Den Nationale Risikovurdering af Terrorfinansiering

Januar 2024

Indhold

Forord

Politiets Efterretningstjeneste (PET) udgiver for tredje gang Den Nationale Risikovurdering af Terrorfinansiering. Risikovurderingen er blevet til i samarbejde med interessenter fra hele rigsfællesskabet, og PET vil gerne takke for interesse, sparring og bidrag. Samarbejdet har været konstruktivt og afspejler de tætte relationer på tværs af myndigheder, brancheorganisationer og underretningspligtige virksomheder og personer i Danmark.

Risikovurderingen er udarbejdet på baggrund af internationale anbefalinger til metode og interessentinddragelse. Samtidigt er der hentet inspiration i andre landes risikovurderinger af terrorfinansiering og hvidvask, ligesom aktuel forskning og risikovurderinger på andre områder er inddraget. Det betyder, at en risikovurdering af terrorfinansiering i Danmark vil ændre metode og format over tid, og denne nye nationale risikovurdering er ingen undtagelse. De væsentligste forskelle fra den seneste risikovurdering fra januar 2020 er, at der i den nye risikovurdering sondres tydeligere mellem henholdsvis trusler, sårbarheder og risici i forbindelse med terrorfinansiering, og hvordan disse begreber har betydning for hinanden. Derudover er der lagt mere vægt på beskrivelse af forskellige risikoområder, hvilket også har været ønsket af mange underretningspligtige.

PET og Hvidvasksekretariatet har et tæt og godt samarbejde, og det er blevet understreget i arbejdet med at udarbejde de nye nationale risikovurderinger for henholdsvis hvidvask og terrorfinansiering. Det har vist sig meget givende at koordinere og dele viden omkring sårbarheder og overlappende temaer.

Tilsvarende har begge risikovurderinger i tilblivelsesfasen ligget som fundament for udarbejdelsen af National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025, der udkom i juli 2022. Den nye nationale strategi pointerer, at kriminalitetsbilledet såvel som samfundsudviklingen er i bevægelse, hvilket fordrer en fokuseret og sammenhængende indsats mod hvidvask og terrorfinansiering.

PET ser frem til at fortsætte den fælles indsats, og Den Nationale Risikovurdering af Terrorfinansiering udgør sammen med Den Nationale Risikovurdering af Hvidvask og EU-Kommissionens overnationale risikovurdering et vigtigt fundament herfor.

God læselyst!
PET

Ordliste og begrebsforklaring

Autoriseret pengeoverførselsvirksomhed: Autoriserede pengeoverførselsvirksomheder kan være virksomheder, der har pengeoverførsel som primær ydelse, eller virksomheder, der i forbindelse med drift af kiosk- eller købmandsvirksomhed fungerer som agent for en større udenlandsk pengeoverførselsvirksomhed. Autoriserede pengeoverførselsvirksomheder er underlagt Finanstilsynets tilsyn og hvidvasklovens forpligtelser.

FATF: Financial Action Task Force er en mellemstatslig organisation med ansvar for at udvikle politikker til bekæmpelse af hvidvask og terrorfinansiering.

Hawala: Pengeoverførselsvirksomhed, hvor ind- og udbetalingslokaliteter er forskellige, og hvor mellemværendet mellem de to virksomheder afregnes separat ud fra de enkelte kunders transaktioner, som derfor ikke fremgår som elektroniske overførsler.

Identitetsmisbrug: Samlebetegnelse for forhold, hvor en (digital) identitet bliver misbrugt til berigelseskriminalitet.

Kryptoaktiver: Digital gengivelse af værdier eller rettigheder, som kan overføres og lagres elektronisk ved hjælp af distributed ledger-teknologi (DLT) eller lignende teknologi.

Nonprofit-området: Foreninger, almennyttige fonde og indsamlinger mv.

Ulovlig pengeoverførselsvirksomhed: Uregistreret og dermed ulovlig erhvervsmæssig overførsel af midler via finansiel virksomhed eller hawala.

Underretningspligtige virksomheder og personer: Det følger af hvidvasklovens § 26, at virksomheder og personer omfattet af hvidvasklovens § 1 skal underrette Hvidvasksekretariatet, hvis virksomheden eller personen er vidende om, har mistanke om eller rimelig grund til at formode, at en transaktion, midler eller en aktivitet har eller har haft tilknytning til hvidvask eller finansiering af terrorisme.

01

Introduktion

Formål

Risikovurderingen har som formål at forhindre terrorfinansiering både i Danmark og i udlandet. Det sker ved, at risikovurderingen er med til at udbygge de underretningspligtige virksomheder og personers viden om terrorfinansiering. De underretningspligtige bør derfor inddrage risikovurderingen, når de vurderer risikoen for, at virksomheden eller personen kan blive misbrugt til hvidvask eller terrorfinansiering, og når de tilrettelægger interne kontroller på området. Derudover kan myndighederne anvende risikovurderingen som grundlag for en risikobaseret tilgang til vejlednings- og kontrolarbejdet.

Analysedesign

Risikovurderingen består af to dele. Første del har en generel karakter, hvor kapitel 2 introducerer terrorfinansiering og risikobegrebet, hvorefter kapitel 3 redegør for den gældende kriminalisering af terrorfinansiering i Danmark. Kapitel 4 og kapitel 5 vedrører henholdsvis truslerne og sårbarhederne med hensyn til terrorfinansiering i Danmark. Kapitel 6 afslutter første del ved særskilt at behandle trusler og sårbarheder relateret til terrorfinansiering i Grønland og på Færøerne.

Anden del af risikovurderingen består af kapitlerne 7-16, der hver især sætter fokus på særligt risikofyldte områder som fx ulovlig pengeoverførselsvirksomhed eller kryptoaktiver. Fokus er her på at foretage en særskilt vurdering af risikoen for terrorfinansiering for hvert enkelt risikoområde.

Hovedfund

Af kapitlerne 4-15 fremgår sammenfatninger, som opsummerer de væsentligste fund for det pågældende kapitel. Risikovurderingens hovedfund er opsummeret nedenfor.

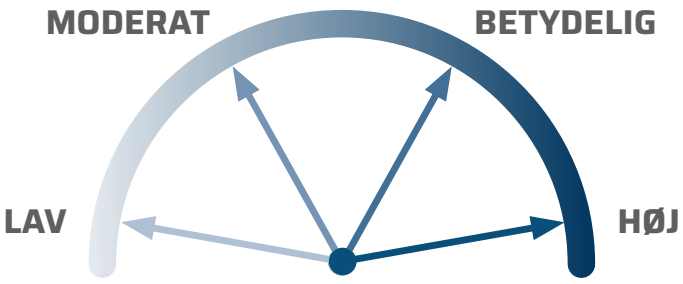
Truslen relateret til terrorfinansiering

PET vurderer med udgangspunkt i Center for Terroranalyses (CTA's) seneste Vurdering af terrortruslen mod Danmark fra marts 2023, at terrorfinansiering fra personer i Danmark primært tilgår militant islamistiske grupper i Syrien, Irak, Somalia og Tyrkiet samt i mindre grad Afghanistan, Libanon og Palæstina. Finansiering er med til at opretholde terrorgrupper og fremme deres virke, og tilførslen af finansielle ressourcer forbedrer gruppernes mulighed for at udføre operationer, rekruttere og fastholde medlemmer.

Sårbarheder relateret til terrorfinansiering

PET vurderer, at der er en række strukturelle sårbarheder relateret til terrorfinansiering, herunder mangelfuld viden og forståelse blandt de underretningspligtige virksomheder og personer, behov for yderligere deling af data og informationer mellem relevante aktører og brug for yderligere IT-understøttelse af datadeling. Hertil kommer, at flere underretningspligtige virksomheder og personer bør registrere sig, så de elektronisk kan underrette ved mistanke om hvidvask eller terrorfinansiering.

BAROMETER FOR VURDERING AF TERRORFINANSIERINGSRISIKOEN



Terrorfinansieringsrisikoen vurderes ud fra ovenstående risikobarometer, som henviser til risikoen for terrorfinansiering, der er et resultat af truslen relateret til terrorfinansiering og de finansielle sårbarheder og konsekvenser. Truslen er relativt ensartet for risikoområderne, mens der ses mere variation i sårbarhederne for de forskellige risikoområder. Eksempelvis i forhold til omkostninger, anonymitet og grænseoverskridende transaktioner.

Barometeret består af fire niveauer: Lav, moderat, betydelig og høj. Det er samme risikobarometer, som fremgår af Den Nationale Risikovurdering af Hvidvask.

Grønland og Færøerne

PET vurderer, at der er **lav** risiko for terrorfinansiering i Grønland og på Færøerne som følge af et minimalt trusselsniveau for terror.

Høj risiko for terrorfinansiering ved kryptoaktiver

PET vurderer, at der er **høj** risiko for, at kryptoaktiver bliver anvendt til terrorfinansiering. Anvendelse af kryptoaktiver er attraktivt i en terrorfinansieringssammenhæng, da der er efterspørgsel på transaktioner, der kan gennemføres hurtigt og uden geografiske begrænsninger.

Høj risiko for terrorfinansiering på nonprofit-området

PET vurderer, at risikoen for terrorfinansiering på nonprofit-området er **høj**. Det skyldes, at PET vurderer, at der er netværk i Danmark med evne og vilje til at fremskaffe midler gennem bl.a. indsamlinger til støtte for terrorbevægelser eller til støtte for terrorlignende aktiviteter.

Høj risiko for terrorfinansiering med kontanter og højværdivarer

PET vurderer, at risikoen for, at kontanter og højværdivarer bruges til terrorfinansiering, er **høj**. Kontanter og højværdivarer er attraktive i flere af terrorfinansieringens faser, og betalingsmidlerne er præget af lav opdagelsesrisiko og lave omkostninger.

Høj risiko for terrorfinansiering ved ulovlig pengeoverførselsvirksomhed

PET vurderer, at risikoen for terrorfinansiering ved ulovlig pengeoverførselsvirksomhed er **høj**. Ulovlig pengeoverførselsvirksomhed er en af de eneste muligheder for at få penge ind i konfliktzoner, og området rummer flere centrale sårbarheder.

Høj risiko for terrorfinansiering ved autoriseret pengeoverførselsvirksomhed

PET vurderer, at der er høj risiko for, at autoriseret pengeoverførselsvirksomhed misbruges til terrorfinansiering. Risikoen for terrorfinansiering er **høj**, idet pengeoverførselsvirksomheder typisk kan transportere midler tættere på konfliktzoner og med lavere omkostninger end bankerne.

Betydelig risiko for terrorfinansiering ved pengeinstitutter

PET vurderer, at der er en **betydelig** risiko for, at pengeinstitutter bliver anvendt til terrorfinansiering.

Pengeinstitutternes ydelser er lettilgængelige og kan anvendes til alle terrorfinansieringens faser. Samtidig har pengeinstitutterne generelt integreret en række mitigerende handlinger og investeret både i tekniske og menneskelige ressourcer.

Betydelig risiko for terrorfinansiering fra organiseret økonomisk kriminalitet

PET vurderer, at risikoen for terrorfinansiering baseret på indtægter fra organiseret økonomisk kriminalitet er **betydelig**. Det skyldes, at der kan være ekstremistiske sympatier i de kriminelle netværk, og at professionaliseret økonomisk kriminalitet indeholder elementer af anonymitet og grænseoverskridende transaktioner, store beløb og en accept af finansielle omkostninger.

Betydelig risiko for terrorfinansiering ved identitetsmisbrug og afledt kriminalitet

PET vurderer, at identitetsmisbrug og afledt kriminalitet udgør en **betydelig** risiko for terrorfinansiering. Området er attraktivt til fremskaffelse af ulovlige midler, og opdagelsesrisikoen kan være reduceret, fordi kriminaliteten kan ligne legale forhold, idet der anvendes ægte digitale identiteter.

Moderat risiko for terrorfinansiering ved socialt bedrageri

PET vurderer, at der er **moderat** risiko for, at socialt bedrageri bliver anvendt til terrorfinansiering. Socialt bedrageri vurderes som værende attraktivt blandt personer i ekstremistiske miljøer, men både myndigheders og underretningspligtige virksomheder og personers betydelige fokus på truslen vurderes at reducere risikoen. ■


4375

02

Terrorfinansiering

Terrorfinansiering forstås som aktiviteter, hvor formålet er økonomisk støtte til en person, en gruppe eller en sammenslutning, der har til hensigt at begå terrorhandlinger. Aktiviteter relateret til terrorfinansiering kan deles op i fire faser[1]:

- Fremskaffelse af midler gennem eksempelvis lovlig indkomst, indsamlinger eller kriminelle aktiviteter
- Opbevaring af midlerne
- Overførsel af midlerne til modtagere i eksempelvis udlandet
- Den konkrete anvendelse af midlerne til terrorrelaterede aktiviteter.

Omfanget af terrorfinansiering i Danmark har historisk været vanskeligt at fastslå, hvilket fortsat vurderes at være tilfældet. PET vurderer, at det økonomiske omfang af terrorfinansiering i Danmark ikke er sammenligneligt med hvidvask, idet terrorfinansiering beløbsmæssigt er mindre.

Der ses i Norden relativt få domme for terrorfinansiering, men der har i Danmark i perioden fra 1. januar 2019 til 1. oktober 2022 været rejst sigtelse for overtrædelse af straffelovens §114 b i fem sager, hvor i alt 13 personer er blevet sigtet.

Det kan være vanskeligt at dokumentere, og dermed bevise, de finansielle spor gennem eller til jurisdiktioner langt uden for Danmark, ligesom det direkte forsæt til terrorfinansiering også kan være vanskeligt at bevise.

PET har et betydeligt efterretningsmæssigt udbytte af hvidvaskunderretninger med mistanke om terrorfinansiering, idet de både bidrager til det generelle efterretningsbillede, men også til PET's konkrete viden om både kendte aktører, og personer og miljøer som ikke i forvejen er kendt af PET.

Der er ingen minimumsgrænse for, hvornår det er relevant at underrette ved mistanke om terrorfinansiering. Ofte vil terrorfinansiering være mindre beløb end ved hvidvask og dermed også ofte finde sted i mindre komplekse konstruktioner end ved eksempelvis fakturafabrikker og handelsbaseret hvidvask. I forhold til beløbsstørrelser vurderer PET, at sagen fra 2016 vedrørende PKK og sagen fra 2022 vedrørende Arab Struggle Movement for the Liberation of Ahwaz (ASMLA), der begge vedrørte tocifrede millionbeløb, ligger beløbsmæssigt højt i forhold til terrorfinansieringsområdet generelt. ASMLA-sagen beskrives yderligere senere.

Midlerne til terrorfinansiering kan være fremskaffet på både lovlig og ulovlig vis. Midlerne kan endvidere skifte mellem at fremstå lovlige og ulovlige flere gange på vej til sin endelige destination. Der kan således både være tale om, at penge sortvaskes, hvilket vil sige, at legalt optjente midler benyttes til finansiering af et ulovligt formål eller på anden vis føres fra lovligt til ulovligt regi, eller at midlerne kommer fra en eller flere kriminelle handlinger og benyttes til finansiering af terrorisme.

