



Wetenschappelijk Onderzoek- en
Datacentrum

Cahier 2024-2

National Risk Assessment Terrorismefinanciering 2023

Cahier 2024-2

National Risk Assessment Terrorismefinanciering 2023

H.C.J. van der Veen
L.F. Heuts

Cahier

De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Inhoud

	Afkortingen	6
	Samenvatting	8
1	Inleiding	16
	1.1 Aanleiding voor het onderzoek	16
	1.2 Wat is terrorismefinanciering?	18
	1.3 Doel, structuur en onderzoeksvragen	21
	1.4 Lessen van de tweede NRA Terrorismefinanciering en de FATF-evaluatie	22
	1.5 Leeswijzer	25
2	Onderzoeksmethodiek	26
	2.1 Sleutelbegrippen	26
	2.2 Uitvoering NRA binnen de ISO 31000 standaard voor risicomanagement	28
	2.3 Ingezette onderzoeksmethoden	28
3	Wat maakt Nederland kwetsbaar voor terrorismefinanciering?	40
	3.1 Geografische en demografische kenmerken	40
	3.2 Religieuze kenmerken	42
	3.3 Sociaal-culturele en politieke kenmerken	42
	3.4 Economische kenmerken	45
	3.5 Criminologische kenmerken	50
	3.6 Terrorisme en terrorismefinanciering	55
	3.7 Tot slot	60
4	Grootste dreigingen terrorismefinanciering	62
	4.1 Girale en contante transacties bij vergunde banken	63
	4.2 Laagdrempelige mogelijkheden om buitenlandse rekeningen te openen	63
	4.3 Internet betaaldiensten (PSP's)	65
	4.4 Girale en/of contante transacties bij vergunde geldtransactiekantoren	65
	4.5 Aanbieders van cryptodiensten	66
	4.6 Onvergonde betaaldienstverleners en hawala-bankieren	66
	4.7 Stichtingen met weinig transparantie over financiën en geen zelfregulering	69
	4.8 Fysieke verplaatsing contant geld en/of grootwaardeproducten	73
	4.9 Legaal verkregen eigen middelen	74
	4.10 Giften (via betaalverzoeken en/of <i>crowdfunding</i> via sociale media)	74
	4.11 Crimineel verkregen middelen: fraude en andere criminaliteitsvormen	76
	4.12 Potentiële impact van grootste tf-dreigingen	76
	4.13 Tot slot	77
5	Weerbaarheid van het beleidsinstrumentarium	79
	5.1 Organisatie van terrorismefinanciering-preventie en -bestrijding	79
	5.2 Beschikbaar beleidsinstrumentarium	80
	5.3 Internationale wet- en regelgeving	81
	5.4 Nationale wet- en regelgeving	83
	5.5 Overige beleidsinstrumenten	88

5.6	Inschatting weerbaarheid beleidsinstrumentarium	90
5.7	Toekomstig beleidsinstrumentarium	92
5.8	Tot slot	93
6	Conclusies	95
6.1	Beantwoording van onderzoeksvragen	95
6.2	Evaluatie van de derde NRA	103
6.3	Lessen voor de volgende NRA	107
	Summary	109
	Literatuur	116
Bijlage 1	Samenstelling begeleidingscommissie	122
Bijlage 2	Lijst van geïnterviewden	123
Bijlage 3	Deelnemers expertmeetings	125
Bijlage 4	FANO-enquête tf-dreigingen en responsoverzicht	126
Bijlage 5	Van longlist naar shortlist grootste tf-dreigingen	131
Bijlage 6	Potentiële impact grootste tf-dreigingen	135
Bijlage 7	Weerbaarheid grootste tf-dreigingen	138
Bijlage 8	Aanvullende analyses	140
Bijlage 9	Kwantitatieve data Justis/TRACK	143

Afkortingen

ABN-AMRO	Algemene Bank Nederland, Amsterdam-Rotterdam Bank
AFM	Autoriteit Financiële Markten
AIO	Anoniem, Internationaal en Ongereguleerd
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMLSC	Standing Committee on anti-money laundering and countering terrorist financing
ANBI	Algemeen Nut Beogende Instelling
ART	Asset-Referenced Token
BCBS	Basel Committee on Banking Supervision
BES	Bonaire, Sint Eustatius en Saba
BFT	Bureau Financieel Toezicht
BBP	Bruto Binnenlands Product
BTWwft	Bureau Toezicht Wwft
CASP	Crypto Asset Service Providers
CBF	Centraal Bureau Fondsenwerving
CBS	Centraal Bureau voor de Statistiek
CCV	Centrum voor Criminaliteitspreventie en Veiligheid
CIA	Central Intelligence Agency
CIO	Interkerkelijk Contact In Overheidszaken
CJIB	Centraal Justitieel Incassobureau
CoMensha	Coördinatiecentrum tegen Mensenhandel
CT	Contraterrorisme
DJI	Dienst Justitiële Inrichtingen
DNB	De Nederlandsche Bank
DTN	Dreigingsbeeld Terrorisme Nederland
DUO	Dienst Uitvoering Onderwijs
EBA	European Banking Authority
ECLI	European Case Law Identifier
EER	Europese Economische Ruimte
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EMT	E-Money Token
ETA	Euskadi Ta Askatasuna
EU	Europese Unie
EVA	<i>Betekenis 1: Europese Vrijhandelsassociatie</i> <i>Betekenis 2: Externe Verwijzingsapplicatie</i>
FANO	Feiten/casus, Aannemelijk, Niet aannemelijk en Onbekend
FATF	Financial Action Task Force
FCI-Net	Financial Criminal Investigations Net
FEC	Financieel Expertise Centrum
FIN	Fondsen in Nederland
FIU	Financial Intelligence Unit
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
G-7	Groep van Zeven
GDR	Group Decision Room
GDSS	Group Decision Support System
iCOV	infobox Crimineel en Onverklaarbaar Vermogen
IBAN	International Bank Account Number
ING	Internationale Nederlanden Groep
IRA	Irish Republican Army
ISIS	Islamitische Staat in Irak en Ahrar Al-Sham
ISKP	Islamitische Staat Khorasan Provincie
ISO	International Organization for Standardization

J5	Joint Chiefs of Global Tax Enforcement
JenV	(Ministerie van) Justitie en Veiligheid
KMar	Koninklijke Marechaussee
KNB	Koninklijke Notariële Beroepsorganisatie
Ksa	Kansspelautoriteit
KvK	Kamer van Koophandel
MCA	Multi Criteria Analyse
MCD	Multi Criteria Decision Analysis
MICAR	Markets in Crypto-Assets Regulation
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NBA	Nederlandse Beroepsorganisatie van Accountants
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NGO	Non-Gouvernementele Organisatie
NOvA	Nederlandse Orde van Advocaten
NRA	National Risk Assessment
NVB	Nederlandse Vereniging van Banken
NVGTK	Nederlandse Vereniging Geld Transactie Kantoren
OFAC	Office of Foreign Assets Control
OM	Openbaar Ministerie
OT	Ongebruikelijke Transactie
OTA	Onafhankelijke Toezichthouder Advocatuur
PKK	Partiya Karkerên Kurdistanê
PPS	Publiek-Private Samenwerking
PSD2	Payment Service Directive 2
PSP	Payment Service Provider
RABO	Raiffeisen Bank, Boerenleenbank
RAF	Rote Armee Fraktion
RPI	Resterende Potentiële Impact
SDN	Specially Designated National
SNRA	Supra National Risk Assessment
SRA	Samenwerkende Registeraccountants en Accountants-Administratieconsulenten
SZW	Sociale Zaken en Werkgelegenheid
TF	Terrorismefinanciering
TFTF	Terrorismefinanciering Taskforce
TMNL	Transactie Monitoring Nederland
TRACK	Toezicht Rechtspersonen, Analyse, Controle & Kennisgeving
UBO	Ultimate Beneficial Owner
VFN	Vereniging van financieringsondernemingen in Nederland
VK	Verenigd Koninkrijk
VN	Verenigde Naties
VNVR	Verenigde Naties Veiligheidsraad
VT	Verdachte Transactie
Wet Bibob	Wet bevordering integriteitsbeoordelingen door het openbaar bestuur
WODC	Wetenschappelijk Onderzoek- en Datacentrum
Wft	Wet op het financieel toezicht
Wiv 2017	Wet op de inlichtingen- en veiligheidsdiensten 2017
Wpe	Wet precursoren voor explosieven
WTO	World Trade Organization
WTR	Wire Transfer Regulation
WvSr	Wetboek van Strafrecht
WvSv	Wetboek van Strafvordering
Wwft	Wet ter voorkoming van witwassen en financieren van terrorisme

Samenvatting

Achtergrond van het onderzoek

Het Nederlandse beleid ter preventie en repressie van terrorismefinanciering is gebaseerd op de aanbevelingen door de *Financial Action Task Force* (FATF) en regelgeving van de Europese Unie (EU). Nederland is als lid van de FATF gebonden aan de aanbevelingen van dit intergouvernementeel orgaan gericht op het nemen van preventieve en repressieve maatregelen gericht op witwassen en terrorismefinanciering, maatregelen ten aanzien van nationale rechtsstelsels en internationale samenwerking. Voor de EU-lidstaten is het grootste deel van de FATF-aanbevelingen omgezet naar verschillende opeenvolgende anti-witwasrichtlijnen. Op grond van deze richtlijnen dienen de EU-lidstaten risicogericht beleid tegen witwassen en terrorismefinanciering te voeren en een *National Risk Assessment* (NRA) vast te stellen. Voor Nederland is de uitvoering van de NRA vastgelegd in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Artikel 1f lid 1 van de Wwft vermeldt dat de Ministers van Financiën en Justitie en Veiligheid (JenV) gezamenlijk een, om de twee jaar te actualiseren, verslag publiceren van de geïdentificeerde, geanalyseerde en beoordeelde nationale risico's op de terreinen van witwassen en het financieren van terrorisme.

