt erfares som begrenset i både omfang og antall. PST ser i denne sammenheng at norske aktører heller ikke har kapasitet til å skaffe til veie store midler, og finansiering fra Norge til terrorvirksomhet i utlandet er sjelden omfattende. Selv om enkelte bidrag kan være betydningsfulle for enkeltaktører eller små grupper som planlegger eller gjennomfører spesifikke angrep, utgjør disse aktivitetene relativt liten risiko i det globale bildet. Norges rolle som kilde til midler for internasjonal terror er derfor fortsatt marginal, men en relevant kapasitet for spesifikke aktører eller operasjoner.

I Norge er situasjonen tilsvarende. Terrorfinansiering skjer primært gjennom individuelle aktører, der bidragene ofte er små og knyttet til egen økonomi. Finansiering fra norske ekstremister internt i Norge retter seg sjelden mot større, organiserte terrornettverk, og risikoen begrenser seg i hovedsak til støtte til enkeltpersoner som planlegger voldelige handlinger i Norge. Dette kan gjøre det mindre krevende for norske sikkerhetsmyndigheter og rapporteringspliktige å forebygge og overvåke enkeltaktører, men fenomenet innebærer fortsatt tydelige sikkerhetsmessige utfordringer.

Vedlegg

§ 135 Terrorfinansiering

Med fengsel inntil 10 år straffes den som rettstridig yter, mottar, sender, fremskaffer eller samler inn penger eller andre formuesgoder med hensikt eller viten om at midlene helt eller delvis skal brukes

a. *Til å utføre en handling som nevnt i §§ 131, 134, 136b eller §§ 137 til 144,*
b. *Av en person eller gruppe som har til formål å begå handlinger som nevnt i §§131, 134, 136b, eller §§ 137 til 144, når personen eller gruppen har tatt skritt for å realisere formålet med ulovlig midler,*
c. *Av et foretak som noen som nevnt i bokstav b eier eller har kontroll over, eller*
d. *Av et foretak eller en person som handler på vegne av eller på instruks fra noen som nevnt i bokstav b.*

På samme måte straffes den som stiller banktjenester eller andre finansielle tjenester til rådighet for personer eller foretak som nevnt i første ledd bokstav b, c eller d.

§ 136a Straff for deltakelse mv. i en terrororganisasjon

Med fengsel i inntil 6 år straffes den som danner, deltar i, rekrutterer medlemmer eller yter økonomisk eller annen materiell støtte til en terrororganisasjon, når organisasjonen har tatt skritt for å realisere formålet med ulovlige midler.

Medvirkning straffes ikke.

POLITIETS
SIKKERHETSTJENESTE

pst.no