Den konkrete anvendelse af midlerne kan udmønte sig i angrebsfinansiering og/eller organisationsfinansiering. Overordnet set vil der i forhold til angrebsfinansiering typisk være tale om én eller få personer, der forbereder angreb og har omkostninger svarende til den igangværende operative opgave. Mens der for organisationsfinansiering typisk vil være tale om en mere langsigtet organisering, hvor der er faste strukturer for indtægter og omkostninger, og hvor det organisatoriske kan minde om en større virksomheds- eller foreningsstruktur.

1) *PET har af formidlingshensyn valgt en fire-fasemodel.*
Se mere om faseinddeling i Davis (2021): Illicit Money: Financing Terrorism in the 21st Century, s. 5.

ANGREBSFINANSIERING	ORGANISATIONSFINANSIERING
Husleje og udgifter til overnatning	Propaganda og rekruttering
Omkostninger til kommunikation som telefoner, taletidskort, internet	Efterretningsvirksomhed og operativ sikkerhed
Køb af våben, eksplosiver og komponenter	Sociale forhold, løn, støtte og understøttelse
Køb af operativt udstyr	Korruption og politisk lobbyisme
Billeje og transportomkostninger	Finansiering af angreb og celler
Øvrige leveomkostninger.	Støtte til andre terrororganisationer.

Terrorfinansiering er desuden karakteriseret ved, at der normalt er tale om en lineær proces, hvor midler anskaffes og transporteres videre i en kæde fra anskaffelse til slutbruger. Dette står i modsætning til hvidvask, hvor der typisk er tale om en cirkulær proces, hvor de kriminelle midler forskydes og hvidvaskes og returnerer til samme kriminelle person.

Der er debat om, hvorvidt nye teknologier vil forandre terrorfinansiering i en markant og stærkt bekymrende retning, eller om de nye teknologier ikke repræsenterer en øget risiko[2]. PET vurderer, at terrorfinansiering er præget af traditionelle metoder og adfærd, men samtidigt er suppleret af nye teknologiske muligheder for både de fremskaffelse, opbevaring og overførsel af midler. Vurderingen deles af forskere fra det EU-støttede Project CRAAFT[3], der skriver følgende om organisationsfinansiering: *"...there are few indications that new technologies have displaced older techniques, such as MSB's, hawala and cash couriering, which continue to dominate the scene. What appears to be the case is the use of old and new methods together, in pragmatic combinations that suit the terrorist financiers."*[4]

Metode til vurdering af terrorfinansieringsrisiko

FATF definerer risiko for terrorfinansiering som en funktion af trusler, sårbarheder og konsekvenser relateret til terrorfinansiering

Financial Actions Task Force (FATF) er en international organisation, der arbejder med bekæmpelse af hvidvask, terrorfinansiering og proliferationsfinansiering (finansiering af spredning af masseødelæggelsesvåben). FATF har vedtaget 40 konkrete anbefalinger for, hvilke tekniske foranstaltninger medlemslandene skal have på plads, og har derudover vedtaget 11 forskellige effektivitetskriterier, som fokuserer på, i hvilket omfang medlemslandene formår at reducere risiko og trusler i relation til hvidvask, terrorfinansiering og proliferationsfinansiering. Mere end 200 jurisdiktioner har på verdensplan tilsluttet sig FATF's arbejde.

Ved truslen relateret til terrorfinansiering forstås personer eller organisationer, der har et ønske om at finansiere terrorangreb eller terrororganisationer. I en strafferetlig kontekst er det truslen om, at personer eller organisationer vil gennemføre terrorfinansiering, jf. straffelovens § 114 b.

2) *Se fx Reimer & Redhead (2022): Bit by Bit – Impacts of New Technologies on Terrorism Financing Risks, s. 11.*
3) *Project CRAAFT is an academic research and community-building initiative designed to build stronger, more coordinated counter terrorist financing (CTF) capacity across the EU and in its neighbourhood. The project engages with authorities and private entities in order to promote cross-border connectivity and targeted research. Project CRAAFT.*
4) *Reimer & Redhead (2022): Bit by Bit – Impacts of New Technologies on Terrorism Financing Risks, s. 37. Se også Davis, Jessica (2022): New Technologies but Old Methods in Terrorism Financing, s. 9.37.*

FATF definerer sårbarheder således: *"The concept of TF vulnerability comprises of those things that can be exploited by the threat or that may support or facilitate its activities. Vulnerabilities may include features of a particular sector, a financial product or type of service that makes them attractive for TF".*[5] En sårbarhed eller en svaghed er i forlængelse heraf noget, som en eventuel trussel kan udnytte eller som kan facilitere eller understøtte aktiviteter relateret til truslen. Sårbarhederne kan være strukturelle, der skyldes svagheder i selve reguleringen eller lovgivningen af et område (der gør det attraktivt at finansiere aktiviteter fra det pågældende land). Sårbarhederne kan også være specifikke for risikoområder, der kan være afgrænset ved brancher eller særlige finansielle produkter og serviceydelser.

Som eksempel på sammenhængen mellem trusler og sårbarheder relateret til terrorfinansiering, så betød den stigende terrorfinansieringstrussel i forbindelse med konflikten i Syrien og Irak, at terrorfinansieringssårbarhederne relateret specifikt til udenlandske overførsler blev aktuelle, idet disse kunne sikre overførsler til konfliktzoner eller nabolande som Tyrkiet, Irak og Libanon.

Teoretisk er der ofte et overlap mellem sårbarheder relateret til hvidvask og terrorfinansiering, og det er også tilfældet i Danmark. Læserne af denne risikovurdering bør også orientere sig i kapitlet "Sårbarheder i den danske hvidvaskindsats" i Den Nationale Risikovurdering af Hvidvask, der er udgivet i januar 2023.

Konsekvenser henviser til situationer, hvor terrorfinansiering gennemføres og dermed muliggør terror. Konsekvenserne ved terrorfinansiering er, sammenlignet med hvidvask, oftest mere fatale, og kan konkret være tab af menneskeliv, tilskadekomne eller beskadigelse af kritisk infrastruktur, men omfatter også mere strukturelle konsekvenser for samfundsordenen og demokratiet.

Kompleksiteten ved at vurdere terrorfinansieringsrisici er høj, da terrortruslen kan være en indenrigstrussel og/eller en udenrigstrussel. Det illustrerer byretsdommen fra marts 2022 vedrørende ASMLA. Her blev tre personer bl.a. dømt for at finansiere og forsøge at finansiere terrorisme ved at have anskaffet 15 mio. kr. og have forsøgt at anskaffe mindst 15 mio. kr. fra en saudiarabisk efterretningstjeneste til ASMLA og dens væbnede fløj Martyr Muhyiddin Al-Nasser Brigaden i Iran[6]. Terrortruslen i

5) *FATF(2019): Terrorist Financing Risk Assessment Guidance 2019, s. 8.*

6) *Retten i Roskilde (2022): Dom i straffesag mod tre medlemmer af ASMLA. Domstol.dk*

ASMLA-sagen var mod Iran, men dele af netværket, der udførte finansieringen, var lokaliseret i Danmark. Pengene, der blev forsøgt fremskaffet, var fra den saudiarabiske efterretningstjeneste. Det bemærkes, at dommen er anket til landsretten, som forventes at behandle sagen i løbet af 2023.

Når PET i kapitlerne 7-16 vurderer, at et risikoområde har et givent risikoniveau, betyder det ikke, at fx alle underretningspligtige, der fungerer som udbydere inden for det pågældende område, har samme risikoniveau. Ofte kan risici variere betydeligt afhængigt af virksomhedens produkter, kunder, geografiske tilhørsforhold mv. De underretningspligtige virksomheder og personer skal i deres egen risikovurdering vurdere deres forretningsmodeller, produkter, kundesegmenter mv. og dermed den specifikke risiko.

Underretningspligtige virksomheder og personer opfordres i høj grad til at arbejde hypotesebaseret, når de undersøger risikoen for hvidvask eller terrorfinansiering i konkrete sager. Det vil sige, at når den underretningspligtige virksomhed eller person konstaterer et mistænkeligt forhold, eksempelvis en kundehenvendelse eller i transaktionsmonitoreringen, så behandles mistanken ud fra forskellige mulige hypoteser. Det vurderes, om der fx kan være tale om handelsbaseret hvidvask, terrorfinansiering, legale forhold, bedrageri, handel med narkotika eller noget helt andet. Og de forskellige hypoteser styrkes eller svækkes med den til rådighed stående data og eventuelle nye indhentede oplysninger. Risikovurderingens metodik kan i den forbindelse bruges som grundlag, når der opstilles hypoteser for, hvad den konkrete mistanke kan vedrøre

PET har igangsat en række fortløbende forebyggende aktiviteter, herunder undervisning, foredrag, awareness og uddannelsesaktiviteter, og risikovurderingen vil indgå centralt i det videre arbejde med at minimere risici forbundet med finansiering af terrorisme. Risikovurderingen af terrorfinansiering fungerer som et fundament for sådanne aktiviteter og for en kontinuerlig dialog med myndighederne, underretningspligtige virksomheder og personer samt forskningssektoren. ■

03

Kriminalisering af terrorfinansiering

I Danmark er terrorfinansiering kriminaliseret i straffelovens § 114 b, der har følgende ordlyd:
"Med fængsel indtil 12 år straffes den, som
1) direkte eller indirekte yder økonomisk støtte til eller,
2) direkte eller indirekte tilvejebringer eller indsamler midler til eller
3) direkte eller indirekte stiller penge, andre formuegoder eller finansielle eller andre lignende ydelser til rådighed for en person, en gruppe eller en sammenslutning, der begår eller har til hensigt at begå handlinger omfattet af § 114 eller § 114 a ".

Bestemmelsen har til formål at modvirke finansiering af terrorvirksomhed i form af økonomisk støtte eller formidling med videre til personer eller grupper, der begår eller har til hensigt at begå terrorisme eller terrorlignende handlinger:

- **§ 114 b, nr. 1,** retter sig mod den enkelte bidragsyder, der af egne midler giver økonomisk støtte til en person, gruppe eller sammenslutning, der begår eller har til hensigt at begå terror eller terrorlignende handlinger omfattet af straffelovens § 114 eller 114 a.

- **§ 114 b, nr. 2**, retter sig mod den mellemmand eller formidlingsorganisation, der indsamler eller på anden måde tilvejebringer midler, fx ved at skaffe lån til en sådan person, gruppe eller sammenslutning, der begår eller har til hensigt at begå handlinger omfattet af § 114 eller § 114 a.

- **§ 114 b, nr. 3**, retter sig mod pengeinstitutter og andre, der i erhvervsmæssig sammenhæng eller på anden måde med henblik på at opnå fortjeneste yder lån eller stiller andre finansielle ydelser til rådighed eller formidler sådanne ydelser til terrorgrupper.

Straffelovens § 114 b er subsidiær i forhold til det egentlige medvirkensansvar efter straffelovens §§ 114 eller 114 a, jf. § 23.

Det er forudsat i forarbejderne til bestemmelsen, at det ikke kun er strafbart at stille midler eller finansielle tjenesteydelser til rådighed for en terrorgruppes ulovlige aktiviteter, men også for gruppens lovlige aktiviteter. Dette forudsætter dog, at der er forsæt med hensyn til, at gruppen har terrorvirksomhed mv. som en del af sine aktiviteter eller formål. Der stilles ikke krav om, at pengene eller tjenesteydelserne direkte overdrages eller stilles til rådighed for gruppen, men alene at det i sidste ende er gruppen, der skal drage fordel heraf.

Efterforsknings- og straffesagskæde

En terrorfinansieringssag kan starte på forskellig vis. Eksempelvis på baggrund af en underretning om mistanke om terrorfinansiering, som PET indledende har visiteret og fundet relevant. PET efterforsker derefter sagen, hvorefter der kan rejses sigtelse og endeligt tiltale.

PET's visitering og indledende efterforskning

Det følger af PET-lovens § 1, stk. 1, nr. 1, at PET bl.a. har til opgave at forebygge, efterforske og modvirke forbrydelser mod statens selvstændighed og sikkerhed samt forbrydelser mod statsforfatningen og de øverste statsmyndigheder mv., jf. straffelovens kapitel 12 og 13. Det fremgår videre af PET-lovens § 6, at PET's efterforskning

og tvangsindgreb (som fx telefonaflytning, ransagning, beslaglæggelse mv.) reguleres af de almindelige regler i retsplejeloven, som også gælder for det øvrige politi. Retsplejeloven indeholder dog på enkelte områder nogle særlige regler for efterforskning af de forbrydelser, der er omfattet af straffelovens kapitel 12 og 13.

Efterforskning af mulige forbrydelser omfattet af straffelovens kapitel 12 og 13 (herunder § 114 b om terrorfinansiering) varetages som udgangspunkt af PET. Hvis PET beslutter, at der skal indledes efterforskning, kan PET efter forelæggelse for statsadvokaten i særlige tilfælde indgå aftale med den pågældende politikreds om, at politikredsen efterforsker sagen i samarbejde med PET.

Sigtelse

Det er PET, som i første række vurderer, om der er grundlag for at rejse sigtelse for overtrædelse af én eller flere bestemmelser i straffelovens kapitel 12 og 13. I givet fald forelægger PET sagen for statsadvokaten. Hvis statsadvokaten er enig i, at der skal rejses sigtelse i sagen, orienterer statsadvokaten Rigsadvokaten om sagen.

Når sigtelse er rejst, gennemføres den videre efterforskning af den pågældende politikreds i samarbejde med PET.

PET skal endvidere orienteres i alle tilfælde, hvor en politikreds overvejer at indlede en efterforskning mod en person, der mistænkes for overtrædelse af straffelovens § 136 med hensyn til forbrydelser omfattet af straffelovens kapitel 12 eller 13.

Det bemærkes i øvrigt, at også National enhed for Særlig Kriminalitet (NSK) giver PET oplysninger, som NSK måtte have om mulige overtrædelser af straffelovens kapitel 12 eller 13. Dette kan dreje sig om oplysninger modtaget på baggrund af hvidvaskloven eller på anden vis. Eventuelle efterforskninger på baggrund af sådanne oplysninger skal behandles på samme måde som andre efterforskninger af mulige forbrydelser omfattet af straffelovens kapitel 12 og 13.

Afgørelse af tiltalespørgsmålet mv.

Hvis statsadvokaten vurderer, at der skal rejses tiltale for overtrædelser af bestemmelser i straffelovens kapitel 12 og 13, forelægger statsadvokaten sagen for Rigsadvokaten, der i givet fald forelægger sagen for justitsministeren med indstilling om, at der rejses tiltale i sagen. Såfremt justitsministeren tiltræder Rigsadvokatens indstilling, kan der rejses tiltale.