Het Wetenschappelijk Onderzoek- en Datacentrum (WODC) heeft in de periode juni 2022 tot en met december 2023 een derde NRA Terrorismefinanciering voor Europees Nederland uitgevoerd.¹ De uitgevoerde risicoanalyse voor de NRA betreft de periode januari 2020² tot en met juni 2023.³ De NRA heeft een vijfledig doel:

- 1 het identificeren van de terrorismefinanciering-dreigingen met de grootste potentiële impact (ofwel de grootste tf-dreigingen);
- 2 het vaststellen van de hoogte van de potentiële impact van de grootste tf-dreigingen;
- 3 het bepalen van de hoogte van de weerbaarheid van het beleidsinstrumentarium ter preventie en/of repressie van de grootste tf-dreigingen;
- 4 het bieden van inzicht in de aard en mechanismen van de grootste tf-dreigingen; en
- 5 het bepalen van het risiconiveau van de grootste tf-dreigingen door de potentiële impact van de dreigingen af te zetten tegen de weerbaarheid van het beleidsinstrumentarium.

¹ Sinds 2017 zijn voor Europees Nederland twee eerdere NRA's op het terrein van terrorismefinanciering uitgevoerd door het WODC. Daarnaast zijn er sindsdien twee NRA's Witwassen uitgevoerd voor Europees Nederland. Voor Caribisch Nederland zijn sinds 2017 ook twee NRA's uitgevoerd, die betrekking hadden op zowel witwassen als terrorismefinanciering. Parallel aan de uitvoering van de derde NRA Terrorismefinanciering heeft het WODC de derde NRA op het terrein van witwassen uitgevoerd (voor Europees Nederland).

² Er wordt uitgegaan van januari 2020 omdat de risicoanalyse van de vorige NRA Terrorismefinanciering betrekking had op de periode tot eind 2019.

³ De gegevens die de basis vormen voor de risicoanalyse in de NRA, zijn verzameld in drie expertmeetings. De laatste expertmeeting vond plaats in juni 2023.

Onderzoeksmethodiek

De structuur van de derde NRA wordt – net als in de eerdere NRA's – bepaald door het ISO 31000 raamwerk voor risicomanagement. De gehanteerde onderzoeksmethodiek kent de volgende onderdelen:

- Een contextanalyse waarin de specifieke kenmerken van Nederland zijn geschetst die van invloed kunnen zijn op de prevalentie van terrorismefinanciering en de potentiële impact daarvan. Deze factoren kunnen een rol spelen bij het bepalen van de in te zetten financieringsmethoden en de te gebruiken financieringsbronnen. Voor deze contextanalyse is een literatuurstudie verricht en zijn relevante kwantitatieve databronnen geraadpleegd.
- Ten behoeve van een inventarisatie van tf-dreigingen zijn recente (sinds 2020 verschenen) rapporten bestudeerd, waaronder de Europese *Supra National Risk Assessment* (SNRA), en is de zogeheten FANO-enquête⁴ uitgezet onder publieke en private partijen met een taak bij de preventie en/of bestrijding van terrorismefinanciering.
- In de eerste expertmeeting hebben vertegenwoordigers van expertorganisaties⁵ de tf-dreigingen met de volgens hen grootste potentiële impact geïdentificeerd.
- In de periode na de eerste expertmeeting is in verdiepende interviews met vertegenwoordigers van expertorganisaties en andere partijen met een taak bij het tegengaan van terrorismefinanciering nader ingegaan op de aard, mechanismen en casuïstiek van de dreigingen die op de voorlopige shortlist van grootste tf-dreigingen stonden.
- In de tweede expertmeeting is – naar aanleiding van de bevindingen van de interviews – de shortlist van grootste tf-dreigingen aangepast en vastgesteld, waarna de experts de potentiële impact van de 12 grootste tf-dreigingen hebben ingeschat aan de hand van een Multi Criteria Analyse (MCA).
- In de derde expertmeeting hebben experts voor elk van de grootste tf-dreigingen de weerbaarheid van het totale beschikbare beleidsinstrumentarium ingeschat. Dit betreft de mate waarin het totaal beschikbare beleidsinstrumentarium de dreiging tegengaat.
- Door de ingeschatte potentiële impact van de tf-dreigingen af te zetten tegen de ingeschatte weerbaarheid is inzicht verkregen in het risiconiveau van de grootste tf-dreigingen.
- Voor alle 12 dreigingen zijn bij een aantal publieke organisaties dataverzoeken ingediend en zijn zoveel mogelijk beschikbare kwantitatieve data evenals recente casuïstiek opgenomen in de rapportage.
- Tot slot zijn in de eindfase van het onderzoek de resultaten van het onderzoek gevalideerd. Het betreft validerende interviews met acht experts werkzaam bij zes sleutelorganisaties afgenomen met als belangrijkste doel na te gaan in hoeverre zij het risiconiveau van de 12 grootste tf-dreigingen herkennen. Daarnaast is voor acht dreigingen in deze derde NRA Terrorismefinanciering die ook terugkomen in de lijst

⁴ In deze *online* enquête is aan de respondenten gevraagd om bij de toegestuurde longlist van dreigingen aan te geven of zij vanuit hun eigen werkzaamheden ervaring hebben met feiten/casus van de dreigingen en in hoeverre zij de prevalentie van de dreigingen al dan niet aannemelijk achten op basis van de bij hun organisatie beschikbare informatie. FANO staat voor Feiten/casus, Aannemelijk, Niet aannemelijk en Onbekend.

⁵ Het betreft publieke en private organisaties die een taak hebben bij de preventie en/of repressie van terrorismefinanciering. In deze NRA zijn dat opsporingsinstanties, handhavers, Wwft-toezichthouders en de brancheorganisatie van de bankensector (de Nederlandse Vereniging van Banken, NVB).

van grootste dreigingen van de parallel uitgevoerde NRA voor witwassen, de samenhang bepaald.

Grootste terrorismefinanciering-dreigingen

Uit een longlist van 27 tf-dreigingen hebben tf-experts in de eerste expertmeeting de tien dreigingen geïdentificeerd die naar hun oordeel binnen de Nederlandse context het hoogst scoorden op potentiële impact. Dit leidde tot een voorlopige shortlist van 15 grootste tf-dreigingen, die in de tweede expertmeeting is ingeperkt tot 12 dreigingen. De NRA legt de focus op deze definitieve shortlist van 12 grootste tf-dreigingen die in tabel S1 gecategoriseerd worden weergegeven omdat de grootste dreigingen qua potentiële impact niet veel uiteenlopen.

Tabel S1 Potentiële impact grootste tf-dreigingen (n=8)

Dreiging	Potentiële impact (op een schaal van 0-100)
Score-categorie '60 of meer'	
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	61
Score-categorie '55 tot en met 59'	
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	58
Financiering met middelen verkregen via horizontale/verticale fraude	57
Financiering via girale of contante transacties bij vergunde banken	57
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering	56
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	55
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	55
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude	55
Score-categorie '50 tot en met 54'	
Financiering met legaal verkregen eigen middelen	50
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	50
Financiering via internet betaaldiensten (<i>Payment Service Providers</i>)	50
Score-categorie 'minder dan 50'	
Financiering via aanbieders van cryptodiensten	48

De tf-dreigingen in tabel S1 betreffen financieringsmethoden en -bronnen die in verschillende combinaties van twee of meerdere dreigingen een tf-constructie kunnen vormen. Zo'n constructie kan vrij eenvoudig van aard zijn, maar kan ook een complex karakter hebben. De dreiging 'financiering via onvergunde betaaldienstverleners en hawala-bankieren' kreeg van de 12 dreigingen de hoogste score, namelijk een score van 61 op een schaal van 0-100. Het laagst in deze lijst met grootste tf-dreigingen

staat 'financiering via aanbieders van cryptodiensten' (score 48). Onderstaande tabel maakt duidelijk dat de potentiële impact van de 12 dreigingen niet in sterke mate van elkaar verschilt (de scores liggen immers tussen 48 en 61).

Weerbaarheid van het beleidsinstrumentarium

Het beschikbare beleidsinstrumentarium ter voorkoming en bestrijding van terrorismefinanciering omvat alle relevante instrumenten die voortvloeien uit internationale en nationale wet- en regelgeving, wet- en regelgeving op gemeentelijk niveau, sectorale en branchegerichte regelgeving, en regelgeving op organisatieniveau. In deze NRA worden ook samenwerkingsverbanden tussen publieke en/of private organisaties en richtlijnen, handreikingen en beleidsplannen van organisaties die een rol spelen bij de preventie en/of bestrijding van terrorismefinanciering, gezien als beleidsinstrument. Tabel S2 geeft een overzicht van het beleidsinstrumentarium dat tot en met juni 2023 – de maand waarin de derde expertmeeting plaatsvond – beschikbaar was ter preventie en bestrijding van terrorismefinanciering.

Tf-experts hebben in de derde expertmeeting voor de 12 grootste tf-dreigingen een inschatting gemaakt van de mate waarin het totale pakket aan bestaande beleidsinstrumenten de potentiële impact van de dreigingen tegengaat. De resultaten van de expertmeeting worden gecategoriseerd weergegeven in tabel S3. Experts zijn bij hun inschatting van de weerbaarheid van het beleidsinstrumentarium uitgegaan van de beleidsinstrumenten die op dat moment (juni 2023) waren geïmplementeerd.