Der henvises i øvrigt til Rigsadvokatens brev af 27. marts 2015, hvor de nærmere retningslinjer for samarbejdet mellem politikredsene, PET og statsadvokaten er beskrevet[7]. ■

7) *Kapitel 3 er baseret på Rigsadvokatens meddelelse (2022): Forelæggelse og indberetning mv.*

04

Trusler relateret til terrorfinansiering

Sammenfatning

PET vurderer med udgangspunkt i Center for Terroranalyses (CTA's) seneste Vurdering af terrortruslen mod Danmark fra marts 2023, at terrorfinansiering fra personer i Danmark primært tilgår militant islamistiske grupper i Syrien, Irak, Somalia og Tyrkiet samt i mindre grad Afghanistan, Libanon og Palæstina. Finansiering er med til at opretholde terrorgrupper og fremme deres virke, og tilførslen af finansielle ressourcer forbedrer gruppernes mulighed for at udføre operationer, rekruttere og fastholde medlemmer.

Ser man på trusselsbilledet for terrorfinansiering baseret på de mange underretninger om terrorfinansiering fremgår det, at de typiske beløbsstørrelser for terrorfinansieringsunderretninger er i størrelsesordenen 0-5000 kroner. Her fremgår det også, at hovedparten af underretningerne vedrører transaktioner inden for Danmark.

Militant islamisme og terrorfinansiering

PET definerer militant islamisme som en fortolkning af islamistisk ideologi, der legitimerer anvendelse af vold for at opnå politiske, religiøse eller ideologiske mål.

CTA vurderer i Vurdering af terrortruslen mod Danmark fra marts 2023, at terrortruslen fra militante islamister mod Danmark er i niveauet alvorlig. Trusselsbilledet er fortsat præget af tilstedeværelsen af militant islamistiske sympatisører i Danmark, som kan have intention om at begå terrorhandlinger i Danmark, og som finder inspiration hos transnationale militant islamistiske grupper som Islamisk Stat og al-Qaida. Det mest sandsynlige militant islamistiske terrorangreb i Danmark er et angreb, der udføres af en soloterrorist eller en mindre gruppe med lettilgængelige midler, skydevåben eller hjemmelavede bomber[8].

I Vurdering af terrortruslen mod Danmark fra marts 2023 vurderer CTA endvidere, at terrorfinansiering fra personer i Danmark primært tilgår militant islamistiske grupper i Syrien, Irak, Somalia og Tyrkiet samt i mindre grad Afghanistan, Libanon og Palæstina. Finansiering er med til at opretholde terrorgrupper og fremme deres virke, og tilførslen af finansielle ressourcer forbedrer gruppernes mulighed for at udføre operationer, rekruttere og fastholde medlemmer[9].

I Danmark er der de seneste år faldet dom i flere sager, hvor personerne er blevet dømt efter straffelovens bestemmelser om finansiel støtte til terrorisme. Fælles for sagerne er, at terrorfinansieringen foregik ved at overføre midler for at understøtte specifikke enkeltpersoner og mindre personnetværk. I november 2022 blev fire personer dømt for bl.a. terrorfinansiering ved at have overført adskillige beløb til to danske udrejste, der havde tilsluttet sig Islamisk Stat i Syrien/Irak i perioden fra 2013 til 2017[10].

8) *CTA (2023): Vurdering af terrortruslen mod Danmark, s. 8.*
9) *CTA (2023): Vurdering af terrortruslen mod Danmark, s. 15.*
10) *CTA (2023): Vurdering af terrortruslen mod Danmark, s. 15-16.*

I relation til mistanke om terrorfinansiering havde myndighederne tidligere fokus på finansiel adfærd og finansielle spor frem mod udrejse til en konfliktzone. Eksempelvis situationer, hvor en eller flere personer realiserede flest mulige likvide midler, optog flere samtidige online-forbrugslån eller overdrog sine identitetspapirer. Opmærksomheden skete på baggrund af, at mindst 161 voksne personer i perioden 2012-2016 udrejste til konfliktzonen i Syrien og Irak for at tilslutte sig militant islamistiske grupper[11].

Ifølge Vurdering af terrortruslen mod Danmark fra marts 2023 er der dog ingen personer, der er udrejst fra Danmark til konfliktzonen i Syrien/Irak siden 2016[12]. PET vurderer på nuværende tidspunkt, at truslen for terrorfinansiering i forbindelse med forestående udrejse til en konfliktzone er væsentligt reduceret.

Højreekstremisme og terrorfinansiering

PET definerer højreekstremisme som en fællesbetegnelse for forskellige politiske holdninger, der ligger yderst til højre i det politiske spektrum, og som kendetegnes ved kombinationer af nationalistiske, autoritære, anarkistiske, anti-parlamentariske, racistiske, xenofobiske og antisemitiske standpunkter. Det ideologiske grundlag for højreekstremisme kan stamme fra nazisme og fascisme såvel som national-konservatisme. Højreekstremister sætter spørgsmålstegn ved eller afviser demokrati og anser anvendelse af vold som et legitimt middel til at opnå politiske mål.

For så vidt angår højreekstremisme, opjusterede CTA terrortruslen i marts 2021 fra begrænset til generel, hvorefter denne trusselsvurdering blev fastholdt i den seneste Vurdering af terrortruslen mod Danmark fra marts 2023.

Underretninger om terrorfinansiering

Fra Hvidvasksekretariatet modtager PET som kompetent myndighed på terrorfinansieringsområdet alle underretninger med mistanke om terrorfinansiering fra underretningspligtige virksomheder og personer, der underretter jf. hvidvasklovens § 26. Underretningerne indgår i det samlede trussels- og risikobillede for terrorfinansiering, men bærer samtidig præg af, at de underretningspligtige virksomheder og personer har en varieret forståelse af risikobilledet for terrorfinansiering, hvilket gør, at underretningerne spænder forholdsvist vidt i forhold til mistankegrundlag og indhold i øvrigt. PET visiterer og vurderer alle indkomne underretninger, som Hvidvasksekretariatet modtager fra de underretningspligtige virksomheder og personer.

PET's vurderinger på baggrund af underretninger med mistanke om terrorfinansiering er underbygget af PET's øvrige kilder, herunder nationale og internationale efterretninger, efterforskninger af terrorfinansiering, kvalitative og kvantitative undersøgelser mv.

PET vurderer, at der ikke bør være en nedre beløbsgrænse for underretning om mistanke om terrorfinansiering, da selv små beløb kan have betydning for terrorangreb.

11) *Se også Politiet/Politiets Sikkerhedstjeneste (2022): Nasjonal risikovurdering Hvitvaskning og terrorfinansiering, s. 73.*

12) *CTA (2023): Vurdering af terrortruslen mod Danmark, s. 13.*

Denne vurdering underbygges af PET's seneste dataanalyse af underretninger fra Hvidvasksekretariatet. Ser man på underretninger i perioden fra sommeren 2020[13] til udgangen af 2021 står det klart, at de typiske beløbsstørrelser for terrorfinansieringsunderretninger er i størrelsesordenen 0-5000 kroner. PET oplever, at underretninger med mindre beløb kan have betydelig efterretnings- og efterforskningsmæssig værdi og altså bidrage til både analyser, efterretningsprodukter og konkrete strafferetlige efterforskninger.

Af samme datagrundlag ses tydeligt, at hovedparten af underretningerne vedrører transaktioner inden for Danmark. PET vurderer, at det hænger sammen med, at banker og pengeinstitutter udgør den klart største kilde til underretninger, og at vægtningen ville forskydes, hvis eksempelvis pengeoverførselsvirksomheder underrettede mere, fordi banker og pengeinstitutter i langt ringere omfang er involveret i overførsler til højrisikoområder.

En gennemgang af de underretninger, der vedrører overførsler til udlandet, har vist, at kvaliteten af underretningerne er høj. Det vil sige, at underretninger er relevante og har et godt beskrevet og velunderbygget mistankegrundlag. En betydelig mængde af transaktioner går til forventede destinationslande som fx Tyrkiet og Djibouti, der fungerer som transitlande til lande som bl.a. Syrien og Somalia. Den geografiske spredning underbygger trusselsvurderingen for terrorfinansiering af militant islamisme. ■

13) *PET og Hvidvasksekretariatet indgik i sommeren 2020 en ny aftale om videregivelseskriterier, hvorfor denne tidsmæssige afgrænsning er foretaget.*

05

Sårbarheder relateret til terrorfinansiering

Sammenfatning

PET vurderer, at der er en række strukturelle sårbarheder, som er relevante for både hvidvask og terrorfinansiering, herunder mangelfuld viden og forståelse blandt de underretningspligtige virksomheder og personer, behov for yderligere deling af data og informationer mellem relevante aktører og brug for yderligere IT-understøttelse af datadeling. Hertil kommer at flere underretningspligtige virksomheder og personer bør registrere sig, så de elektronisk kan underrette ved mistanke om hvidvask eller terrorfinansiering. PET vurderer, at det er en sårbarhed, at fasen for overførsel af midler til terrorfinansiering er underrepræsenteret i underretningerne, fordi eksempelvis pengeoverførselsvirksomhederne ikke underretter i tilstrækkeligt omfang.

Strukturelle sårbarheder

Terrorfinansiering og hvidvask har en række centrale strukturelle sårbarheder til fælles, som adresseres i den seneste nationale strategi på området[14]:

Mangelfuld viden og forståelse er en sårbarhed hos både myndigheder, brancheorganisationer og underretningspligtige virksomheder og personer. I forhold til at modvirke truslen fra terrorfinansiering er det afgørende, at alle arbejder risikobaseret og har et retvisende billede af trusserne og risici. Ikke mindst blandt de underretningspligtige virksomheder, der ofte udgør det første værn mod terrorfinansiering. PET vurderer, at de finansielle institutioner de senere år har opnået en stærkere risikoforståelse end de ikke-finansielle brancher, og at den knytter sig til såvel forståelsen af kriminelle aktører og risici. En vurdering, der i øvrigt deles af Hvidvasksekretariatet[15].

Det er fortsat en sårbarhed, at deling af data og informationer påvirkes af forskellige regelsæt blandt myndighederne. Konsekvensen er, at retshåndhævende og administrative myndigheder samt tilsynsmyndigheder ikke uhindret kan dele oplysninger, der tjener til bekæmpelse af hvidvask og terrorfinansiering. Hertil kommer, at de underretningspligtige ikke har mulighed for at dele oplysninger med hinanden om specifikke aktører. For eksempel kan et pengeinstitut på nuværende tidspunkt ikke dele viden ved mistanke om terrorfinansiering med et andet pengeinstitut, når en kunde forsøger at etablere sig som kunde i det nye pengeinstitut.
Denne sårbarhed relaterer sig også til IT-understøttelse af myndighedernes AML-/CFT-indsats, hvor behovet for automatiseret datadeling og søgning i fælles systemer er stigende. Terrorfinansierings- og hvidvaskområdet er præget af betydelige mængder data og sager, eksempelvis modtog Hvidvasksekretariatet ca. 90.000 hvid-

14) *Regeringen (2022): National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025.*
15) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 04.4.*

vaskunderretninger i 2022, og derfor fordrer en hensigtsmæssig sagsbehandling, at data og informationer kan indhentes automatisk.

Som det fremgår af National Risikovurdering af Hvidvask, har kun ca. 10 % af de underretningspligtige virksomheder og personer oprettet sig i goAML (IT-platform anvendt af Hvidvasksekretariatet til at modtage underretninger), hvilket gør dem i stand til at underrette om hvidvask og terrorfinansiering[16]. De underretningspligtige er ikke forpligtet til at være oprettet i goAML, men det er en forudsætning for at kunne underrette, da det som udgangspunkt ikke er muligt at underrette ad andre kommunikationskanaler. Det udgør naturligt en sårbarhed på terrorfinansieringsområdet, at så mange underretningspligtige virksomheder og personer ikke kan underrette. Det gør sig i særdeleshed gældende for underretningspligtige virksomheder og personer uden for den finansielle sektor.

Som det fremgår af kapitlet omkring Trusler for terrorfinansiering, har disse ofte tilknytning til geografiske områder, der har svage mekanismer til bekæmpelse af terrorfinansiering og hvidvask, og hvor banker og i visse tilfælde også pengeoverførselsvirksomheder kan have svært ved at være til stede. Det betyder, at mulighederne for at gennemskue og dokumentere pengesporene forringes, og at danske myndigheders juridiske værktøjer til indhentning af informationer begrænses.

Over- og underrepræsentation i underretninger om terrorfinansiering

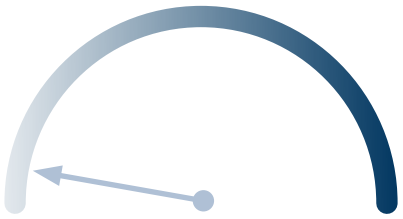
Pengeinstitutterne stod i 2021 for en meget betydelig del af underretningerne om terrorfinansiering, hvorimod PET modtog relativt få underretninger fra pengeoverførselsvirksomheder.

PET vurderer, at det er en sårbarhed, at underretninger vedrørende overførsler til udlandet er underrepræsenteret i underretningerne, fordi eksempelvis pengeoverførselsvirksomhederne ikke underretter i tilstrækkeligt omfang. At størstedelen af de modtagne hvidvaskunderretninger vedrører overførsler inden for Danmark, står i kontrast til PET's vurdering af, at terrorfinansiering fra personer i Danmark primært tilgår militant islamistiske grupper i Syrien, Irak, Somalia, Libanon, Afghanistan og Palæstina. PET vurderer, at dette formentlig skyldes flere forhold – eksempelvis at bankerne kun i meget begrænset omfang gennemfører transaktioner til højrisikolande, men også at en række andre underretningspligtige ikke underretter i det omfang, deres risikoprofil umiddelbart tilsiger. ■

16) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 04.3.*

06

Grønland og Færøerne



Sammenfatning

PET vurderer, at der er **lav** risiko for terrorfinansiering i Grønland og på Færøerne som følge af et minimalt trusselsniveau for terror. Både i Grønland og på Færøerne er der sårbarheder med hensyn til terrorfinansiering, men da truslen er minimal, er betydningen af disse fortsat begrænset.

Det følger af Vurdering af terrortruslen mod Danmark fra marts 2023, at terrortruslen mod Grønland er i niveauet minimal. Det betyder i henhold til PET's definitioner, at der ikke er nogen indikationer på en trussel: Hensigt, kapacitet eller begge dele er ikke erkendt. CTA vurderer, at voldelig ekstremisme er mindre udbredt i Grønland. Ekstremistisk propaganda kan dog også påvirke personer i Grønland til at begå voldelige handlinger. Socialt marginaliserede og sårbare unge kan være særligt modtagelige over for radikalisering.

PET vurderer, at risikoen for terrorfinansiering i væsentlig grad er påvirket af, at terrortruslen i Grønland er minimal, hvorfor trusselsniveauet reducerer den risikomæssige betydning af sårbarhederne. PET har gennemført en grundig kortlægning af sårbarheder i den grønlandske finansielle infrastruktur i samarbejde med Hvidvasksekretariatet. I den forbindelse henvises der til National Risikovurdering af Hvidvask, der indeholder et fyldestgørende kapitel om Grønland, der også kan danne grundlag for risikoarbejdet i relation til terrorfinansiering.

Størrelsen af det grønlandske samfund indebærer en sårbarhed i forhold til risiko for interessekonflikter eller -sammenfald mellem nærtstående personer. Risikoen er eksempelvis til stede, når en medarbejder skal gennemføre kundekendskabsprocedurer eller undersøge mistænkelige forhold vedrørende en kunde, som medarbejderen i forvejen kender i anden sammenhæng. Det er ligeledes en relevant sårbarhed, at Grønland er et mere kontantintensivt samfund, hvilket indebærer større muligheder for at indsamle eller overføre penge til terrorformål uden at blive opdaget. Håndteringen af udenlandske virksomhedsstrukturer vurderes at udgøre en sårbarhed i forhold til mulighederne for at identificere reelle ejere.

CTA vurderer også, at terrortruslen mod Færøerne er i niveauet minimal. CTA vurderer, at voldelig ekstremisme er mindre udbredt på Færøerne. Ekstremistisk propaganda kan påvirke personer på Færøerne eller tilrejsende til at begå voldelige handlinger. Dette kan være udløst af politiske enkeltsager som fx dyrevelfærd. Socialt marginaliserede og sårbare unge kan være særligt modtagelige over for radikalisering.

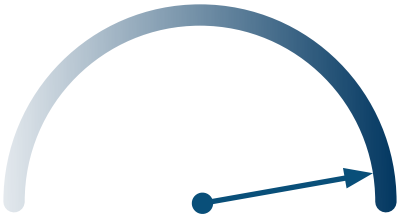
Som i Grønland har PET også gennemført en kortlægning af sårbarheder på Færøerne i samarbejde med Hvidvasksekretariatet. Der henvises til Hvidvasksekretariatets risikovurdering, hvor Færøerne behandles grundigt. I forhold til terrorfinansiering er især sårbarhederne omkring korrespondentbanker, kontroltryk hos Skráseting Føroya (bl.a. ansvarlig for det færøske virksomhedsregister) og reelle ejere samt forsinket implementering af dansk hvidvasklov relevante og bør tages i betragtning af såvel myndigheder som underretningspligtige. Disse sårbarheder bidrager til at muliggøre terrorfinansiering, men fordi trusselsniveauet er minimalt, bliver den samlede terrorfinansieringsrisiko **lav**. ■

07

Kryptoaktiver

Sammenfatning

PET vurderer, at der er **høj** risiko for, at kryptoaktiver bliver anvendt til terrorfinansiering. Anvendelse af kryptoaktiver er attraktivt i en terrorfinansieringssammenhæng, da der er efterspørgsel på transaktioner, der kan gennemføres hurtigt og uden geografiske begrænsninger. Samtidig er sløringsmekanismer og varierende global regulering og kontrol vigtige terrorfinansieringssårbarheder[17].



PET vurderer, at der er interesse for kryptoaktiver i danske netværk, der har ønske om at foretage terrorfinansiering. Risikoen for, at kryptoaktiver bliver anvendt til terrorfinansiering, er øget siden den seneste nationale risikovurdering af terrorfinansiering i Danmark, og truslen har manifesteret sig ved konkret interesse og brug. CTA vurderer, at Islamisk Stat i stigende grad vil forsøge at udnytte kryptovaluta til at tiltrække donationer[18].

Terrorfinansiering med kryptoaktiver har en høj terrorfinansieringsrisiko, da de kan anvendes både til opbevaring af værdier, overførsel af værdier til modtagere i udlandet og konkret anvendelse til terrorrelaterede aktiviteter[19]. Samtidigt har det været muligt at opnå en økonomisk gevinst – eller et tab – ved spekulation, da kursen på kryptoaktiver varierer.

Terrorfinansiering med kryptoaktiver er attraktivt, da der er tale om transaktioner, der kan gennemføres med meget høj hastighed og samtidigt kan være grænseoverskridende, da de kan gennemføres fra bruger til bruger (peer-to-peer) uafhængigt af, hvor brugerne kan befinde sig geografisk og uden brug af eksempelvis korrespondentbanker.

17) *EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 95-97.*

18) *CTA (2023): Vurdering af terrortruslen mod Danmark, s. 15.*

19) *Se også Politiet/Politiets Sikkerhedstjeneste (2022): Nasjonal risikovurdering Hvitvaskning og terrorfinansiering, s. 80.*

Terrorgrupper som Islamisk Stat og al-Qaida er i stand til at modtage overførsler med kryptoaktiver, og der er internationale eksempler på, at dette er sket. Der er fx åbnet kryptovaluta-vekselerer i den nordvestlige del af Syrien, som ud over lovlige formål bruges til at kanalisere penge til terrorgrupper. Vekselereren "BitcoinTransfer" i Idlib blev fx i august 2020 af det amerikanske justitsministerium sat i forbindelse med sager om terrorfinansiering[20].

Det har betydning for terrorfinansieringsrisikoen, hvorvidt det er brugeren selv, der har nøglen til sin wallet (non-custodial wallet), eller om det er en tredjepart, der har nøglen i sin varetægt på vegne af brugeren (custodial wallet). Risikoen er højere, når brugeren selv har nøglen til sin wallet (non-custodial wallet), da brugeren herved er sin egen bank. Udbydere af en custodial wallet er i Danmark omfattet af hvidvaskloven.

Der er en betydelig sammenhæng mellem kryptoaktiver og nonprofit-området. Kryptoaktiver gør terrorister og terrorgrupper i stand til i stigende grad at misbruge indsamlinger og crowdfunding[21], imens man samtidigt beholder en høj grad af hastighed og en vis grad af anonymitet for donorer og modtagere.

Der har internationalt været indikationer på et skift væk fra traditionelle pengeoverførselsvirksomheder til kryptoaktiver siden 2020, hvilket er intensiveret i 2021. Som eksempel har der i EU-medlemsstater været foretaget terrorfinansiering til brugere uden for EU ved hjælp af forudbetalte kryptokuponer med en værdi på mellem 50-250 EUR[22].

Kryptoaktiver har også betydning for pengeinstitutter og betalingstjenester. Forskellige kryptobørser tilbyder deres brugere at oprette et debetkort via aftale med fx Visa eller Mastercard, hvilket gør brugerne i stand til at foretage almindelige køb i anerkendte betalingsvalutaer såsom danske kroner eller amerikanske dollar.

Sporbarheden ved terrorfinansiering med kryptoaktiver varierer, afhængigt af hvordan transaktionen gennemføres. Sporbarheden er som udgangspunkt høj, når transaktionen foretages på blockchainen (on-chain) og dermed er dokumenteret og gennemført digitalt. Blockchain er den teknologi, der ligger bag kryptoaktiver som for eksempel Bitcoin. Blockchain kan beskrives som et "fælles register", hvor transaktioner, der foretages med kryptoaktiver mellem konto tilknyttet blockchainen, registre-

20) *Chainalysis (2020): Chainalysis Intelligence Brief: How Syria-based Cryptocurrency Exchange BitcoinTransfer Facilitated Terror Financing Campaigns.*

21) *Se også EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 54-57.*

22) *Europol (2022): Terrorism Situation and Trend Report (TE-SAT), side 19.*

res[23]. Omvendt er sporbarheden lav, når transaktionen gennemføres uden for blockchainen (off-chain), det vil sige, at transaktionen ikke gennemføres og dokumenteres digitalt, men alene er en aftale mellem to brugere, der indbyrdes aftaler dette. Det kan ske ved, at bruger A overdrager sin wallet til bruger B ved at oplyse sine hemmelige kodeord. Terrorfinansieringstruslen er derfor også højere, når transaktionerne gennemføres uden for blockchainen mellem to brugere, frem for når de gennemføres og dokumenteres digitalt på blockchainen.

Mixere kan også have betydning for sporbarheden. Mixere er en finansiel service, der slører blockchain-transaktioner ved at mixe fx forskellige kryptovalutaer.

Det er en væsentlig sårbarhed i forhold til kryptoaktiver, at efterforskningen af mistænkelige kryptotransaktioner kræver specialistkompetencer og potentielt udveksling af information mellem nationale og internationale myndigheder og virksomheder. Det har betydning for opdagelsesrisikoen og gør det attraktivt at anvende kryptoaktiver til opbevaring, transport og køb. Hvis en person med ønske om at foretage terrorfinansiering veksler fra kryptovaluta til fiat-valuta, vil det være attraktivt at vælge en børs i et land, hvor myndighedernes kontroltryk er lavt. Dette er et vigtigt opmærksomhedspunkt.

Det er en sårbarhed, at den teknologiske udvikling for kryptoaktiver går stærkt og stiller nye krav til regulering. Det er eksemplificeret ved privacy coins, der med et stort fokus på kryptering og anonymitet er blevet attraktive for kriminelle. Kryptoaktivet Monero er et eksempel på en privacy coin. Monero blev introduceret som kryptoaktiv i 2014 og blev fx først taget af den britiske kryptobørs Kraken i 2021.

Den finansielle regulering af kryptoaktiver har globalt set været svag siden teknologien kom frem. Gennemførelsen af EU's 5. hvidvaskdirektiv i Danmark[24] den 10. januar 2020 var første gang, at udbydere af veksling til kryptoaktiver og virtuelle tegnebøger blev omfattet af hvidvaskloven som underretningspligtige virksomheder.

Finanstilsynet fører hvidvask- og terrorfinansieringstilsyn med udbydere af virtuelle tegnebøger og veksling, men disse er endnu ikke underlagt et finansielt tilsyn fra de danske myndigheder, og det samme gælder handelstjenesterne. Dette vil imidlertid blive ændret, når den nye EU-forordning om markedet for kryptoaktiver (MiCA) bliver implementeret. Herved sikres det, at Finanstilsynet fremover vil kunne føre finansielt tilsyn med udbydere af virtuelle tegnebøger og veksling til kryptoaktiver. ■

23) *Finanstilsynet (2022): Blockchain-teknologi kan udgøre en effektiv infrastruktur til betalingstjenester, s. 2.*

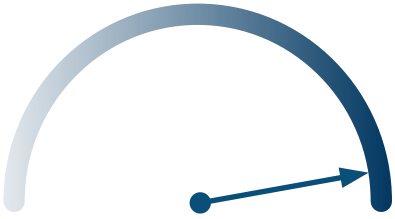
24) *LOV nr. 553 af 07.05.2019.*

08

Nonprofit-området

Sammenfatning

PET vurderer, at risikoen for terrorfinansiering på nonprofit-området er **høj**. Det skyldes, at PET vurderer, at der er netværk i Danmark med evne og vilje til at fremskaffe midler gennem bl.a. indsamlinger til støtte af terrorbevægelser eller støtte af terrorlignende aktiviteter. Samtidig er der på nonprofit-området en række sårbarheder, der gør området attraktivt til især fremskaffelse af midler, men også til overførsel af midler.



Risikoområdet dækker over hele nonprofit-området under temaerne foreninger, almennyttige fonde og indsamlinger. Både foreninger og almennyttige fonde kan virke som organisationsformer til brug for terrorfinansiering[25].

PET vurderer, at der generelt er en høj risiko for terrorfinansiering forbundet med nonprofit-området, og at truslen særligt er forbundet med fremskaffelsen af midler ved indsamlinger eller donationer. PET vurderer, at covid-19-restriktionerne i kombination med den digitale udvikling de senere år kan have fremmet online-indsamlinger frem for fysiske indsamlinger.

PET vurderer, at nonprofit-området muliggør terrorfinansiering ved både indsamlinger af mindre beløb til bestemte formål og ved en generel og mere vedvarende fremskaffelse af større beløb, der tilfalder terrororganisationer. Terrorgrupper kan nyde godt af donorer, men det er samtidigt en sårbar finansieringsmodel for en terrororganisation, hvis den er afhængig af ekstern finansiering alene[26]. PET vurderer derfor, at det er sandsynligt, at terrororganisationer i højere grad vil anvende nonprofit-området til at iværksætte mindre indsamlinger til konkrete formål frem for som kilde til egentlig organisationsfinansiering.

PET udgav i april 2020 en selvstændig risikovurdering af terrorfinansiering på nonprofit-området i Danmark, og den er i vid udstrækning fortsat aktuel. Finanstilsynet

25) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 04.7. om begrænset kontrol med ikke-erhvervsdrivende fonde.*

26) *Davis, Jessica (2021): Illicit Money: Financing Terrorism in the 21st Century, s. 13.*

har i oktober 2022 udgivet en vejledning til virksomheder omfattet af hvidvaskloven til vurdering af foreninger i forhold til risikoen for hvidvask og terrorfinansiering[27]. Begge udgivelser er helt centrale for forståelsen af risikofaktorer på nonprofit-området.

Som det fremgår af risikovurderingen på nonprofit-området, kan risikoen ved foreninger – og almennyttige fonde – antage forskellige former[28]. Organisationen kan være etableret med terrorfinansiering for øje, enten med eller uden medlemmers og donorers vidende og accept. Organisationen kan også være etableret og drevet med et legitimt formål, ofte nødhjælp, men med et sideløbende ulovligt formål, hvor midler eller genstande tilfalder terrorgrupper. I disse tilfælde vil udskillelsen til ulovlige formål ofte ske uden for Danmarks grænser og ikke nødvendigvis med hele organisationens vidende. Endelig kan der være risiko for uagtsom terrorfinansiering i de tilfælde, hvor en i øvrigt velmenende og veldrevet fond eller forening samarbejder med personer eller organisationer, der viser sig at være kriminelle[29]. Sidstnævnte situation understreger nødvendigheden af, at organisationer i Danmark har et betydeligt fokus på at vurdere og kontrollere sine lokale samarbejdspartnere.

Risikoprofilen for foreninger og almennyttige fonde varierer ganske betydeligt, og alle underretningspligtige virksomheder og personer bør have opmærksomhed herpå. PET henviser i den forbindelse til Finanstilsynets Vejledning til virksomheder omfattet af hvidvaskloven til vurdering af foreninger i forhold til risikoen for hvidvask og terrorfinansiering, der i vidt omfang også kan benyttes ved risikovurdering af almennyttige fonde. Det er vigtigt, at de underretningspligtige virksomheder og personer anlægger en risikobaseret vurdering, så ikke alle foreningskunder behandles ens. Foreninger som fx ejerforeninger, antenneforeninger og almene boligforeninger er som udgangspunkt forbundet med begrænset risiko, fordi de er karakteriseret ved et snævert afgrænset formål. I den anden ende af risikoskalaen er foreninger med manglende registrering, betydelige kontantaktiviteter, aktiviteter i konfliktzoner mv.

For så vidt angår foreninger og almennyttige fonde med øget risiko, bør de underretningspligtige virksomheder og personer have fokus på, om fondene indgår i atypiske organisatoriske sammenhænge med aktører som eksempelvis friskoler, moskéer eller enkeltmandsvirksomheder.