Tabel S2 Beleidsinstrumentarium ter preventie en bestrijding van terrorismefinanciering

Internationale wet- en regelgeving	Nationale wet- en regelgeving	Overige beleidsinstrumenten
<ul style="list-style-type: none"> FATF-aanbevelingen EU anti-witwasrichtlijnen Verenigde Naties Veiligheidsraad Resoluties en EU Verordeningen Overige internationale sanctielijsten Europese verordening Aangifte liquide middelen <i>Wire Transfer Regulation 2</i> 	<ul style="list-style-type: none"> Wet ter voorkoming van witwassen en financieren van terrorisme⁶ Sanctiewet 1977 en sanctieregelingen Wetboek van Strafrecht Wetboek van Strafvordering Wet op de inlichtingen- en veiligheidsdiensten 2017 Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding Wet precursoren voor explosieven Wet op het financieel toezicht Algemene Douanewet Wet controle op rechtspersonen Handelsregisterwet 2007 (inclusief UBO-registers) Fiscale wetgeving Sociale wetgeving Wet op de economische delicten Wet Bibob 	<ul style="list-style-type: none"> Nationale samenwerkingsverbanden Internationale samenwerkingsverbanden Sectorale regelgeving en voorwaarden Richtlijnen, handreikingen en beleidsplannen

Bij drie tf-dreigingen oordelen de experts dat de weerbaarheid van het beleidsinstrumentarium de potentiële impact met meer dan de helft tegengaat (scores groter dan 50), namelijk bij financiering via girale of contante transacties bij vergunde banken (score 58), met middelen verkregen via horizontale/verticale fraude (score 57) en via girale of contante transacties bij vergunde geldtransactiekantoren (score 54). De vier tf-dreigingen met de laagste weerbaarheidsscore hebben allen een score lager dan 30: financiering via onvergunde betaaldienstverleners en hawala-bankieren (score 28), met legaal verkregen eigen middelen (score 27), via aanbieders van cryptodiensten (score 25) en via laagdrempelige (*online*) mogelijkheden om buitenlandse bankrekening te openen (score 23). De lage scores houden dus in dat het totale beleidsinstrumentarium deze tf-dreigingen – volgens experts – slechts in relatief beperkte mate tegengaat. Onderstaande tabel laat zien dat de weerbaarheid van het beleidsinstrumentarium sterk kan verschillen tussen de 12 grootste tf-dreigingen (de scores liggen namelijk tussen 23 en 58).

⁶ In Nederland verplicht de Wet ter voorkoming van witwassen en financieren van terrorisme een groot aantal instellingen om ongebruikelijke transacties te melden bij de *Financial Intelligence Unit – Nederland*.

Tabel S3 Weerbaarheid beleidsinstrumentarium per grootste tf-dreiging (n=6)

Dreiging	Weerbaarheid <i>(op een schaal van 0-100)</i>
Score-categorie '50 of meer'	
Financiering via girale of contante transacties bij vergunde banken	58
Financiering met middelen verkregen via horizontale/verticale fraude	57
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	54
Score-categorie '40 tot en met 49'	
Financiering via internet betaaldiensten (<i>Payment Service Providers</i>)	41
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering	41
Score-categorie '30 tot en met 39'	
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	39
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude	36
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	34
Score-categorie '20 tot en met 29'	
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	28
Financiering met legaal verkregen eigen middelen	27
Financiering via aanbieders van cryptodiensten	25
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	23

Ondanks de mitigerende werking van het beschikbare instrumentarium op de 12 grootste tf-dreigingen, kunnen deze dreigingen dus nog steeds in meer of mindere mate impact hebben. De mitigerende werking hangt samen met de mate waarin het AIO-principe⁷ van toepassing is op de tf-dreigingen. Bij de meeste tf-methoden zijn één of meer van de drie AIO-componenten van toepassing. Hoe meer de AIO-elementen van toepassing zijn bij de tf-dreigingen, hoe lager de weerbaarheid van het beleidsinstrumentarium ter preventie en repressie van de dreigingen.

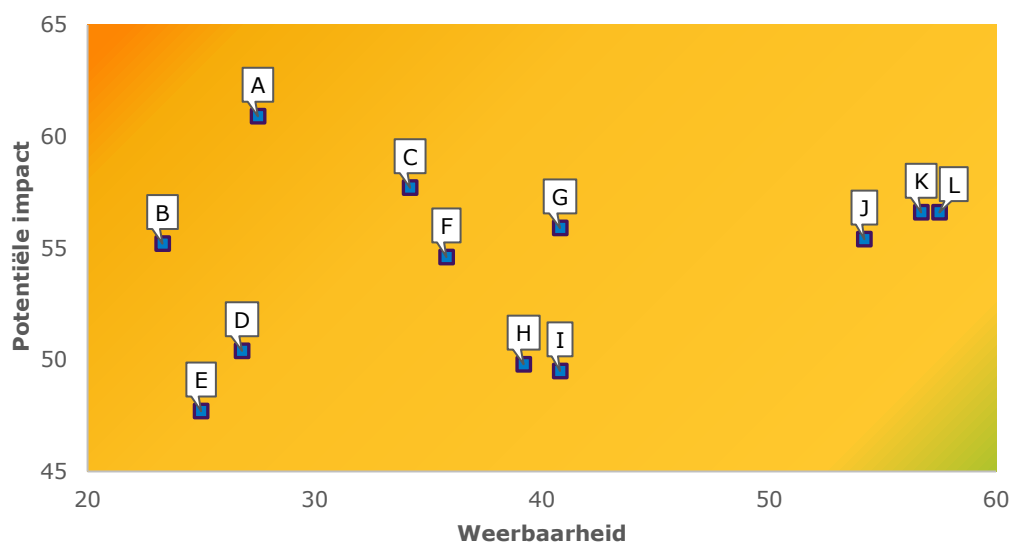
Risiconiveau grootste terrorismefinanciering-dreigingen

In figuur S1 worden in een *heatmap* de expertinschattingen van de potentiële impact en de weerbaarheid van het beleidsinstrumentarium voor de 12 grootste tf-dreigingen tegen elkaar afgezet. De hoogste risico's zijn de dreigingen met een hoge potentiële impact en waarbij sprake is van een lage weerbaarheid van het beschikbare beleidsinstrumentarium. Deze *heatmap* kan worden gezien als samenvatting van de

⁷ AIO staat voor Anonimiteit (de methode verhuult de identiteit van de financier van terrorisme), Internationaal (de methode heeft een internationaal karakter en wordt via of vanuit het buitenland ingezet) en Ongereguleerd (de methode heeft betrekking op c.q. wordt ingezet in een ongereguleerde sector).

derde NRA Terrorismefinanciering. Wel dient hierbij in ogenschouw te worden gehouden dat de *heatmap* alleen de grootste tf-dreigingen weergeeft en dat de andere dreigingen die zijn opgenomen in de longlist en eveneens deel uitmaken van de NRA, door de experts als minder hoog risico worden gezien.

Figuur S1 Heatmap derde NRA: potentiële impact afgezet tegen weerbaarheid voor de grootste tf-dreigingen^a



A	Onvergonde betaaldienstverleners en hawala-bankieren	G	Stichtingen met weinig transparantie over financiën en geen zelfregulering
B	Laagdrempelige (<i>online</i>) mogelijkheden openen buitenlandse bankrekening	H	Giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media
C	Fysieke verplaatsing (grote hoeveelheden) contant geld/grootwaardeproducten	I	Internet betaaldiensten (<i>Payment Service Providers</i>)
D	Legaal verkregen eigen middelen	J	Girale/contante transacties vergunde geldtransactiekantoren
E	Aanbieders cryptodiensten	K	Middelen verkregen via horizontale/verticale fraude
F	Middelen verkregen via andere criminaliteitsvorm dan fraude	L	Girale/contante transacties bij vergunde banken

a Om zo duidelijk mogelijk de verschillen in beeld te brengen is de weergegeven figuur een uitsnede uit een figuur met assen die lopen van 0 tot en met 100, waarbij de kleuren verlopen van linksboven: rood (hoogste potentiële impact en laagste weerbaarheid) naar rechtsonder: groen (laagste potentiële impact en hoogste weerbaarheid). De volledige figuur is opgenomen in bijlage 8, figuur B8.1.

De figuur laat zien dat het risiconiveau van de 12 grootste tf-dreigingen niet sterk van elkaar afwijkt. Dit geldt met name voor de potentiële impactscores die uiteenlopen van 48 tot 61. De weerbaarheid tegen de dreigingen laat een grotere spreiding zien. Alle dreigingen bevinden zich in het oranje gebied. Van al deze risicovolle tf-dreigingen hebben de volgende twee dreigingen het hoogste risiconiveau (het meest linksboven in de figuur weergegeven):

- *Financiering via onvergonde betaaldienstverleners en hawala-bankieren (A in figuur S1)*. Met name door een laag ingeschatte weerbaarheid heeft deze tf-dreiging zo'n hoog risiconiveau. De dreiging biedt – volgens het AIO-principe – mogelijkheden

om op anonieme wijze geld over te maken, heeft een internationaal karakter en wordt veelal via en/of naar het buitenland ingezet, en heeft betrekking op een ongereguleerde 'sector'. Verder is deze tf-methode relatief eenvoudig toegankelijk voor individuen, groepen en/of organisaties die terrorisme willen financieren.

- *Financiering via laagdrempelige (online) mogelijkheden om een buitenlandse bankrekening te openen (B)*. Bij deze tf-dreiging wordt het hoge risiconiveau met name door een zeer laag ingeschatte weerbaarheid veroorzaakt. Dit is te relateren aan het feit dat sommige digitale buitenlandse bankrekeningen relatief eenvoudig – met, afhankelijk van het land, mogelijk minder strenge tf-regelgeving en -toezicht ten aanzien van financiële dienstverleners – geopend kunnen worden en dat er momenteel geen beleidsinstrumentarium bestaat om dit aan te pakken. Zodra iemand eenmaal beschikt over een buitenlandse bankrekening, kan hij of zij transacties naar, via of vanuit deze rekening laten lopen, die lastig zijn te monitoren door Nederlandse banken en minder inzichtelijk zijn voor opsporingsdiensten die daardoor over een minder goede informatiepositie beschikken.

Van de 12 grootste tf-dreigingen ligt het minst hoge risiconiveau bij de vier tf-dreigingen die het meest rechtsonder in de figuur staan: financiering 'via internet betaaldiensten (*Payment Service Providers*)' (I), via 'girale/contante transacties bij vergunde geldtransactiekantoren' (J), via middelen verkregen via horizontale/verticale fraude (K) en via 'girale/contante transacties bij vergunde banken' (L). Hoewel bij deze dreigingen nog steeds sprake is van een aanzienlijk risiconiveau, wordt hun risiconiveau verhoudingsgewijs het laagst ingeschat. Dat relatief lage risiconiveau wordt met name veroorzaakt door de hoog ingeschatte weerbaarheid, wat te relateren is aan de verbetering van het cliëntonderzoek en transactiemonitoring in de afgelopen jaren door zowel vergunde banken als vergunde geldtransactiekantoren.