27) *Finanstilsynet (2022): Vejledning til virksomheder omfattet af hvidvaskloven til vurdering af foreninger i forhold til risikoen for hvidvask og terrorfinansiering. Finanstilsynet.dk.*

28) *PET (2020): National risikovurdering af terrorfinansiering på NPO-området i Danmark, s. 14.*

29) *EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 239.*

Der er i stigende grad international opmærksomhed rettet mod konsekvenserne af standarderne på hvidvaskområdet, og udelukkelse af kunder med høj risiko kan være en sådan konsekvens (de-risking). En forening eller fond kan have høj risiko af helt legitime årsager, og det udgør en sårbarhed, at sådanne kunder risikerer at blive ekskluderet fra de normale finansielle markeder[30].

Især til konfliktzoner og omkringliggende områder kan der være ringe legitime finansielle adgangsveje, hvilket kan friste eksempelvis danske nødhjælpsorganisationer til at benytte metoder som hawala[31] og kontanttransporter, der er kendetegnet ved højere risiko og ringere mulighed for tilsyn og kontrol.

Indsamlingsaktiviteter kan finde sted i regi af foreninger eller almennyttige fonde, men også uden for, og derfor behandles temaet selvstændigt her. Indsamling er en klassisk metode til at anskaffe midler eller genstande af værdi blandt ekstremistiske støttenetværk i Danmark. Overordnet kan man med fordel sondre mellem indsamling med og uden tilladelse fra Indsamlingsnævnet, hvilket de fleste indsamlingsformer kræver. Der er en række undtagelser, der fremgår af Indsamlingsnævnets hjemmeside. Indsamlingsnævnet, som er placeret under Civilstyrelsen, giver tilladelse til indsamlinger og fører kontrol med, at indsamlede midler anvendes til de formål, som indsamler har oplyst. Det er i den forbindelse centralt, at Civilstyrelsen har de fornødne muligheder for at indhente data til kontrol af indsamlers oplysninger.

I sager om indsamling bør man som underretningspligtig undersøge, om der foreligger indsamlingstilladelse, eller om indsamlingen er undtaget. En oversigt over godkendte indsamlinger findes på Civilstyrelsens hjemmeside[32]. En godkendt indsamling er ikke en garanti for, at de indsamlede midler går til rette lovlige formål, og underretningspligtige virksomheder og personer bør fokusere på midlernes overførsel og anvendelse. Herunder om indsamlingsaktiviteten er en naturlig aktivitet for ansøgeren, og om indsamlingen er proportional i forhold til formålet. Der vil eksempelvis være en øget risiko, hvor der ikke er transparens i indsamlingens dokumentation eller i tilfælde, hvor kun en delmængde af de indsamlede midler tilfalder de dokumenterede modtagere i eller ved konfliktzoner.

Et tilbagevendende opmærksomhedspunkt i hvidvaskunderretninger med mistanke om terrorfinansiering er indsamlingslignende adfærd uden indsamlingstilladelse. Eksempelvis hvor indbetalinger sker ved overførsel via MobilePay eller kontant i en ikke-erhvervsmæssig sammenhæng til konti tilhørende en forening, en privatperson, en enkeltmandsvirksomhed eller lignende. Ikke-godkendte indsamlinger har myndighedernes interesse, og indsamlingslignende adfærd bør udløse yderligere undersøgelse.

Digitale platforme udgør en betydelig del af indsamlingsaktiviteten, og det har øget mulighederne for at indsamle bredere og med færre omkostninger. Men det betyder også, at afstanden mellem donor og modtager kan være lang, og at donor kan have meget ringe muligheder for at træffe sin donationsbeslutning på et oplyst grundlag og for at kontrollere donationens anvendelse. De norske myndigheder beskriver også, at flere kendte udenlandske og norske ekstremistiske organisationer og miljøer beder om finansiel støtte på sociale medier[33]. Det anbefales, at de underretningspligtige virksomheder og personer fastholder fokus på indsamlingstilladelse, transparens og dokumentation uanset indsamlingsformen. ■

30) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 04.6 og EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 239.*

31) *Se figur side 37.*

32) *Godkendte indsamlinger (civilstyrelsen.dk)*

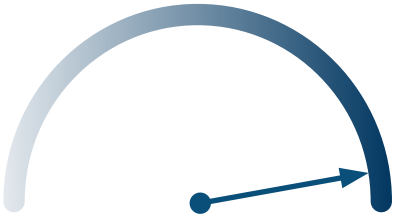
33) *Politiet/Politiets Sikkerhedstjeneste (2020): Nasjonal risikovurdering Hvitvaskning og terrorfinansiering, s. 60.*

09

Kontanter og højværdivarer

Sammenfatning

PET vurderer, at risikoen for, at kontanter og højværdivarer bruges til terrorfinansiering, er **høj**. Kontanter og højværdivarer er attraktive i flere af terrorfinansieringens faser, og betalingsmidlerne er præget af lav opdagelsesrisiko og lave omkostninger.



Dette kapitel bør læses i tæt sammenhæng med tilsvarende kapitler i National Risikovurdering af Hvidvask. Det anbefales også at læse kapitlet "Cash-related products" i EU-Kommissionens seneste risikovurdering[34].

Kontanter udgør fortsat et oplagt valg i alle faserne af terrorfinansiering. I forhold til fremskaffelse kan kontanter indsamles, stjæles eller tjenes både sort og hvidt, og de kan veksles til udenlandske valutaer som fx amerikanske dollars og euro. Der bør blandt banker og valutavekslingsbureauer[35] være øget opmærksomhed på veksling af danske kontanter til amerikanske dollars og euro i forhold til midlernes oprindelse, kundens fremtoning og forklaring samt generelt kundekendskab. Både i forhold til kontanter og højværdivarer vurderes opdagelsesrisikoen at være lav, ligesom omkostningerne ved begge også er lave. Disse forhold bidrager i betydelig grad til at gøre området attraktivt for terrorfinansiering.

Valutaveksling udgør i sig selv en risiko for terrorfinansiering, idet vekslingen slører midlernes oprindelse og kan muliggøre midlernes transport eller overførsel til udlandet. PET vurderer, at valutavekslingsvirksomheder har en høj iboende risiko for hvidvask og terrorfinansiering, og at denne risiko kun forøges, såfremt der er tale om uregistreret og dermed ulovlig valutavirksomhed, der således ikke er under tilsyn[36].

34) *EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 6.*

35) *De svenske myndigheder har en række relevante betragtninger om valutaveksling i deres seneste nationale risikovurdering, The Swedish Police Authority (2021): National risk assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021, s. 71-77.*

36) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 06.11 om valutavekslingsvirksomhed.*

I forhold til opbevaring af kontante midler til terrorfinansiering udgør tyveri eller opdagelse en risiko for de kriminelle, hvilket kan være et incitament til, at opbevaringsfasen er relativt kort frem mod overførsel. PET vurderer ikke, at den fysiske opbevaring af kontanter udgør en praktisk udfordring, idet beløbene er relativt små. Det er omvendt en praktisk udfordring, der kan gøre sig gældende ved hvidvask, hvis en kriminel fysisk skal opbevare mange millioner i kontanter – især hvis det ikke er nye pengesedler. For forståelsens skyld fylder en million kroner i nye 100-kronesedler lidt mere end en almindelig pakke A4-printerpapir og vejer næsten 10 kilo.

Især i forhold til overførsel af midler udgør kontanter en risiko for terrorfinansiering. Kontanter kan smugles forholdsvis simpelt ved at gemme dem på kroppen, i bagage eller andre medbragte genstande. 20.000 euro fylder omtrent det samme som to mobiltelefoner, hvis de er vekslet til nye 200-eurosedler. Dette øger muligheden for smugling på eksempelvis flyafgange. Toldstyrelsen og politiet bør fortsat have betydelig opmærksomhed på forsøg på kontantsmugling. Tilsvarende på deklarerede beløbs oprindelse og ejerforhold.

Kontanttransport er også attraktivt til at overføre midler til konfliktzoner, da det ofte er vanskeligt at overføre penge ved bankoverførsel. Det gør sig også gældende for nødhjælpsaktører, der kan have vanskeligt ved at overføre midler til partnere i eller tæt på konfliktzoner og derfor benytter kontanttransport eller en kombinationsløsning, hvor midler overføres elektronisk til eksempelvis Tyrkiet eller Libanon, hvor de hæves og transporteres kontant det sidste stykke vej. I forhold til anvendelsen af kontanter, så har kontanter den åbenlyse fordel, at der ikke er sporbarhed ved købet. Det gør sig især gældende ved angrebsfinansiering, hvor det vil være attraktivt at undgå transaktionsmonitorering og at efterlade digitale spor.

Som Hvidvasksekretariatet skriver i Den Nationale Risikovurdering af Hvidvask 2022[37], så falder antallet af danskere, der anvender kontanter. Ikke desto mindre vurderer PET, at kontanter i stigende grad vil være attraktive til brug for terrorfinansiering, især ved overførsel af midler til anvendelse i udlandet.

Højværdivarer har et højt risikopotentiale, fordi store værdier let kan skjules[38]. PET vurderer især, at overførsel af midler ved hjælp af ædelmetaller vil være en attraktiv mulighed. Som eksempel fylder ét kilo 24-karat guld til en værdi af mere end 400.000 kroner lidt mere end en tændstikæske. Som opbevaring af midler vil højværdivarer også være relevant, men dog med risiko for værditab, opdagelse eller tyveri. ■

37) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 02.2.*

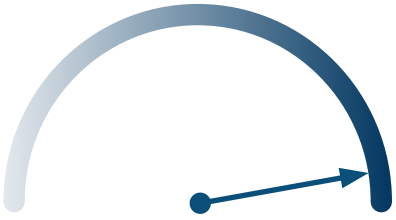
38) *Området behandles også i EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s.164-170.*

10

Ulovlig pengeoverførselsvirksomhed

Sammenfatning

PET vurderer, at risikoen for terrorfinansiering ved ulovlig pengeoverførselsvirksomhed er **høj**. Ulovlig pengeoverførselsvirksomhed er en af de eneste muligheder for at få penge ind i konfliktzoner, og området rummer flere centrale sårbarheder, da pengeoverførslerne netop er karakteriseret af lave omkostninger, betydelig anonymitet og manglende registrering samt tilsyns- og kontrolmuligheder.

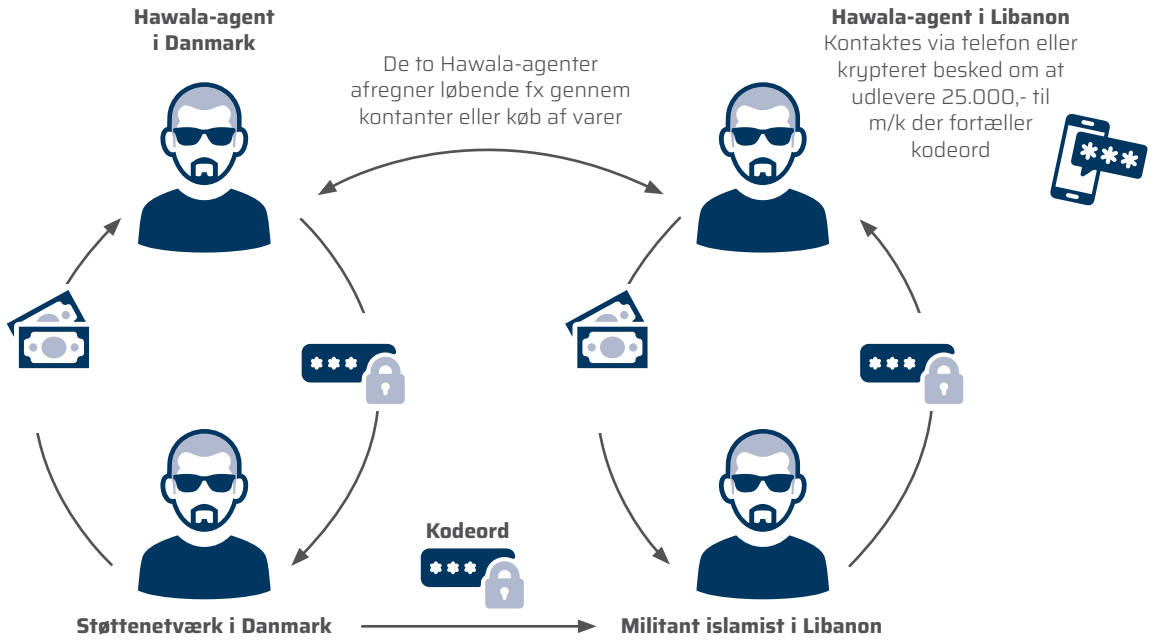


Risikoområdet kan opdeles i to kategorier: 'Ulovlig erhvervsmæssig overførsel af midler via bankkonti' og 'hawala'. Ulovlig erhvervsmæssig overførsel af midler via bankkonti er karakteriseret ved, at en aktør anvender banksystemet til at overføre penge for andre mod betaling, uden at vedkommende har tilladelse fra Finanstilsynet. Typisk vil der være tale om, at en specifik konto anvendes til transaktioner ud af Danmark, og at pengene enten indsættes kontant eller overføres fra andre konti i danske pengeinstitutter. Midlerne, der tilgår kontoen, samles i større summer, som så overføres samlet til udlandet. Den specifikke konto kan eksempelvis være tilknyttet en forening, en enkeltmandsvirksomhed eller være en privatkonto. Motivet for at anvende den ulovlige metode er, at omkostningerne ved større samlede enkeltoverførsler ofte er lavere end ved mange mindre overførsler, og at anonymiteten for kunderne er højere, fordi der ikke er etablerede kundekendskabsprocedurer og kun ringe muligheder for at afdække identiteten på den reelle kunde. Metoden er baseret på, at kunderne har tillid til, at aktøren gennemfører deres ønskede transaktioner.

Ulovlig pengeoverførselsvirksomhed er overordnet karakteriseret ved, at der ikke er nogen tilsynsmyndighed, der kontrollerer, at hvidvaskloven overholdes. PET vurderer, at de lave omkostninger og den høje grad af anonymitet gør uautoriserede pengeoverførselsvirksomheder attraktive til brug for terrorfinansiering. Det understøttes af, at terrorfinansiering ofte vil være mindre beløb end ved hvidvask, hvilket reducerer risikoen for opdagelse. Opdagelsesrisikoen udgøres overvejende af bankernes monitorering af kunder og transaktioner. Der bør i den forbindelse være øget opmærksomhed på ovenstående adfærd, hvor forskellige beløb fra forskellige afsendere samles og overføres samlet til udlandet.

Ulovlig erhvervsmæssig overførsel af midler via hawala indeholder ligeledes et betydeligt tillidselement, idet der ofte ingen dokumentation er for pengeoverførslen. Systemet findes i flere udgaver, men enkelt forklaret er fremgangsmåden, at kunden kontakter en hawaladar (udbyder af hawala) i sit eget land og afleverer den sum penge, som ønskes overført. Der aftales et gebyr og et kodeord for udleveringen af penge, der så sker hos en anden udbyder af hawala i det land, hvor pengene ønskes udbetalt. Kunden sender derefter kodeordet, eksempelvis via krypteret kommunikationsteknologi, til

EKSEMPEL PÅ HAWALAOVERFØRSEL



modtageren, mens hawaladaren gør det samme til sin kollega i udbetalingslandet. Modtageren går så til hawaladaren i modtagerlandet, oplyser kodeordet og får pengene udbetalt. Dermed flyttes pengene ikke ved overførslen, idet der i stedet opstår en intern gæld mellem de to hawaladarer. Denne gæld vil typisk variere over tid og kan udlignes ved fysiske møder og betalinger i guld, varer med over- eller underfakturering eller kontanter helt uafhængigt af kunderne. Metoden indebærer et fravær af myndigheds- og tilsynskontrol og er vanskelig at opdage. Dermed udgør den en betydelig risiko for terrorfinansiering, fordi høj grad af anonymitet, lav opdagelsesrisiko og lave omkostninger er tillokkende.

Samlet set udgør ulovlig pengeoverførselsvirksomhed en høj risiko for terrorfinansiering[39]. Området er karakteriseret ved en betydelig grad af anonymitet, lave omkostninger og svage opdagelsesmekanismer.

PET vurderer, at den ulovlige pengeoverførselsvirksomhed blandt andet anvendes i miljøer knyttet til Syrien, Libanon og Somalia. Truslen relateret til terrorfinansiering er høj for disse områder, da overførslerne går på tværs af landegrænser, opdagelsesrisikoen er lav, og det samtidig er en af få kanaler til at få penge ind i konfliktzoner.

Både de retshåndhævende myndigheder og tilsynsmyndighederne bør være opmærksomme på mulig hawala under udførelsen af deres opgaver. Hawala kan ofte forekomme i sammenhæng med anden erhvervsmæssig virksomhed som kiosker, registreret pengeoverførselsvirksomhed, valutaveksling mv.[40-41] ■

39) *Det samme gør sig gældende i Norge, hvor der ses en særligt stor risiko. Politiet/Politiets Sikkerhedstjeneste (2020): Nasjonal risikovurdering Hvitvaskning og terrorfinansiering, s. 59.*

40) *Den svenske nationale risikovurdering fokuserer også på hawala som risikoområde og pointerer blandt andet, at hawala i visse geografiske regioner kan være den eneste måde at overføre midler på. The Swedish Police Authority (2021): National risk assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021, s. 102.*

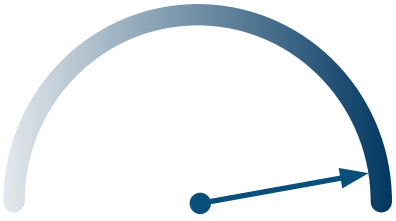
41) *Se også kapitlet "Illegal transfers of funds – Hawala" i EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 81-85.*

11

Autoriseret pengeoverførsels-virksomhed

Sammenfatning

PET vurderer, at der er høj risiko for, at autoriseret pengeoverførselsvirksomhed misbruges til terrorfinansiering. Risikoen for terrorfinansiering er **høj**, idet pengeoverførselsvirksomheder typisk kan transportere midler tættere på konfliktzoner og med lavere omkostninger end bankerne. Samtidig er det vanskeligt for operatørerne at sondre mellem kriminelle og legale kunder og transaktioner, og den lavere opdagelsesrisiko og manglende regeloverholdelse øger risikoen.



Risikoområdet dækker over pengeoverførsel, der sker ved autoriserede pengeoverførselsvirksomheder, som udbyder betalinger mellem personer eller virksomheder, uden at der oprettes en konto i hverken betalerens eller modtagerens navn.

Pengeoverførselsvirksomheder kan være virksomheder, der har pengeoverførsel som primær ydelse, eller virksomheder der i forbindelse med drift af kiosk- eller købmandsvirksomhed fungerer som agent for en større udenlandsk pengeoverførselsvirksomhed.

Pengeoverførselsvirksomheder er underlagt Finanstilsynets tilsyn og hvidvasklovens forpligtelser. Hos pengeoverførselsvirksomheder, der aktivt overholder hvidvaskloven, herunder gennemfører kundekendskabsprocedurer og transaktionsmonitorering, er risikoen for terrorfinansiering reduceret.

For personer, der ønsker at sende penge ud af Danmark, udgør pengeoverførselsvirksomheder et attraktivt alternativ til pengeinstitutter, idet omkostningerne ofte vil være lavere, hastigheden for overførslen højere og kravene om kundetilhørsforhold mindre. Det kan fx være flygtninge, indvandrere eller personer, der opholder sig i Danmark på grund af arbejde. Desuden kan pengeoverførselsvirksomheder i en række udviklingslande have bedre muligheder for at udbetale penge end den lokale banksektor, da de er bedre repræsenteret med kontorer.

Det stiller store krav til virksomhedernes kontrolprocedurer at identificere en overførsel til terrorfinansiering, da der samtidigt kan være mange legitime kundetransaktioner, der ligner med hensyn til beløbsstørrelse og destination.

PET vurderer, at der er en betydelig risiko for, at kundekendskabsprocedurer og andre hvidvaskforanstaltninger ikke bliver udført i tilstrækkelig grad. Det gælder særligt for de agenter, hvor pengeoverførselsvirksomhed er et sekundært forretningsområde[42]. Det åbner også en mulighed for, at der kan anvendes stråmænd til at få gennemført en transaktion ved en pengeoverførselsvirksomhed.

Den manglende regeloverholdelse blandt pengeoverførselsvirksomhederne sammenholdt med den lave opdagelsesrisiko og de lave omkostninger[43] gør pengeoverførselsvirksomheder attraktive for personer, der har et ønske om at finansiere terrorisme.

PET's vurdering af pengeoverførselsvirksomheder er i overensstemmelse med internationale vurderinger. Europol skriver i deres Terrorism Situation and Trend Report fra 2022:

"Jihadist actors commonly use money transfer services, such as MoneyGram and Western Union, or informal value transfer systems (IVTS), such as hawala".[44]

42) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 06.05 om betalingstjenesteområdet, samt Politiet/Politiets Sikkerhedstjeneste (2022): Nasjonal risikovurdering Hvitvaskning og terrorfinansiering, s. 78.*

43) *De norske myndigheder har samme betragtninger i den seneste nationale risikovurdering (Politiet/Politiets Sikkerhedstjeneste 2022: Nasjonal risikovurdering Hvitvaskning og terrorfinansiering, s. 6).*

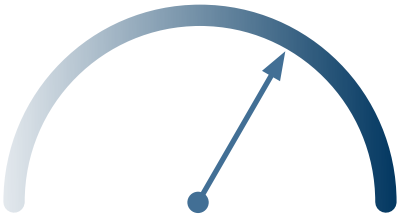
44) *Europol (2022): Terrorism Situation and Trend Report (TE-SAT), s. 18. Se også EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 76.*

12

Pengeinstitutter

Sammenfatning

PET vurderer, at der er en **betydelig** terrorfinansieringsrisiko relateret til pengeinstitutterne. Pengeinstitutternes ydelser er lettilgængelige og kan anvendes til alle terrorfinansieringens faser. Pengeinstitutterne har generelt integreret en række mitigerende handlinger og investeret både i tekniske og menneskelige ressourcer.



Pengeinstitutter udbyder finansielle tjenesteydelser, der henvender sig til private kunder og erhvervskunder, herunder også foreninger og fonde. Det følger af god-skik-reglerne i lov om betalingskonti, at alle forbrugere har ret til en basal indlånskonto i et pengeinstitut.

Der er i 2022 etableret 89 pengeinstitutter i Rigsfællesskabet, hvoraf 55 er lokaliseret i Danmark, 4 på Færøerne og 1 pengeinstitut i Grønland. De resterende 29 pengeinstitutter er filialer af udenlandske pengeinstitutter, som er lokaliseret i Rigsfællesskabet.

Det danske marked for pengeinstitutter er generelt kendetegnet ved en høj koncentration, hvilket vil sige, at få banker dækker størstedelen af markedet for finansielle ydelser og serviceydelser. De to største danske banker har en markedsandel på 60 %, og de fire største banker har tilsammen en markedsandel på 88 %[45].

Pengeinstitutter kan anvendes til samtlige af terrorfinansieringens faser. Et pengeinstitut stiller kredit til rådighed og kan dermed bruges til fremskaffelse af midler, og en potentiel terrorist kan opbevare penge på en bankkonto, overføre penge til andre personer og virksomheder samt sikre betaling af varer og ydelser.

Samtidig er pengeinstitutter kendetegnet ved høj tilgængelighed, og det kræver ingen særlig viden eller ekspertise at benytte dem til terrorfinansiering. Det er let at oprette en bankkonto, og bankernes netbankløsninger er tilgængelige for selvbetjening døgnet rundt og giver mulighed for straksoverførsler mellem konti og mellem pengeinsti-

45) *Copenhagen Economics (2021): Konkurrencen i den danske banksektor.*

tutter. Endvidere er der med bankerne adgang til udlandstransaktioner via korrespondentbankforbindelserne.[46]

Den Europæiske Banktilsynsmyndighed (EBA) rapporterer, at 70 % af de europæiske tilsynsmyndigheder finder, at der er signifikant eller meget signifikant risiko for hvidvask og terrorfinansiering blandt betalingsinstitutter. Der er en række faktorer, der forklarer den betydelige risiko for hvidvask og terrorfinansiering blandt betalingsinstitutter, herunder bl.a. tilstedeværelsen af kontanter, de enkeltstående og sporadiske pengeoverførsler til forskel for faste overførsler, de manglende faste kundeforhold og det høje tempo, som betalinger bliver eksekveret i, samt anvendelsen af ny teknologi til at onboarde kunder digitalt[47]. EBA noterer sig også, at institutterne har en gatekeeper-rolle, der lukker penge og kunder ind i det finansielle system.[48]

Risikoen for terrorfinansiering varierer dog også for pengeinstitutter, da det afhænger af forretningsmodel, kundesegmenter, og hvilke markeder, finansielle serviceydelser og produkter som pengeinstituttet udbyder. Overordnet set kan risikoen vurderes i forhold til de to store kundegrupper: private kunder og erhvervskunder. Herefter kan risikoen gradueres efter, hvilke produkter pengeinstituttet udbyder til de to kundegrupper.

Terrorfinansieringsrisikoen for finansielle serviceydelser til private kunder, som fx forbrugerkredit og udstedelse af betalingskort, er høj, da man som sektor er eksponeret ved at have et meget stort antal kunder, og ved selv at stille små beløb til rådighed risikerer pengeinstitutterne at blive misbrugt til terrorfinansiering. Risikoen ved genstandsbestemte lån vurderes at være lavere end ved kontantlån, da genstandsbestemte lån typisk ville indeholde et videresalgselement og derfor er mindre attraktive.

Kontanthævninger og brug af bankautomater er blandt de serviceydelser, hvor pengeinstitutter har den højeste risiko for eksponering. Det fremgår af EU-Kommissionens seneste supranationale risikovurdering, at terrorgrupper ofte indsætter midler på indlånskonti med henblik på terrorfinansiering. Dog fremgår det også, at det kræver viden og opmærksomhed at sikre, at pengene fremstår legitime. I konfliktzoner kan kontanthævninger fra betalingsautomater være besværliggjort af, at den underliggende betalingsinfrastruktur er langsom eller ikke-fungerende[49].

Det er vanskeligt at være anonym i et pengeinstitut, hvilket delvist reducerer, hvor attraktivt det som privatperson er at anvende pengeinstitutter til terrorfinansiering. Personer, der finansierer terrorisme, kan dog opnå delvis

46) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 06.1 om pengeinstitutter.*

47) *European Banking Authority (2021): Opinion of the European Banking Authority on the risks of money laundering and the terrorist financing affecting the European Union's financial sector, s. 34.*

48) *European Banking Authority (2021): Opinion of the European Banking Authority on the risks of money laundering and the terrorist financing affecting the European Union's financial sector, s. 11 og s. 26-32.*

49) *EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 38.*

anonymitet ved at anvende stråmænd. Der har historisk været eksempler på, at særligt pårørende har ageret stråmænd for militante ekstremister.

Hvis der er fravær af fysisk kundekontakt hos pengeinstitutterne (eller betalingsinstitut eller e-pengeinstitut), eksempelvis ved digital onboarding, stiller det store krav til kundekendskabsprocedurer, der udgør et vigtigt element i forebyggelsen af terrorfinansiering. Aktører uden interaktion med kunderne har i ringere grad mulighed for at danne sig et indtryk af kunden og må nødvendigvis forlade sig mere på transaktionsmonitorering. Når der samtidig ofte er tale om udenlandske aktører, bliver afstanden mellem kunde, samfund og finansiel virksomhed endnu større.

Hvidvasksekretariatet bemærker i Den Nationale Risikovurdering af Hvidvask, at der ses flere delkunder, dvs. personer eller virksomheder, der er kunder i mere end en bank[50]. Den udvikling betyder, at det både for den primære bankforbindelse og for de sekundære banker bliver vanskeligere at opdage mistænkelige aktiviteter, fordi bankerne ikke kan vurdere en kundes samlede aktiviteter.

Udviklingen med flere delkunder skyldes blandt andet, at kunderne i en periode har været pålagt negative renter og derfor har spredt deres engagement. Men at sprede sine engagementer kan imidlertid også være attraktivt for kriminelle. En risikofyldt kunde med fx fem forskellige banker vil ikke nødvendigvis fremstå som risikofyldt i det enkelte institut. Det betyder alt andet lige, at den enkelte bank ikke har det fulde finansielle billede, hvilket samlet set øger risikoen for pengeinstitutterne[51].

Delkunders konti kan bruges til at sløre og skjule midlers tilstedeværelse og transit, det gælder også, hvis de flyttes videre til eksempelvis kryptomarkeder. Hvis der samtidig er tale om udenlandske finansielle virksomheder, bliver det vanskeligere og mere tidskrævende for danske myndigheder at få indsigt i informationerne, og det bliver sværere at vurdere mistænkelige forholds karakter og omfang.

Terrorfinansieringsrisikoen vedrørende erhvervskunder er moderat. EU's supranationale risikovurdering fra 2022 nævner omkring erhvervskunder og institutionelle investeringer, at de forskellige risikofaktorer såsom produkter, kunder, geografi og servicekanaler betyder, at disse ydelser ikke er attraktive for terrorister. I mange tilfælde vil personer, der ønsker at foretage terrorfinansiering ikke have den nødvendige ekspertise til at få adgang til sektoren.