1 Inleiding

1.1 Aanleiding voor het onderzoek

Het Nederlandse beleid ter preventie en repressie⁸ van terrorismefinanciering is gebaseerd op de aanbevelingen door de *Financial Action Task Force* (FATF, 2012-2023). en regelgeving van de Europese Unie (EU). De FATF is een intergouvernamenteel orgaan, opgericht door de G-7⁹ in 1989, dat zich richt op het op mondiaal niveau voorkomen en bestrijden van witwassen, de financiering van terrorisme en andere hieraan verwante bedreigingen voor de integriteit van het internationale financiële stelsel. Leden van de FATF, waaronder Nederland, zijn gebonden aan de aanbevelingen gericht op het nemen van preventieve en repressieve maatregelen tegen witwassen en terrorismefinanciering, maatregelen ten aanzien van nationale rechtsstelsels en internationale samenwerking. Daarnaast ziet de FATF toe op de juiste werking en de effectiviteit van die (wettelijke) regels.¹⁰ Voor de EU-lidstaten is het grootste deel van de FATF-aanbevelingen omgezet naar verschillende opeenvolgende anti-witwasrichtlijnen. Op grond van deze richtlijnen dienen de EU-lidstaten risicogericht beleid tegen witwassen en terrorismefinanciering te voeren en een *National Risk Assessment* (NRA) vast te stellen. Voor Nederland is de uitvoering van de NRA vastgelegd in de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Artikel 1f lid 1 van de Wwft vermeldt dat de Ministers van Financiën en Justitie en Veiligheid (JenV) gezamenlijk een, om de twee jaar te actualiseren, verslag publiceren van de geïdentificeerde, geanalyseerde en beoordeelde nationale risico's op de terreinen van witwassen en het financieren van terrorisme.¹¹

De uitgangspunten voor de NRA zijn in 2016 vastgesteld in een methoden- en dataverkenning die het Wetenschappelijk Onderzoek- en Datacentrum (WODC) in samenwerking met de Universiteit Utrecht uitvoerde. Sindsdien bepaalt de ISO 31000 standaard voor risicomanagement de structuur van de NRA's. Andere uitgangspunten die nog steeds van toepassing zijn, betreffen de wetenschappelijke benadering, de (mede) gerichtheid op in Nederland nog niet gesignaleerde risico's en de risico's die zich in de toekomst kunnen materialiseren. Ook zouden voor de risicoanalyses voor witwassen en terrorismefinanciering van de start af aan afzonderlijke NRA's uitgevoerd moeten worden. Om te kunnen leren van ervaringen bij de uitvoering van de NRA's en te kunnen profiteren van voortschrijdende inzichten zou er transparant moeten worden gerapporteerd en zouden de NRA's een zelfevaluatie moeten bevatten. Hiermee kregen de NRA's het karakter van een groeimodel (Van der Veen & Ferwerda, 2016).

In 2017 voerde het WODC de eerste NRA's voor witwassen en terrorismefinanciering uit voor het Europese deel van Nederland, gevolgd door een tweede NRA op beide terreinen in 2020 (Van der Veen & Heuts, 2017a, 2017b, 2020a, 2020b). Ook voor

⁸ In deze NRA worden de begrippen 'repressie' en 'bestrijding' als synoniem gezien. Ter afwisseling worden in dit rapport beide begrippen gebruikt.

⁹ De G-7 is een intergouvernamenteel forum van zeven vooraanstaande industriële staten en de Europese Unie. Het gaat om Canada, Duitsland, Frankrijk, Italië, Japan, het Verenigd Koninkrijk, de Verenigde Staten en de Europese Unie.

¹⁰ [Home \(fatf-gafi.org\)](https://www.fatf-gafi.org/).

¹¹ [wetten.nl - Regeling - Wet ter voorkoming van witwassen en financieren van terrorisme - BWBR0024282 \(overheid.nl\)](https://wetten.nl/Regeling-Wet%20ter%20voorkoming%20van%20witwassen%20en%20financieren%20van%20terrorisme-BWBR0024282-overheid.nl).

Caribisch Nederland – ofwel de eilanden Bonaire, Sint Eustatius en Saba – voerde het WODC tweemaal een NRA op het terrein van zowel witwassen als terrorismefinanciering uit (Van der Veen & Heuts, 2018, 2021).¹²

Uit het *Mutual Evaluation Report* van de FATF ten aanzien van het Nederlands beleid tegen witwassen en terrorismefinanciering uit 2022 valt af te leiden dat de resultaten van de NRA's inmiddels een brede toepassing vinden (FATF, 2022). Toezichthouders, opsporings- en handhavingsorganisaties die zijn belast met de preventie en repressie van witwassen en terrorismefinanciering, worden verondersteld bij de inrichting van hun werkprocessen rekening te houden met de risicobepaling in de NRA's. Ook de Algemene Rekenkamer maakt in een rapport over de witwasbestrijding in Nederland de brede toepassing van de resultaten van de NRA's inzichtelijk (Algemene Rekenkamer, 2022). Hoewel dit rapport zich richt op anti-witwasbeleid en niet specifiek op anti-terrorismefinancieringsbeleid, geldt de boodschap in het rapport in principe voor zowel de NRA Witwassen als de NRA Terrorismefinanciering. Volgens de Algemene Rekenkamer vormen de witwasrisico's die zijn geprioriteerd in de NRA's de basis voor de activiteiten binnen de meldketen voor ongebruikelijke transacties (OT's). De *Financial Intelligence Unit* (FIU) Nederland, de Nationale Politie, de Fiscale Inlichtingen- en Opsporingsdienst (FIOD)¹³ en het Openbaar Ministerie (OM) gebruiken de geprioriteerde witwasrisico's om de focus van hun werkzaamheden te bepalen. Ditzelfde geldt in feite ook voor de risico's die naar voren komen in de NRA Terrorismefinanciering.

Voor Europees Nederland is nu een derde NRA Terrorismefinanciering uitgevoerd, die net als de eerdere NRA's als doel heeft de grootste risico's op het terrein van terrorismefinanciering in kaart te brengen en te prioriteren. Daartoe zijn de terrorismefinanciering-dreigingen (vanaf nu: tf-dreigingen) met de grootste potentiële impact geïdentificeerd, is een inschatting gemaakt van de impact die deze dreigingen kunnen hebben en is de 'weerbaarheid'¹⁴ van het beleidsinstrumentarium gericht op de preventie en/of repressie van terrorismefinanciering bepaald. Het WODC heeft de voorliggende NRA in de periode juni 2022 tot en met december 2023 uitgevoerd. De uitgevoerde risicoanalyse voor de NRA heeft betrekking op de periode januari 2020¹⁵ tot en met juni 2023.¹⁶

Parallel aan de uitvoering van de derde NRA Terrorismefinanciering is de derde NRA op het terrein van witwassen uitgevoerd (voor Europees Nederland).

¹² Er is destijds voor gekozen om voor het Europese en Caribische deel van Nederland afzonderlijke NRA's uit te voeren vanwege de aanzienlijke verschillen wat betreft geografische, demografische, economische en sociaal-culturele kenmerken die de gebieden meer of minder kwetsbaar kunnen maken voor witwassen en terrorismefinanciering. Ook bestaan er verschillen tussen beide gebieden wat betreft het beschikbare beleidsinstrumentarium om de dreigingen tegen te gaan evenals de wijze waarop daaraan uitvoering wordt gegeven.

¹³ Hoewel de afkorting FIOD hier voluit wordt geschreven, hanteert de organisatie zelf alleen nog de afkorting.

¹⁴ Bij weerbaarheid gaat het om de werking van het beleidsinstrumentarium, waarbij geldt: hoe hoger de weerbaarheid, hoe beter de dreigingen worden tegengegaan. Het betreft zowel de inhoud/strekking als de uitvoering van de beleidsinstrumenten.

¹⁵ Er wordt uitgegaan van januari 2020 omdat de risicoanalyse van de vorige NRA Terrorismefinanciering betrekking had op de periode tot eind 2019.

¹⁶ De gegevens die de basis vormen voor de risicoanalyse in de NRA, zijn verzameld in drie expertmeetings. De laatste expertmeeting vond plaats in juni 2023.

1.2 Wat is terrorismefinanciering?

Deze paragraaf gaat in op wat verstaan kan worden onder terrorisme en de financiering daarvan, en geeft een toelichting op de inhoudelijke afbakening van deze NRA.

Terrorisme

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) hanteert de volgende definitie van terrorisme¹⁷: *'het uit ideologische motieven (voorbereiden van het) plegen van op mensenlevens gericht geweld of het veroorzaken van maatschappij-ontwrichtende schade, met als doel (een deel van) de bevolking ernstige vrees aan te jagen, maatschappelijke veranderingen te bewerkstelligen en/of politieke besluitvorming te beïnvloeden.'*¹⁸ De definitie van terrorisme volgens de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) sluit hierop aan (maar wel met een licht afwijkende formulering).¹⁹

Schulten et al. (2019) onderscheiden vijf vormen van terrorisme:

- religieus gemotiveerd terrorisme, zoals de terroristische activiteiten van ISIS (Islamitische Staat in Irak en Ahrar Al-Sham) en Al Qa'ida;
- rechts-extremistisch gemotiveerd terrorisme, zoals de rechts-terroristische aanslag in het Nieuw-Zeelandse Christchurch gericht tegen moslims in 2019;
- links-extremistisch gemotiveerd terrorisme, zoals de terroristische activiteiten die de Rote Armee Fraktion (RAF) in de periode 1970-1998 in Duitsland verrichtten;
- nationalistisch en separatistisch gemotiveerd terrorisme, zoals de terroristische activiteiten van de Irish Republican Army (IRA) in Ierland, de Partiya Karkerên Kurdistanê (Koerdische Arbeiderspartij PKK) in Turkije en Iraaks-Koerdistan, en de Euskadi Ta Askatasuna (ETA) in Spanje;
- *single-issue* gemotiveerd terrorisme, zoals de terroristische activiteiten van (groepen) personen met een ideologisch motief wat betreft 'single issues' als anti-abortus of dierenrechten.

Terroristische daden kunnen gepleegd worden door organisaties of groepen maar ook door individuen:

- terroristische organisaties variëren qua organisatiegraad. Het kan gaan om omvangrijke en complexe organisaties als ISIS, Al Qa'ida en Boko Haram, maar ook om kleine gedecentraliseerde groepen met een platte organisatie;
- individuen die terroristische daden plegen, zogeheten *lone actors*, zijn niet direct verbonden aan een terroristisch netwerk (De Goede, 2007) maar handelen tegelijkertijd zelden zonder enige externe invloed of ondersteuning (zij kunnen toch zijn beïnvloed door de ideologieën van terroristische organisaties waarmee ze *online* of *offline* contact hebben of hadden) (Egmont Group of Financial Intelligence Units, 2019, Van Wonderen et al., 2023).

¹⁷ Het Wetboek van strafrecht bevat geen definitie voor de term terrorisme.

¹⁸ [Terrorisme | AIVD](#).

¹⁹ [Definities gebruikt in het Dreigingsbeeld Terrorismen Nederland | Dreigingsbeeld Terrorismen Nederland | Nationaal Coördinator Terrorismebestrijding en Veiligheid \(nctv.nl\)](#). De NCTV hanteert de volgende definitie voor terrorisme: 'het uit ideologische motieven plegen van op mensenlevens gericht geweld, dan wel het aanrichten van maatschappij-ontwrichtende zaakschade, met als doel maatschappelijke ondermijning en destabilisatie te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden'.

Terrorismedinanciering

Artikel 421 van het Wetboek van Strafrecht (WvSr) gaat in op de strafbaarstelling van het financieren van terrorisme. Hierin staat het volgende:

- 1 Als schuldig aan het financieren van terrorisme wordt gestraft met een gevangenisstraf van ten hoogste acht jaren of geldboete van de vijfde categorie:
 - a. *hij die zich of een ander opzettelijk middelen of inlichtingen verschaft dan wel opzettelijk voorwerpen verzamelt, verwerft, voorhanden heeft of aan een ander verschaft, die geheel of gedeeltelijk, onmiddellijk of middellijk, dienen om geldelijke steun te verlenen aan het plegen van een terroristisch misdrijf of een misdrijf ter voorbereiding of vergemakkelijking van een terroristisch misdrijf;*
 - b. *hij die zich of een ander opzettelijk middelen of inlichtingen verschaft dan wel opzettelijk voorwerpen verzamelt, verwerft, voorhanden heeft of aan een ander verschaft, die geheel of gedeeltelijk, onmiddellijk of middellijk, dienen om geldelijke steun te verlenen aan het plegen van een van de misdrijven omschreven in:*
 - *de artikelen 117 tot en met 117b alsmede artikel 285, indien dat misdrijf is gericht tegen een internationaal beschermd persoon of diens beschermde goederen;*
 - *de artikelen 79 en 80 van de Kernenergiewet, de artikelen 161quater, 173a en 284a alsmede de artikelen 140, 157, 225, 310 tot en met 312, 317, 318, 321, 322 en 326, indien het feit opzettelijk wederrechtelijk handelen betreft met betrekking tot kernmateriaal;*
 - *de artikelen 162, 162a, 166, 168, 282a, 352, 385a tot en met 385d;*
 - *de artikelen 92 tot en met 96, 108, 115, 121 tot en met 123, 140, 157, 161, 161bis, 161sexies, 164, 170, 172, 287, 288 en 289, indien het feiten betreft die worden gepleegd door middel van het opzettelijk wederrechtelijk tot ontlading of ontploffing brengen van een springstof of ander voorwerp, of het laten vrijkomen, verspreiden of inwerken van een voorwerp, waardoor levensgevaar, gevaar voor zwaar lichamelijk letsel voor een ander of aanzienlijke materiële schade te duchten is.*
- 2 Onder voorwerpen worden verstaan alle zaken en alle vermogensrechten.

Kort samengevat gaat het dus om het opzettelijk (1) verschaffen van middelen of inlichtingen aan zichzelf of een ander, (2) verzamelen, verwerven of voorhanden hebben van voorwerpen voor zichzelf of een ander, en (3) aan een ander verschaffen van voorwerpen, bedoeld om deels of volledig en (on)middelbaar financiële steun te verlenen aan het plegen van een terroristisch misdrijf, een misdrijf ter voorbereiding of vergemakkelijking van een terroristisch misdrijf of aan het plegen van één van de misdrijven omschreven in een groot aantal artikelen in de WvSr. In deze NRA Terrorismedinanciering wordt niet nader ingegaan op alle misdrijven die onder de noemer 'terroristisch' geschaard kunnen worden; bovenstaande verwijzingen naar de betreffende criminaliteitsvormen volstaat voor deze NRA.

Uit de WvSr blijkt ook dat terrorismedinanciering breder opgevat kan worden dan alleen het verlenen van financiële steun. Het OM geeft aan dat het een verzamelnaam is voor alle vormen van bijstand aan terroristische groeperingen of individuele personen met terroristisch oogmerk, waaronder het werven van fondsen, het voorhanden hebben van geld dat dient om een aanslag te financieren, het geven van

informatie over financiering en het beschikbaar stellen van goederen, diensten of financiële steun.²⁰

De (financiële) middelen die gebruikt worden voor terrorismefinanciering, kunnen een criminele maar ook een legale *herkomst* hebben. De *bestemming* van (financiële) middelen kan sterk verschillen: middelen kunnen worden verstrekt ten behoeve van het levensonderhoud van een terrorist en/of zijn voorbereidingen om een aanslag te plegen, maar ook ten behoeve van de organisatiekosten van een terroristische groep of organisatie en/of hun voorbereidingen voor terroristische activiteiten. Deze verschillende mogelijke bestemmingen van (financiële) middelen worden in deze NRA samengenomen onder de noemer 'terrorisme'.

Inhoudelijke afbakening van deze NRA

In deze derde NRA Terrorismefinanciering gaat het bij terrorismefinanciering om:

- de financiering van terroristische activiteiten in Nederland, al dan niet vanuit het buitenland; en
- de financiering van terroristische activiteiten in het buitenland vanuit Nederland.

De NRA richt zich specifiek op de financiering van terrorisme en dus niet op de financiering van activiteiten die door de AIVD en de NCTV niet onder de noemer 'terrorisme' geschaard worden. De financiering van extremisme vormt dus geen onderdeel van de NRA. De AIVD en de NCTV beschrijven extremisme als '*het uit ideologische motieven bereid zijn om niet-gewelddadige²¹ en/of gewelddadige²² activiteiten te verrichten die de democratische rechtsorde ondermijnen*'.²³ Extremisme kan volgens de AIVD in zijn uiterste vorm tot terrorisme leiden, namelijk als maatschappij-ontwrichtende schade wordt aangericht en/of grote groepen mensen angst wordt aangejaagd.²⁴

Omdat de huidige terroristische dreiging voor Nederland volgens de AIVD en NCTV vooral jihadistisch van aard is (zoals toegelicht zal worden in hoofdstuk 3) en omdat er in de periode 2020-2022 geen sprake is geweest van andere vormen van terrorisme in Nederland (Institute for Economics & Peace, 2023) – waardoor er ook weinig tot geen kennis over de financiering hiervan bestaat bij expertorganisaties op het terrein van terrorismefinanciering – legt deze NRA de focus op de financiering van jihadistisch terrorisme. Wel zal in hoofdstuk 3 kort stilgestaan worden bij een terroristische dreiging vanuit rechts-extremistische hoek, waarvan expertorganisaties verwachten dat die dreiging de komende jaren kan toenemen.

²⁰ [Hoe maken jullie het onderscheid tussen financiering van humanitaire hulp en financiering van terrorisme? | Openbaar Ministerie \(om.nl\)](#).

²¹ Als voorbeelden van niet-gewelddadige ondemocratische middelen noemt de AIVD systematisch haatzaaien, angst verspreiden, doelbewust desinformatie verspreiden, demoniseren en intimideren, het verwerpen van wet en regelgeving, en het doen van pogingen om een parallelle samenleving tot stand te brengen waarbij het gezag van de Nederlandse overheid en het rechtssysteem wordt afgewezen

²² Als voorbeelden van gewelddadige methodes noemt de AIVD geweldplegingen, mishandelingen of ernstiger vormen van geweld.

²³ [Extremisme | AIVD](#) en [Extremisme | Nationaal Coördinator Terrorismebestrijding en Veiligheid \(nctv.nl\)](#).

²⁴ [Extremisme | AIVD](#). Volgens de AIVD vallen (ultra)rechtse of (ultra)linkse partijen of organisaties die binnen de kaders van de democratische rechtsorde opereren, niet onder de definitie van extremisme. Wel kunnen activisten die neigen te radicaliseren tot extremisten, onder de aandacht van de AIVD komen.

Hoewel het volgens de WvSr bij terrorismefinanciering om meer gaat dan alleen het verwerven van financiële middelen en het bieden van financiële steun ten behoeve van een terroristische activiteit of organisatie (zie vorige subparagraaf), ligt de focus van deze NRA wel op financieringsmethoden en -bronnen. De reden daarvan is dat alleen deze typen dreigingen door vertegenwoordigers van expertorganisaties op het terrein van terrorismefinanciering zijn genoemd in de enquête, interviews en expertmeetings (zie hoofdstuk 2 voor meer informatie hierover).

1.3 Doel, structuur en onderzoeksvragen

Doel NRA

Het doel van deze derde NRA Terrorismefinanciering is vijfledig:

- 1 het identificeren van de grootste tf-dreigingen;
- 2 het vaststellen van de hoogte van de potentiële impact van de grootste tf-dreigingen;
- 3 het bepalen van de hoogte van de weerbaarheid van het beleidsinstrumentarium ter preventie en/of repressie van de grootste tf-dreigingen;
- 4 het bieden van inzicht in de aard en mechanismen van de grootste tf-dreigingen; en
- 5 het bepalen van het risiconiveau van de grootste tf-dreigingen door de potentiële impact van de dreigingen af te zetten tegen de weerbaarheid van het beleidsinstrumentarium.