Den primære risiko for terrorfinansiering vedrørende erhvervskunder knytter sig til mindre erhvervsdrivende, erhvervsdrivende fonde eller foreninger. Risikoen kan knyttes til indsamling, donationer, indtægter fra enkeltmandsvirksomhed eller lignende. Se i den forbindelse kapitlet om nonprofit-området. Der kan også være tale om overførsler via danske eller udenlandske betalingstjenester eller kryptobørser. Det kan være særdeles vanskeligt at identificere mistænkelige aktiviteter, hvorfor der bør fokuseres på elementer af konfliktzone-involvering, tegn på kriminalitet, tegn på tilknytning til ekstremistiske miljøer eller aktører, som kan rette mistanken mod terrorfinansiering.

50) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 06.1.*

51) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 06.5.*

For både erhvervs- og privatkunder er formueforvaltning og herunder investeringsrådgivning et område, hvor PET vurderer, at der er lav terrorfinansieringsrisiko. Formueforvaltning henvender sig til velhavende kunder, der over en lang tidshorisont ønsker at forrente deres formue. PET har ikke indikationer på, at formuer, der har været forvaltet i et pengeinstitut eller er undergået investeringsrådgivning, har været brugt til terrorfinansiering.

Som modvægt til den iboende terrorfinansieringsrisiko har pengeinstitutterne generelt integreret en række mitigerende handlinger i deres forretningsgange, ligesom de har investeret i transaktionsmonitorering og menneskelige ressourcer. PET vurderer, at denne indsats reducerer truslen relateret til terrorfinansiering, da personer, der har et ønske om at yde terrorfinansiering, er bekendt med de mange kontrolforanstaltninger og kundekendskabsprocedurer og derfor i nogle tilfælde bevidst vælger pengeinstitutternes service fra på grund af den øgede opdagelsesrisiko.

Pengeinstitutterne er generelt kendetegnet ved at have en betydelig grad af risikobevidsthed med hensyn til terrorfinansiering, men samtidig stå over for en vanskelig opgave med at omsætte risikobevidstheden til konkrete risikoreducerende tiltag, eksempelvis at kalibrere transaktionsmonitoreringen til at finde de relevante transaktioner.

Det fremgår af EU's supranationale risikovurdering, at der kan være en tendens til at pengeinstitutter håndterer terrorfinansieringsrisiko på samme vis som risiko for hvidvask[52]. PET vurderer, at denne sårbarhed også er til stede i en dansk kontekst, hvor der har været eksempler på, at pengeinstitutter ikke differentierer tilstrækkeligt, når de håndterer de to forskellige risici, som kan have afgørende indbyrdes forskelle, hvilket også afspejles i de to nationale risikovurderinger af hhv. hvidvask og terrorfinansiering.

Det er en sårbarhed med hensyn til terrorfinansiering, at pengeinstitutterne ikke i tilstrækkeligt omfang har tilladelse til at dele oplysninger om deres kunder med andre pengeinstitutter. Det betyder, at hvis et pengeinstitut afviser at gennemføre en transaktion eller stiller kritiske spørgsmål til en kundes ønske om at overføre penge til et højrisikoland, så kan kunden gå til et nyt pengeinstitut, uden at det nye pengeinstitut kender til kundens historik. Finans Danmark anfører i deres status over hvidvaskindsatsen for 2021, at:

"Pengeinstitutterne kan kun se, hvad der sker inden for egen forretning. Det betyder, at der kan være transaktioner, der indgår i et større netværk på tværs af mange institutter, som det enkelte institut ikke kan se omfanget af, og dermed er mistanken måske heller ikke tydelig for det enkelte institut".[53]

Pengeinstitutterne har tidligere tegnet sig for en betydelig andel af alle transaktioner, men i dag kommer der flere udbydere af finansielle serviceydelser, eksempelvis betalingstjenester og e-pengeinstitutter, der også foreståar eller initierer transaktioner. Det medfører, at det for det enkelte institut bliver vanskeligere at have det fulde billede af deres kunders adfærd. Selvom denne udvikling kan være til gavn for den enkelte kunde, besværliggør det bankernes opgave med at monitorere deres kunders aktiviteter. Der er ikke noget, der tyder på, at denne fragmentering vil blive mindre fremover. ■

52) *EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 39.*

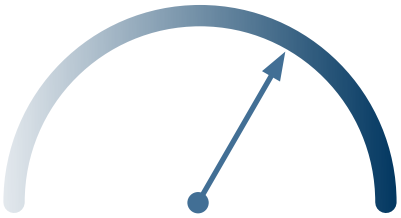
53) *Finans Danmark (2021): Hvidvaskindsats, Status 2021, s. 13.*

13

Terrorfinansiering fra organiseret økonomisk kriminalitet

Sammenfatning

PET vurderer, at risikoen for terrorfinansiering baseret på indtægter fra organiseret økonomisk kriminalitet er **betydelig**. Det skyldes, at der kan være ekstremistiske sympatier i de kriminelle netværk, og at nogle af de barrierer, der er i forhold til terrorfinansiering, allerede er passeret, idet professionaliseret økonomisk kriminalitet indeholder elementer af anonymitet og grænseoverskridende transaktioner, store beløb og en accept af finansielle omkostninger.



Terrorfinansiering, herunder særligt organisationsfinansiering, kan være relateret til almindelig økonomisk kriminalitet, i særdeleshed skatte- og momssvig, som er et meget profitabelt kriminalitetsområde. PET henviser i den forbindelse til afsnit 05.1 i Den Nationale Risikovurdering af Hvidvask, som nærmere vedrører skatte- og momssvig. Området er dog også relevant i forhold til terrorfinansiering, idet PET har identificeret en risiko for, at kriminelt udbytte i en vis udstrækning tilfalder terrorgrupper i eller omkring konfliktzoner.

Det konkrete modus kan bestå i, at kriminelle netværk i Danmark ved eksempelvis kædesvig eller momskarruselsvindel genererer et kriminelt udbytte, der overføres til udlandet. Såfremt de kriminelle bagmænd har ekstremistiske sympatier, kan mindre dele af det kriminelle udbytte slutteligt tilfalde militant islamistiske grupper som et bidrag eller en religiøs aflad. Både underretningspligtige virksomheder og personer samt de relevante myndigheder kan have meget vanskeligt ved at identificere denne form for terrorfinansiering, fordi der i forvejen er tale om kriminelt udbytte, der er forsøgt skjult i udlandet for

så delvist at tilfalde terrorgrupper. Det er således vigtigt, at både myndigheder og underretningspligtige virksomheder og personer vurderer, om den mistænkte potentielt kan have relationer til kendte ekstremistiske grupperinger.

Der er eksempler på, at den organiserede økonomiske kriminalitet udføres ved brug af professionelle rådgivere – eksempelvis inden for skat, jura og revision[54]. National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025 har blandt andet fokus på den komplekse og organiserede kriminalitet, herunder brugen af professionelle rådgivere og facilitatorer[55]. Det er vigtigt, at både retshåndhævende myndigheder og tilsynsmyndigheder fokuserer på at identificere rådgivere, som bevidst assisterer kriminelle. Desuden bør eksempelvis advokater og revisorer have skærpet opmærksomhed på, om deres rådgivning reelt skal anvendes til kriminelle aktiviteter – eksempelvis ved etableringen af en bestemt selskabs- eller fondskonstruktion[56]. Specifikt i forhold til terrorfinansiering kunne det være i relation til selskaber i eller ved konfliktzoner, etablering af atypiske selskabskonstruktioner omkring moskéer, friskoler, udenlandske donationer eller almennyttige fonde. ■

54) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, side 110 om professionelle rådgivere.*

55) *Regeringen (2022): National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025, s. 13.*

56) *EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 187.*

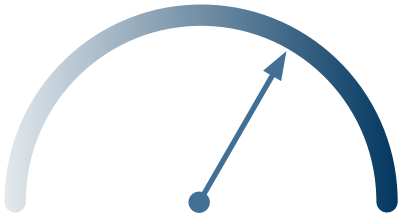

DEN EUROPÆISKE UNION
DANMARK
PAS

14

Identitetsmisbrug og afledt kriminalitet

Sammenfatning

PET vurderer, at identitetsmisbrug og afledt kriminalitet udgør en **betydelig** risiko for terrorfinansiering. Området er attraktivt til fremskaffelse af ulovlige midler, og opdagelsesrisikoen kan være reduceret, fordi kriminaliteten kan ligne legale forhold, idet der anvendes ægte digitale identiteter.



Risikoområdet dækker over misbrug eller tyveri af identiteter og afledt berigelseskriminalitet. Identitetsmisbrug er en samlebetegnelse for forhold, hvor en (digital) identitet bliver misbrugt til berigelseskriminalitet. Oftest vil der være tale om digitale forhold, fordi det vil være betydeligt mere risikabelt at misbruge identiteten ved fysisk fremmøde i fx en bank. Forholdene kan stamme fra tyveri eller fjendtlig overtagelse af en digital identitet, men også fra situationer, hvor en person overlader sin digitale identitet til andre, velvidende at det er med kriminalitet for øje[57]. Med overtagelsen følger typisk besiddelse af vedkommendes personlige oplysninger, eventuelt pas eller kørekort samt MitID.

Identitetsmisbrug er overvejende relevant for terrorfinansiering i forbindelse med fremskaffelse af midler eller genstande. Muligheden for at misbruge en andens identitet åbner en række muligheder for økonomisk kriminalitet. Det kan være varekøb uden efterfølgende betaling, handel på online-lokationer som DBA.dk, optagelse af flere online-forbrugslån, etablering af virksomheder med efterfølgende moms- og/eller skatteunddragelse.

Risikoen ved identitetsmisbrug stiller store krav til de underretningspligtige virksomheder og personers kundekendskabsprocedurer og løbende monitorering, fordi tingene umiddelbart fremstår legitime, da der anvendes en gyldig digital identitet og legitimation. Identitetsmisbrug udnytter en sårbarhed i datadelingen mellem relevante aktører blandt myndigheder og private virksomheder. Eksempelvis når en forbrugslånsvirksomhed skal kreditvurdere en kunde, som er i stand til at legitimere sig digitalt, men hvis øvrige data ikke understøtter ansøgningen. Eller hvis en identitet ønsker at oprette et selskab, men anden offentlig data indikerer, at der er tale om en betydelig risiko for et kriminelt formål. Jo flere datakilder, som myndigheder og private virksomheder har til at bekræfte en identitet og risikovurdere adfærden, desto færre muligheder for kriminalitet. ■

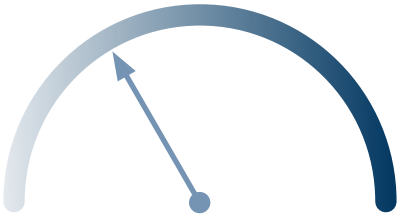
57) *Se også EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s. 107-110.*

15

Socialt bedrageri

Sammenfatning

PET vurderer, at der er **moderat** risiko for, at socialt bedrageri bliver anvendt til terrorfinansiering. Socialt bedrageri vurderes som værende attraktivt blandt personer i ekstremistiske miljøer, men både myndigheders og underretningspligtige virksomheder og personers betydelige fokus på truslen vurderes at reducere risikoen.



Risikoområdet dækker over misbrug af alle former for sociale ydelser, som bevidst er modtaget uberettiget. I forhold til risikoen for terrorfinansiering kan man inddele socialt bedrageri i tre kategorier – udrejse til konfliktzoner, udrejse til andre destinationer og socialt bedrageri i Danmark.

PET så bl.a., at personer udrejste til konfliktzoner samtidig med, at de modtog sociale ydelser som fx SU eller dagpenge. Sagerne blev omtalt i medierne, hvor PET oplyste, at PET havde foretaget 39 personindberetninger til Styrelsen for Arbejdsmarked og Rekruttering[58]. Som nævnt tidligere har der siden 2016 ikke været tilgang af fremmedkrigere, men modus omkring udrejse med sociale ydelser bør fortsat være i fokus for de underretningspligtige virksomheder og personer, især hvis der opstår en ny udrejsetendens.

PET vurderer, at myndighederne og de underretningspligtige virksomheder og personer har et solidt fokus på socialt bedrageri. Det gør sig også gældende for sociale ydelser til personer på andre destinationer end konfliktzoner. Dette vil typisk være nabolande eller lande i geografisk nærhed til Syrien, Irak, Somalia, Libanon, Afghanistan og Palæstina. De typiske kendetegn ved disse sager vil være længerevarende ophold uden for Danmark, køb af flybilletter, bortfald af faste udgifter i Danmark og markant ændring i finansiel adfærd efter udrej-

58) *Samrådstale om fremmedkrigere på offentlige ydelser (30. august 2018, FT.dk).*

se. Der vil formentlig ofte være tvivl hos de underretningspligtige virksomheder og personer, for så vidt angår en mistanke om mulig terrorfinansiering eller almindeligt socialt bedrageri/anden kriminalitet.

Den sidste kategori indebærer socialt bedrageri i Danmark, hvor de uberettigede midler anvendes til økonomisk støtte til personer eller grupper, der er involveret i terrorisme eller terrorlignende handlinger. Her kan der være tale om angrebs- eller organisationsfinansiering, hvor førstnævnte typisk vil være knyttet til personen selv eller en nærtstående person eller gruppe, som modtager midler eller får betalt genstande eller ydelser i angrebsøjemed. For så vidt angår organisationsfinansiering, kan der være tale om mindre overførsler direkte til individer i udlandet, eksempelvis via en pengeoverførselsvirksomhed til en mellemmand i eller ved en konfliktzone. Det kan også være midler, der forsætligt eller uforsætligt overføres eller doneres kontant til foreninger, almennyttige fonde, konkrete indsamlinger eller lignende, som understøtter en terrororganisation[59].

Samlet set vurderer PET, at myndighedernes samarbejde og fælles fokus på bekæmpelse af socialt bedrageri relateret til relevante miljøer, sammenholdt med de underretningspligtiges stigende fokus på at underrette ved mistanke om socialt bedrageri reducerer risikoen for terrorfinansiering. ■

59) *Se også PET (2020): National risikovurdering af terrorfinansiering på NPO-området i Danmark, s. 13-14 om uagtsomhed.*

16

Øvrige risikoområder

Repatrieringsydelse og hjemrejsestøtte

PET vurderer, at der er **moderat** risiko for, at repatrieringsydelser og hjemrejsestøtte bliver brugt til terrorfinansiering. Ved repatriering forstås personers frivillige tilbagevenden til deres hjemland eller tidligere opholdsland med henblik på at tage varig bopæl. Efter reglerne i repatrieringsloven kan der søges kommunal hjælp til repatriering, og for en familie, hvor alle modtager repatrieringsydelse, kan det beløbe sig til flere hundrede tusinde kroner. Det har i visse tilfælde været vanskeligt for de ydelsesberettigede at få udbetalt repatrieringsydelse og hjemrejsestøtte, da danske pengeinstitutter ikke har kunnet gennemføre overførsler til for eksempel Iran og Syrien. Der er derfor i april 2022 indført regler om fleksibel udbetaling af hjælp til repatriering eller hjemrejsestøtte til Syrien og Iran i sager, som er under behandling den 1. maj 2022 eller senere, således at ydelserne kan udbetales kontant ved afrejse fra Danmark. Dette medfører efter PET's vurdering en øget risiko for forsætlig og uforsætlig terrorfinansiering i forbindelse med transit, indrejse og ankomst til lande i eller omkring konfliktzoner. Eksempelvis ved visitation ved grænseovergange, hvor der opstår krav om beskatning eller gebyr. Risikoen forøges med beløbenes størrelse.