In box 1.1 worden de voor deze NRA geldende verschillen tussen tf-dreigingen en tf-risico's gedefinieerd.

Box 1.1 Tf-dreigingen en tf-risico's

Bij 'tf-dreigingen' gaat het om methoden die (kunnen) worden ingezet om terroristische activiteiten te financieren en/of de financiële middelen hiertoe te verwerven. Het kan in deze NRA gaan om financieringsmethoden en financieringsbronnen. Bij de inzet van deze tf-methoden wordt veelal (maar niet altijd) gebruik dan wel misbruik gemaakt van bepaalde kanalen. Dit kunnen bijvoorbeeld banken en cryptodienstverleners zijn.

Het onderscheid tussen 'tf-dreigingen' en 'tf-risico's' in deze NRA ligt in het feit dat er bij 'dreigingen' nog geen sprake is geweest van een risicoanalyse. Bij de risicoanalyse wordt de potentiële impact van de tf-dreigingen afgezet tegen de weerbaarheid van het beleidsinstrumentarium ter preventie en/of bestrijding van deze dreigingen. Het tf-risico van een dreiging stijgt naarmate een dreiging hoger scoort op potentiële impact en lager scoort op weerbaarheid.

Vanwege het ontbreken van een (overkoepelende) dataset waarmee de potentiële impact van alle mogelijke tf-dreigingen onderling kan worden vergeleken en de weerbaarheid van het beschikbare beleidsinstrumentarium tegen de afzonderlijke dreigingen kan worden vastgesteld (zie ook paragraaf 1.4), worden de potentiële impact en weerbaarheid bepaald door vertegenwoordigers van publieke en private expertorganisaties op het gebied van terrorismefinanciering. In deze NRA zijn dat opsporingsinstanties, handhavers, Wwft-toezichthouders en de brancheorganisatie van de bankensector (de Nederlandse Vereniging van Banken, NVB) die alle een taak hebben bij de preventie en/of repressie van terrorismefinanciering. Op deze keuze

wordt dieper ingegaan bij de bespreking van het uitnodigingsbeleid voor de expertmeetings die in het kader van deze NRA plaatsvonden (zie paragraaf 2.3).

Structuur NRA

De structuur van de derde NRA wordt – net als in de eerdere NRA's – bepaald door het ISO 31000 raamwerk voor risicomanagement. Hieruit volgt dat de NRA is opgebouwd met de volgende elementen:

- Een contextanalyse waarin de specifieke en relatief vaststaande kenmerken van Nederland worden geschetst die van invloed (kunnen) zijn op de prevalentie van terrorismefinanciering, de potentiële impact daarvan en de keuze van personen voor de door hen in te zetten tf-methoden.
- In de fase van de risico-identificatie worden de grootste tf-dreigingen uit een longlist van dreigingen vastgesteld en geordend naar hun ingeschatte potentiële impact door vertegenwoordigers van publieke en private expertorganisaties op het terrein van de preventie en/of repressie van terrorismefinanciering.
- De fase van de risicoanalyse biedt inzicht in de mate waarin het beschikbare beleidsinstrumentarium ter preventie en/of repressie van terrorismefinanciering de grootste tf-dreigingen tegengaat ('weerbaarheid'). De weerbaarheid van het beleidsinstrumentarium wordt ingeschat door vertegenwoordigers van publieke en private expertorganisaties op het terrein van terrorismefinanciering. Door de expert-inschattingen van de potentiële impact en de weerbaarheid tegen elkaar af te zetten, ontstaat in deze fase inzicht in de grootste tf-risico's.

Onderzoeksvragen

De onderzoeksvragen voor de NRA zijn:

- 1 Welke contextfactoren van Nederland zijn (mogelijk) van invloed op de prevalentie van terrorismefinanciering, de potentiële impact daarvan en de keuze van personen voor de door hen in te zetten financieringsmethoden en/of te gebruiken financieringsbronnen?
- 2 Wat zijn de aard, mechanismen en potentiële impact van de grootste tf-dreigingen in Nederland?
- 3 Welke tf-dreigingen zijn in Nederland nog niet gesignaleerd maar zouden in de toekomst actueel kunnen worden?
- 4 Welk beleidsinstrumentarium is in Nederland beschikbaar ter preventie en bestrijding van de grootste tf-dreigingen?
- 5 Wat is de weerbaarheid van het in Nederland beschikbare beleidsinstrumentarium ter preventie en bestrijding van de grootste tf-dreigingen?
- 6 Wat zijn de grootste tf-risico's in Nederland, uitgaande van de ingeschatte potentiële impact van de tf-dreigingen en weerbaarheid van het beschikbare beleidsinstrumentarium?
- 7 Wat zijn concrete, recente voorbeelden van de grootste tf-risico's?
- 8 Welke verbeterpunten zijn te benoemen voor volgende NRA's?

1.4 Lessen van de tweede NRA Terrorismefinanciering en de FATF-evaluatie

In de tweede NRA Terrorismefinanciering is een aantal lessen geleerd ten aanzien van de uitvoering van het onderzoek, die mogelijk benut kunnen worden bij aankomende NRA's (Van der Veen & Heuts, 2020b). Verder heeft de FATF in 2022 een landenevaluatie van het Nederlandse anti-witwas- en terrorismefinancieringsbeleid uitgevoerd, waarin ook enkele aandachtspunten zijn benoemd ten aanzien van de

NRA's die voor Nederland worden uitgevoerd (FATF, 2022).²⁵ Hieronder wordt beschreven hoe met deze lessen en aandachtspunten is omgegaan in deze derde NRA Terrorismedinanciering.

Gebruik van meer kwantitatieve data

De FATF noemde in haar landenevaluatie van het Nederlandse anti-witwas- en terrorismedinancieringsbeleid dat er bij aankomende NRA's meer gebruikgemaakt zou moeten worden van kwantitatieve data over de tf-risico's. In deze derde NRA is als volgt gehoor gegeven aan dit aandachtspunt.

Nadat de definitieve shortlist van grootste tf-dreigingen was vastgesteld (zie hoofdstuk 2 voor meer informatie), heeft het WODC dataverzoeken ingediend bij de FIU-Nederland, de FIOD, het Financieel Expertise Centrum (FEC)²⁶, het OM en de afdeling Toezicht Rechtspersonen, Analyse, Controle & Kennisgeving (TRACK) van screeningsautoriteit Justis.²⁷ In het dataverzoek werd gevraagd om voor iedere tf-dreiging²⁸ in de shortlist zoveel mogelijk beschikbare relevante kwantitatieve data en casuïstiek aan te leveren (zie ook hoofdstuk 2). Dit heeft ertoe geleid dat er in algemene zin voor terrorismedinanciering (in hoofdstuk 3) en specifiek voor enkele tf-dreigingen (in hoofdstuk 4) aanvullende kwantitatieve data zijn opgenomen in deze derde NRA Terrorismedinanciering. Bij De Nederlandsche Bank (DNB) is voor een selectie van financiële instellingen die aan terrorismedinanciering kunnen worden gerelateerd, opgevraagd hoeveel er in Nederland actief zijn met een geldige DNB-vergunning of buitenlandse vergunning (deze informatie is opgenomen in hoofdstuk 3).

Ten aanzien van het FATF-aandachtspunt om meer gebruik te maken van kwantitatieve data kan wel een belangrijke kanttekening worden geplaatst. Hoewel de kwantitatieve data in deze derde NRA extra informatie bieden over de aard van enkele van de grootste tf-risico's, is het (nog) niet mogelijk om op basis van kwantitatieve data de impact die de dreigingen kunnen hebben, rekening houdend met de weerbaarheid tegen de dreigingen en de Nederlandse context, te bepalen. Daarvoor kunnen de volgende redenen worden gegeven:

- De risicoanalyse ten behoeve van de NRA vereist een overkoepelende dataset die voor alle dreigingen de benodigde gegevens van voldoende kwaliteit bevat. De NRA betreft een complexe analyse over zowel de gekende als nog niet gekende tf-dreigingen heen. Om een ordening te kunnen aanbrenge in het risiconiveau van de tf-dreigingen dienen de verschillende dreigingen en databronnen met elkaar in relatie te worden geanalyseerd. Gezien de grote verscheidenheid in de aard van de tf-dreigingen is een groot aantal typen kwantitatieve data nodig, namelijk indicatoren die niet alleen iets zeggen over de prevalentie(kans) maar ook over de potentiële impact van de tf-dreigingen en de weerbaarheid van het beleidsinstrumentarium. Niet alleen ontbreken die data momenteel grotendeels, ook is er nog onvoldoende kennis van en inzicht in welke mate de databronnen die

²⁵ [The Netherlands' measures to combat money laundering and terrorist financing \(fatf-gafi.org\)](https://www.fatf-gafi.org/publications/netherlands/documents/2022-01-10-the-netherlands-measures-to-combat-money-laundering-and-terrorist-financing).

²⁶ Het FEC is een samenwerkingsverband waarbinnen de Autoriteit Financiële Markten, De Nederlandsche Bank, het OM, de Nationale Politie, de FIU-Nederland, de FIOD en de Belastingdienst met elkaar samenwerken. Zie hoofdstuk 5 voor meer informatie over het FEC.

²⁷ Justis is de screeningsautoriteit van het Ministerie van JenV die een controle op de integriteit van rechtspersonen uitvoert en op die van bestuurders, andere betrokken personen en bedrijven.

²⁸ Aan de afdeling TRACK van Justis is alleen een dataverzoek ingediend ten aanzien van de tf-dreiging die betrekking had op stichtingen (zie hoofdstuk 4 voor meer informatie over deze dreiging).

wel beschikbaar zijn, voldoen aan kwaliteitseisen qua volledigheid, betrouwbaarheid, validiteit en onderlinge compatibiliteit.