Når de underretningspligtige virksomheder og personer undersøger en mistanke om terrorfinansiering, så bør radikalisering eller misligholdelse af udrejseaftalen være indikationer på mulig terrorfinansiering. Ligeledes skal kommunerne, der træffer afgørelse om udbetaling af fx repatrieringsydelse, indhente en udtalelse fra politiet, hvis der er grund til at antage, at ansøgeren har til hensigt at deltage i aktiviteter i udlandet, som kan indebære eller forøge en fare for statens sikkerhed eller andre staters sikkerhed eller en væsentlig trussel mod den offentlige orden.

Leasing

PET vurderer, at der er **lav** risiko for, at leasing bliver anvendt til terrorfinansiering. Leasing er fortsat et risikoområde, hvor der foreligger en begrænset empiri i forhold til at vurdere risikoen for terrorfinansiering. Risikoen ved leasing er primært forbundet med fremskaffelse af midler, hvor fx en leaset bil bliver solgt ulovligt af den leasende kunde, og de fremskaffede midler bliver anvendt til støtte for terrorisme. Der kan også være tilfælde, hvor fx en leaset bil bliver ulovligt transporteret til en konfliktzone som bidrag til konflikten. Risikoen ved dette modus er formindsket i takt med, at situationen i Syrien og Irak har udviklet sig i retning af betydeligt mere isolerede zoner, hvortil adgang er særdeles vanskelig.

Sårbarhederne omkring leasing er fortrinsvis knyttet til mulighederne for validering og kontrol af kundens identitet, betalingsevne og opholdsgrundlag.

Kunst og krigsbytte

PET vurderer, at der er **lav** risiko for, at kunst og krigsbytte i Danmark bliver anvendt til terrorfinansiering. Risikoområdet vedrører terrorfinansiering ved handel med kunst, antikviteter og artefakter. Området kaldes i FATF-regi for Art, antiquities and other cultural objects, AACO. PET opdeler området i to kategorier.

Den første kategori berører risikoen for opbevaring og overførsel af midler ved hjælp af værdifuld kunst eller en kunstlignende genstand. Det vil sige, at midler til terrorfinansiering investeres i en kunstgenstand, som senere sælges eller realiseres på anden vis i geografisk nærhed af, hvor midlerne skal anvendes. PET vurderer ikke, at metoden er attraktiv i forhold til terrorfinansiering i en dansk kontekst sammenlignet med andre tilgængelige metoder, hverken til opbevaring eller overførsel[60]. Hvidvasksekretariatet bemærker, at den subjektive værdiansættelse af kunst kan gøre det vanskeligt at vurdere, om der ved kunsthandel er overført midler, der overstiger kunstværkets faktiske værdi[61]. PET vurderer dog, at risikoen er begrænset i en dansk terrorfinansieringskontekst.

Den anden kategori vedrører risikoen for salg af krigsbytte, herunder kunstværker, smykker, mønter mv., som er kommet terrorgrupper i hænde i forbindelse med en konkret konflikt. Islamisk Stats plyndringer i Syrien og Irak er et eksempel herpå. Krigsbytte kan transporteres ud af konfliktzonen og herefter sælges på både legale og illegale kunstmarkeder og dermed fungere som en metode til anskaffelse af betydelige midler. Dette kan ske med eller uden oprindelsescertifikater, der kan være falske eller udstedt af illegitime aktører som eksempelvis Islamisk Stat. ■

60) *Se også EU-Kommissionens risikovurdering for "High value goods – artefacts and antiquities" i EU-Kommissionen (2022): Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, s.153.*

61) *Hvidvasksekretariatet (2022): Den Nationale Risikovurdering af Hvidvask, afsnit 06.13 om kunst.*

17

Empiri og litteratur

Beskrivelse af empiri
Denne risikovurdering bygger i vid udstrækning på samme empiriske og metodiske tilgang som risikovurderingen fra 2019.

Risikovurderingen er med hensyn til identifikation af de finansielle sårbarheder udarbejdet i tæt samarbejde med Hvidvasksekretariatet, da der er et stort overlap mellem finansielle sårbarheder relateret til hvidvask og terrorfinansiering. Et lignende samarbejde har gjort sig gældende i den norske risikovurdering fra november 2022[62].

PET vurderer risikoen for terrorfinansiering i et holistisk perspektiv i overensstemmelse med Financial Action Task Forces (FATF's) vejledning på området[63]. Det betyder, at risikovurderingen af terrorfinansiering empirisk er funderet på forskellige kilder af viden, der har både en kvalitativ og kvantitativ karakter, ligesom ophavet til viden også kan være både nationalt og internationalt.

Efterforskninger og straffesager relateret til terrorfinansiering i en national og international kontekst er vigtige kvalitative kilder til at forstå modus for terrorfinansiering. Efterforskninger og straffesager kan dog ikke afgøre, hvorvidt der er tale om en trend inden for terrorfinansiering, da enkelte sager ikke nødvendigvis er repræsentative. Viden om de nationale efterforskninger og straffesager vedrørende terrorfinansiering er primært forankret i PET og de danske politikredse, hvorimod PET har indhentet viden om internationale efterforskninger og straffesager i bl.a. FATF og Counter ISIS Finance Group (CIFG). PET er derudover en del af et stærkt skandinavisk samarbejde omkring risikovurderinger, hvor de skandinaviske lande udveksler viden om terrorfinansiering.

PET har udarbejdet kvantitative analyser på baggrund af Hvidvasksekretariatets underretninger om mistanke om terrorfinansiering og PET's efterfølgende bearbejdning af underretningerne. Øvrige empiriske kilder er PET's samarbejde med danske myndigheder om at inddrage både virksomheder og brancheorganisationer i identifikationen af trusler og finansielle sårbarheder. Analyser og risikovurderinger fra internationale organisationer er også inddraget, herunder bl.a. EU-Kommissionens vurdering af risici for hvidvask af penge og finansiering af terrorisme samt Europols analyser og vurderinger. ■

62) *Politiet/Politiets Sikkerhedstjeneste (2022): Nasjonal risikovurdering Hvitvaskning og terrorfinansiering, s. 5.*
63) *FATF (2019): Terrorist Financing Risk Assessment Guidance 2019, s. 20.*

Litteratur

Center for terroranalyse (2023): *Vurdering af terrortruslen mod Danmark.* PET.dk.

Chainalysis (2020): *Chainalysis Intelligence Brief: How Syria-based Cryptocurrency Exchange BitcoinTransfer Facilitated Terror Financing Campaigns.* Chainalysis.com.

Copenhagen Economics (2021): *Konkurrencen i den danske banksektor.* Finansdanmark.dk.

Davis, Jessica (2021): *Illicit Money: Financing Terrorism in the 21st Century*, Lynne Rienner Publishers.

Davis, Jessica (2022): *New Technologies but Old Methods in Terrorism Financing, The CRAAFT Research Briefing Series 2020-2022.*

Retten i Roskilde (2022): *Dom i straffesag mod tre medlemmer af ASMLA.* Domstol.dk

European Banking Authority (2021): *Opinion of the European Banking Authority on the risks of money laundering and the terrorist financing affecting the European Union's financial sector.* Eba.europa.eu.

EU-Kommissionen (2022): *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.* Europa.eu.org. COM(2022) 554 final.

EU-Kommissionen (2022): *Commission staff working document accompanying the document Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities.* Europa.eu.org. SWD(2022) 344 final.

Europol (2022): *Terrorism Situation and Trend Report (TE-SAT).* Europol.europa.eu.

FATF (2019): T*errorist Financing Risk Assessment Guidance.* FATF-GAFI.org.

Finans Danmark (2021): *Hvidvaskindsats, Status 2021.* Finansdanmark.dk

Finanstilsynet (2022): *Blockchain-teknologi kan udgøre en effektiv infrastruktur til betalingstjenester.* Finanstilsynet.dk

Finanstilsynet (2022): *Vejledning til virksomheder omfattet af hvidvaskloven til vurdering af foreninger i forhold til risikoen for hvidvask og terrorfinansiering.* Finanstilsynet.dk.

Hvidvasksekretariatet (2022): *Den Nationale Risikovurdering af Hvidvask.* Anklagemyndigheden.dk.

PET (2020): *National risikovurdering af terrorfinansiering i Danmark 2019.* PET.dk.

PET (2020): *National risikovurdering af terrorfinansiering på NPO-området i Danmark*. PET.dk.

Politiet/Politiets Sikkerhedstjeneste (2020): *Nasjonal risikovurdering Hvitvaskning og terrorfinansiering.* PST.no.

Politiet/Politiets Sikkerhedstjeneste (2022): *Nasjonal risikovurdering Hvitvaskning og terrorfinansiering.* PST.no.

Regeringen (2022): *National strategi for forebyggelse og bekæmpelse af hvidvask og terrorfinansiering 2022-2025.* Justitsministeriet.dk.

Reimer & Redhead (2022): *Bit by Bit – Impacts of New Technologies on Terrorism Financing Risks.* Project CRAAFT, RUSI Occasional Paper, April 2022.

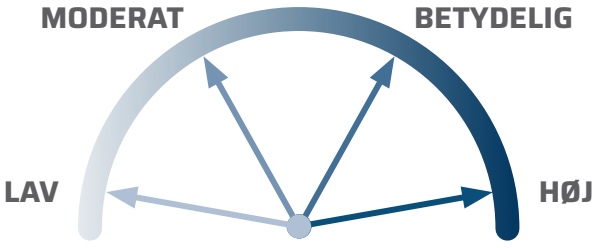
Samrådstale om fremmedkrigere på offentlige ydelser, 30. august 2018. FT.dk

The Swedish Police Authority (2021): *National risk assessment of Money Laundering and Terrorist Financing in Sweden 2020/2021*. FI.se.

Bilag 1

Model til vurdering af særlige risikoområder

Overforstående model, der også fremgår af Den Nationale Risikovurdering af Hvidvask i en lignende udgave, er anvendt til vurderingen af særlige risikoområder for terrorfinansiering. Risikoområderne er hver især karakteriseret ved, at de er afgrænset af en række ydelser og betalingsmidler. Det er i høj grad sårbarhederne relateret til disse ydelser og betalingsmidler, der er omdrejningspunktet for sårbarhedsanalysen.



POLITIETS EFTERRETNINGSTJENESTE
DEN NATIONALE RISIKOVURDERING AF TERRORFINANSIERING
UDGIVELSESÅR: 2023
FOTOS: ADOBE STOCK

		BEGRÆNSET RISIKO	MODERAT RISIKO	BETYDELIG RISIKO	HØJ RISIKO
TRUSSEL	Omfang	Ydelser og betalingsmidler m.m. benyttes så vidt vides ikke eller kun af en lille kreds i ekstremistiske miljøer.	Ydelser og betalingsmidler m.m. opfattes i moderat grad som attraktive til terrorfinansiering i ekstremistiske miljøer.	Ydelser og betalingsmidler m.m. opfattes i betydelig grad som attraktive til terrorfinansiering i ekstremistiske miljøer.	Ydelser og betalingsmidler m.m. opfattes i høj grad som attraktive til terrorfinansiering i ekstremistiske miljøer.
SÅRBARHED	Tilgængelighed	Ydelser og betalingsmidler m.m. er svært tilgængelige, kræver betydelig planlægning, viden og/eller teknisk ekspertise.	Ydelser og betalingsmidler m.m. er forholdsvist tilgængelige, kræver moderat planlægning, viden og/eller teknisk ekspertise.	Ydelser og betalingsmidler m.m. er tilgængelige, kræver lidt eller ingen planlægning, viden og/eller teknisk ekspertise.	Ydelser og betalingsmidler m.m. er let tilgængelige, kræver lidt eller ingen planlægning, viden og/eller teknisk ekspertise.
	Volumen, transaktionsstørrelse og hurtighed i transaktioner	Det samlede antal transaktioner er lavt. Udbyderen er uegnet til terrorfinansiering med høj volumen. Transaktionerne foregår ikke hurtigt.	Det samlede antal transaktioner er moderat. Udbyderen er moderat egnet til terrorfinansiering med høj volumen. Transaktionerne foregår i et moderat tempo.	Det samlede antal transaktioner er betydeligt. Udbyderen er i betydelig grad egnet til terrorfinansiering med høj volumen. Transaktionerne foregår i et betydeligt tempo.	Det samlede antal transaktioner er stort. Udbyderen er i høj grad egnet til terrorfinansiering med høj volumen. Transaktionerne foregår i højt tempo.
	Potentiale for at føre midler ind eller ud af Danmark (grænseoverskridende transaktioner)	Ydelser og betalingsmidler m.m. giver begrænset mulighed for udlandstransaktioner. Det er ikke let at transportere værdier ind eller ud af Danmark.	Ydelser og betalingsmidler m.m. giver moderat mulighed for udlandstransaktioner. Det er moderat tilgængeligt at transportere værdier ind eller ud af Danmark.	Ydelser og betalingsmidler m.m. giver betydelig mulighed for udlandstransaktioner. Det er relativt nemt at føre værdier ind og ud af Danmark.	Ydelser og betalingsmidler m.m. giver i vidt omfang mulighed for udlandstransaktioner. Det er nemt at føre værdier ind eller ud af Danmark.
	Omkostninger	Omkostningerne forbundet med terrorfinansiering er høje. Det er dyrt at udføre terrorfinansiering vha. ydelser og betalingsmidler / risikoen for svind og tab er høj.	Omkostningerne forbundet med terrorfinansiering er betydelige. Det er relativt dyrt at udføre terrorfinansiering vha. ydelser og betalingsmidler / risikoen for svind og tab er betydelig.	Omkostningerne forbundet med terrorfinansiering er moderate. Det er forholdsvist billigt at udføre terrorfinansiering vha. ydelser og betalingsmidler / risikoen for svind og tab er moderat.	Omkostningerne forbundet med terrorfinansiering er lave. Det er billigt at anvende ydelser og betalingsmidler til terrorfinansiering, og/eller risikoen for svind og tab er lav.
	Anonymitet/sandsynlighed for identifikation af kriminel aktivitet	Det er sandsynligt, at det opdages, hvis der forekommer forsøg på terrorfinansiering.	Det er mindre sandsynligt, at det opdages, hvis der forekommer forsøg på terrorfinansiering.	Det er forholdsvist svært at opdage, hvis der forekommer forsøg på terrorfinansiering.	Det er svært at opdage, hvis der forekommer forsøg på terrorfinansiering

POLITIETS EFTERRETNINGSTJENESTE · KLAUSDALSBROVEJ 1 · 2860 SØBORG · +45 45 15 90 07 • PET@PET.DK • WWW.PET.DK