- Aangezien de NRA zich ook richt op tf-dreigingen waarvan er nog weinig zicht is op de prevalentie en dat de NRA ook geschikt moet zijn voor nog niet (in Nederland) waargenomen en toekomstige dreigingen, zullen voor die tf-dreigingen sowieso kwantitatieve data ontbreken.
- Daarnaast is het verkrijgen van toestemmingen voor het gebruik van de data die afkomstig zijn van een groot aantal verschillende databronhouders, geen sinecure. Dit bleek al uit de exercitie met betrekking tot het uitvoeren van een kwantitatieve data-analyse in de tweede NRA Terrorismefinanciering (Van der Veen & Heuts, 2020b).
- De kwantitatieve analyse die in de tweede NRA is uitgevoerd, maakte de beperkingen van een kwantitatieve analyse op basis van beschikbare data inzichtelijk. De kwantitatieve analyse bood inzicht in ongebruikelijke situaties die lijken te wijzen op terrorismefinanciering, maar waarvoor een harde relatie met terrorismefinanciering niet vast te stellen is zonder nader opsporingsonderzoek.²⁹

Nadere specificatie tf-dreigingen

Een ander aandachtspunt dat genoemd werd in de FATF-evaluatie, is een gewenste nadere specificering van de tf-dreigingen in aankomende NRA's. Hieraan is op verschillende manieren gehoor gegeven in deze derde NRA Terrorismefinanciering, namelijk door een (beperkte) uitbreiding van de longlist van tf-dreigingen ten behoeve van de FANO-enquête (van 25 in de tweede NRA naar 28 in de derde NRA) en door nadrukkelijke aandacht voor de specificering van de tf-dreigingen in de expertmeetings en verdiepende interviews. In hoofdstuk 2 wordt nader ingegaan hierop.

Onderbouwing FANO-enquête

Een les die in de tweede NRA Terrorismefinanciering werd genoemd, was het verder versterken van de FANO-enquête door hierin nog explicieter te vragen naar de *eigen* praktijkkennis van (vertegenwoordigers van) organisaties met de prevalentie van de tf-dreigingen in de longlist. Hiertoe is in deze derde NRA gevraagd naar een beknopte toelichting op casuïstiek in het geval dat een respondent aangaf bekend te zijn met feiten/casus van een bepaalde tf-dreiging. Dit zorgde voor meer onderbouwing van de antwoorden van respondenten en maakte nog beter inzichtelijk welke respondenten wel/niet over relevante expertise op het terrein van terrorismefinanciering beschikten.

Nauwere betrokkenheid experts bij MCA-criteria

Een andere genoemde les in de tweede NRA Terrorismefinanciering was het nauwer betrekken van experts bij het formuleren en vaststellen van de criteria die onderdeel waren van de Multi Criteria Analyse (MCA) waarmee de potentiële impact van de grootste dreigingen werd ingeschat door experts (zie hoofdstuk 2 voor een nadere toelichting). Hiermee kon nog meer draagvlak voor de te hanteren criteria worden

²⁹ Deze conclusie uit de tweede NRA geldt nog steeds. In de tweede NRA is in samenwerking met Justis de nodige aandacht besteed aan een kwantitatieve data-analyse. Hoewel de kwantitatieve data-analyse inzicht heeft geboden in een aantal ongebruikelijke situaties op het terrein van rechtsvormen, was het op basis van de data niet mogelijk een directe relatie met terrorismefinanciering te leggen. Aangegeven werd dat, zelfs wanneer in een volgende NRA aanvullende databronnen bij het onderzoek betrokken worden, het niet de verwachting is dat deze inzicht zullen bieden in de prevalentie en/of potentiële impact van de tf-dreigingen. Een harde relatie met terrorismefinanciering is immers niet vast te stellen zonder nader opsporingsonderzoek.

bereikt en kon de lijst van MCA-criteria mogelijk verder worden aangescherpt. In deze derde NRA is de lijst van criteria eerst voorgelegd aan de wetenschappelijke begeleidingscommissie van het onderzoek, waarna het – na accordering door de begeleidingscommissie – is voorgelegd aan de deelnemers aan de tweede expertmeeting.

Kwantitatieve inschatting invloed contextfactoren

In de tweede NRA werd aangegeven dat bij een volgende NRA ervoor gekozen kan worden om de deelnemers aan de expertmeetings niet alleen een kwantitatieve inschatting te laten maken van de potentiële impact van de grootste tf-dreigingen en de weerbaarheid van het beschikbare beleidsinstrumentarium, maar ook van de mate waarin contextfactoren (ofwel 'Kwetsbaarheden', zie hoofdstuk 2) van invloed kunnen zijn op de prevalentie of potentiële impact van de dreigingen. In deze derde NRA is hier toch vanaf gezien, omdat het de complexiteit van de risicoanalyse verder zou vergroten en het veel kennis en expertise ten aanzien van een groot aantal contextfactoren zou vergen waarover naar verwachting niet alle tf-experts die aan de expertmeetings deelnemen, beschikken. De kwantitatieve inschattingen door de experts zouden daardoor naar verwachting minder goed onderbouwd kunnen worden.

1.5 Leeswijzer

Hoofdstuk 2 gaat nader in op de onderzoeksmethoden die zijn ingezet bij de voorliggende derde NRA op het terrein van terrorismefinanciering. Ook wordt een beschrijving gegeven van de centrale sleutelbegrippen in de NRA die in deze rapportage gehanteerd worden.

Hoofdstuk 3 zet de Nederlandse kwetsbaarheden voor terrorismefinanciering die in eerder onderzoek naar voren zijn gekomen, uiteen en onderbouwt dit aan de hand van enkele geografische, demografische, religieuze, sociaal-culturele, politieke, economische en criminologische kenmerken van Nederland die van invloed (kunnen) zijn op de prevalentie van terrorismefinanciering, de potentiële impact daarvan en de keuze van personen voor de door hen in te zetten tf-methoden.

In hoofdstuk 4 wordt een beschrijving gegeven van de grootste tf-dreigingen. Daarbij wordt aandacht besteed aan de aard en mechanismen van de dreigingen, recente casuïstiek over de dreigingen, de door experts ingeschatte potentiële impact van de dreigingen en – voor zover beschikbaar – kwantitatieve databronnen die in meer of mindere mate iets zeggen over de prevalentie en mogelijke impact van de dreigingen.

Hoofdstuk 5 beschrijft allereerst het beleidsinstrumentarium dat beschikbaar is voor de preventie en bestrijding van de grootste tf-dreigingen, gaat vervolgens in op de door experts ingeschatte weerbaarheid van dit beleidsinstrumentarium en besluit met een beknopte toelichting op toekomstige ontwikkelingen ten aanzien van het beleidsinstrumentarium.

In hoofdstuk 6 worden allereerst de onderzoeksvragen die centraal staan in deze NRA, beantwoord. Vervolgens wordt de uitvoering van de NRA geëvalueerd, waarbij ook enkele geleerde lessen worden getrokken die meegenomen kunnen worden bij de uitvoering van volgende NRA's.

2 Onderzoeksmethodiek

Dit hoofdstuk beschrijft de onderzoeks aanpak van deze derde NRA. Allereerst worden de sleutelbegrippen in de NRA geïntroduceerd en gedefinieerd. Vervolgens worden de opzet van het onderzoek en de toegepaste methoden beschreven aan de hand van de drie fasen in de NRA: de contextanalyse, de risico-identificatie en de risicoanalyse. Deze fasen maken deel uit van de ISO 31000 standaard voor risicomanagement³⁰ dat – net als in de eerdere NRA's – het structurerende kader voor de NRA vormt.

2.1 Sleutelbegrippen

Net als in de eerdere uitgevoerde NRA's op het terrein van Terrorismefinanciering wordt aangesloten bij de definities volgens de *FATF Guidance* (FATF, 2013) voor de sleutelconcepten Dreigingen, Gevolgen en Kwetsbaarheden:

- **Dreigingen** zijn in deze NRA alle activiteiten die betrekking hebben op het verzamelen/verwerven, voorhanden hebben of het verstrekken van financiële middelen en/of niet-financiële middelen (producten die in geld omgezet kunnen worden) door (groepen) personen om deze zelf aan te wenden voor het (beoogd) plegen van terroristische activiteiten of ten behoeve van andere (groepen) personen of organisaties die terroristische activiteiten (beogen te) plegen. Belangrijk om te melden is dat terroristische daden an sich in deze NRA geen Dreiging vormen. Het onderzoek gaat immers over risico's ten aanzien van de financiering van terrorisme.
- **Gevolgen** betreffen de effecten die kunnen optreden als gevolg van het zich voordoen van de Dreigingen. In de NRA worden deze gevolgen aangeduid als de *Potentiële Impact* van de tf-dreigingen. Tf-dreigingen kunnen verschillen in de mate waarin ze hun uitwerking hebben op de prevalentie van terroristische activiteiten in Nederland en/of in het buitenland, de aantasting van de financiële sector, de subjectieve veiligheid, de ondermijning van gezag en het imago van Nederland in het buitenland.³¹
- **Kwetsbaarheden** zijn relatief vaststaande contextfactoren die van invloed kunnen zijn op de prevalentie van Dreigingen waarop niet of niet direct door beleidsmaatregelen kan worden ingegrepen. Ook kunnen zij van invloed zijn op de potentiële impact van Dreigingen en/of de keuze van terroristen voor de door hen in te zetten financieringsmethoden of te gebruiken financieringsbronnen. In deze NRA worden geografische, demografische, religieuze, sociaal-culturele, politieke, economische en criminologische contextfactoren beschreven die invloed kunnen hebben op de kans dat Dreigingen zich voordoen in Nederland en/of op de gevolgen daarvan.

Net als in de eerder uitgevoerde NRA's wordt aan de bovengenoemde sleutelconcepten het element Weerbaarheid toegevoegd:

- Bij **Weerbaarheid** gaat het om de werking van het beleidsinstrumentarium dat in Nederland beschikbaar is voor de preventie en/of repressie van

³⁰ Risicomanagement volgens de standaarden van de International Organization for Standardization (ISO).

³¹ De hier opgesomde elementen vormen de criteria die zijn toegepast in de Multi Criteria Analyse, waarmee in deze NRA de omvang van de Potentiële Impact van de grootste tf-dreigingen is bepaald. Meer hierover in paragraaf 2.3.

terrorismedinanciering. Bij Weerbaarheid gaat het zowel om de inhoud/strekking van de beleidsinstrumenten als de uitvoering van die instrumenten. Het begrip Weerbaarheid omvat de elementen absorptie, adaptatie en transformatie (Béné et al., 2012). Er is sprake van *absorptie* wanneer het beschikbare beleidsinstrumentarium in staat is de impact van dreiging volledig op te vangen. Bij *adaptatie* kan het beschikbare beleidsinstrumentarium de impact van de dreiging niet (volledig) opvangen maar zijn er mogelijkheden om het beschikbare beleidsinstrumentarium er (eventueel stapsgewijs) op aan te passen. Tenslotte kan er sprake zijn van *transformatie* wanneer het beschikbare beleidsinstrumentarium de dreiging niet kan tegengaan en er geen mogelijkheden bestaan voor aanpassing van het beschikbare beleidsinstrumentarium en dat nieuw beleid ontworpen dient te worden om de impact van de dreiging tegen te gaan. Het vermogen tot transformatie betreft de mogelijkheden die er bestaan voor het ontwerpen van nieuw beleid.

De Weerbaarheid kan zowel bepalend zijn voor de kans dat Dreigingen zich voordoen als voor de hoogte van de Potentiële Impact van de Dreigingen. Hierbij geldt: hoe hoger de Weerbaarheid, hoe meer de impact die de dreigingen kunnen hebben, kan worden tegengegaan. In tegenstelling tot de Kwetsbaarheden die relatief ongevoelig zijn voor beleidsmaatregelen gaat het bij Weerbaarheid dus om de factoren waarop in meer of mindere mate door beleidsingrepen invloed kan worden uitgeoefend. In deze NRA betreft het in feite de strekking en de uitvoering van de beleidsmaatregelen die kunnen worden doorgevoerd om het optreden van terrorismedinanciering te voorkomen of tegen te gaan.

In het laatste sleutelconcept **Risico** worden de vier bovengenoemde elementen gecombineerd. De elementen die in de NRA per Dreiging het Risico bepalen, zijn een uitwerking van de gangbare risicodefinitie waarin Risico wordt bepaald door Impact en Kans (Lees, 1980).

- **Kans** heeft in deze NRA betrekking op de kans dat Dreigingen actueel worden. Deze kans wordt bepaald aan de hand van de elementen *Kwetsbaarheden* en *Weerbaarheid*. De kans dat een tf-dreiging zich al dan niet voordoet, wordt bepaald door zowel de contextuele factoren die van invloed zijn op de Kwetsbaarheden van Nederland als de Weerbaarheid van het bestaande Nederlandse beleidsinstrumentarium ter preventie en/of bestrijding van terrorismedinanciering.
- **Impact** staat gelijk aan het hierboven beschreven begrip *Gevolgen of Potentiële Impact*. In deze NRA wordt de Potentiële Impact bepaald op basis van een Multi Criteria Analyse (MCA)³², waarbij de potentiële impact van de belangrijkste dreigingen op een aantal criteria, zoals aantasting van de financiële sector en vermindering van de subjectieve veiligheid, wordt ingeschat door experts op het terrein van tf (zie paragraaf 2.3 voor meer informatie over de MCA en de daarbij toegepaste criteria).
- Per Dreiging wordt uiteindelijk het **Risico** bepaald door het bijeenbrengen van de bovengenoemde sleutelementen.³³

³² Een andere term voor een MCA is *Multi Criteria Decision Analysis* (MCDA).

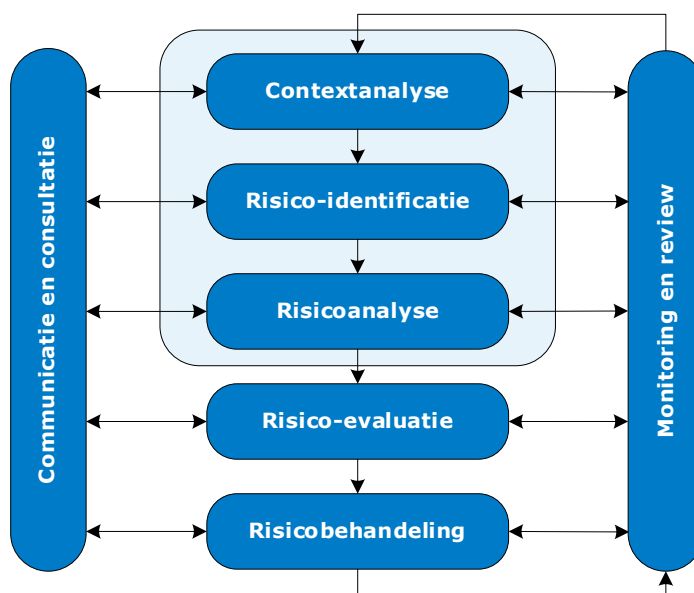
³³ Voor iedere dreiging d geldt de volgende risicofunctie:

$$\text{Risico}_d = f(\text{Kwetsbaarheid}_d, \text{Potentiële Impact}_d, \text{Weerbaarheid}_d).$$

2.2 Uitvoering NRA binnen de ISO 31000 standaard voor risicomanagement

De ISO 31000 standaard voor risicomanagement vormt het raamwerk voor de NRA (zie figuur 2.1; ISO 31000:2009, 2009a; ISO/IEC 31010:2009, 2009b). Binnen dit internationaal gestandaardiseerde kader kunnen allerlei methoden worden toegepast. Op hoofdlijnen volgt ook de *FATF Guidance* deze structuur FATF (2013). De NRA doorloopt niet de complete ISO 31000 cyclus van risicomanagement, maar beperkt zich tot contextanalyse, risico-identificatie en risicoanalyse. De fases van risico-evaluatie en risicobehandeling vallen buiten de hier gepresenteerde NRA omdat in die fases beslissingen dienen te worden genomen over de mate waarin risico's acceptabel of tolerabel zijn en of er nieuw of aangepast beleid noodzakelijk is. Het nemen van dergelijke normatieve beslissingen verhoudt zich slecht met de wetenschappelijke benadering van de hier voorliggende NRA.

Figuur 2.1 Risicomanagement volgens de ISO 31000 standaard met in lichtblauw de focus van de NRA



2.3 Ingezette onderzoeksmethoden

Bij de beantwoording van de onderzoeksvragen voor deze derde NRA zijn verschillende onderzoeksactiviteiten uitgevoerd. Hieronder wordt per fase aangegeven welke onderzoeksactiviteiten zijn verricht.

Voorfase onderzoek: kick-off bijeenkomst

Voorafgaand aan de start van de NRA werd een *online kick-off* bijeenkomst belegd voor de in het onderzoek te benaderen publieke en private partijen. Het doel van deze bijeenkomst was deze partijen te informeren over de start van de derde NRA Terrorismefinanciering, de onderzoeksactiviteiten die zouden worden verricht en de momenten waarop de aangeschreven partijen in het onderzoek zouden worden betrokken. De verwachting was dat dit positief zou uitwerken op de medewerking van deze partijen. Dit betrof zowel publieke als private partijen die beschikken over

specifieke kennis van en ervaring met betrekking tot de preventie en/of repressie van terrorismefinanciering. Publieke partijen zijn de toezichthouders in het kader van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft), opsporingsinstanties, handhavers en andere aan de overheid gelieerde organisaties die een rol spelen bij de preventie en/of bestrijding van terrorismefinanciering. Private partijen zijn de Wwft-poortwachters, die op grond van de Wwft OT's moeten melden bij de FIU-Nederland en verplicht zijn onderzoek te doen naar hun cliënten, hun branche-/koepelorganisaties en non-gouvernementele organisaties (ngo's), vooral goede doelen organisaties. Deze partijen zijn gedurende het onderzoek benaderd om casusmateriaal en andere informatie aan te leveren over hun ervaringen met de preventie en/of repressie van terrorismefinanciering. Daarnaast is in de kick-off bijeenkomst aangekondigd dat een selectie van deze partijen gevraagd zou worden om relevante kwantitatieve dataoverzichten aan te leveren en mee te werken aan interviews en expertmeetings. Aan de kick-off bijeenkomst namen 25 personen van 17 publieke en private organisaties deel. Ook één van de aanvragers van het onderzoek, het ministerie van Financiën, was vertegenwoordigd in de kick-off bijeenkomst.

Fase: contextanalyse

In de contextanalyse werd ingegaan op de verschillende kenmerken van Nederland die van invloed kunnen zijn op de prevalentie van terrorismefinanciering, de potentiële impact daarvan en de keuze van personen voor de door hen in te zetten tf-methoden, Het betreft kenmerken die via beleidsmaatregelen niet of slechts beperkt beïnvloedbaar zijn. Ingezoomd werd onder meer op geografische, demografische, religieuze, sociaal-culturele, politieke, economische en criminologische kenmerken van (Europees) Nederland. Bij de beschrijving vormden kenmerken uit de tweede NRA het uitgangspunt. Deze zijn daar waar nodig geactualiseerd aan de hand van informatie uit relevante openbare bronnen en wetenschappelijke literatuur. Nieuw voor de hier voorliggende derde NRA is dat er aanvullende kwantitatieve bronnen zijn gebruikt ter onderbouwing van de gerapporteerde kwalitatieve kenmerken.

Nieuw voor de hier voorliggende derde NRA is dat er naast de Justis/TRACK data aanvullende kwantitatieve bronnen zijn gebruikt ter onderbouwing van de gerapporteerde kwalitatieve kenmerken. Het betreft de volgende data:

- Data van de FIU-Nederland over onder meer OT's, verdachte transacties (VT's) en VT-dossiers. Deze data zijn afkomstig uit de Jaaroverzichten 2020-2022 van deze organisatie.
- Data van het OM over het aantal gestarte tf-onderzoeken in de periode 2020-2022 en het aantal afgeronde, onherroepelijke tf-zaken sinds de vorige NRA Terrorismefinanciering. Deze data zijn verkregen naar aanleiding van een dataverzoek van het WODC.
- Data van DNB over de actuele aantallen van de diverse typen van financiële instellingen die in Nederland opereren met een geldige Nederlandse of buitenlandse vergunning. Deze data zijn verkregen naar aanleiding van een dataverzoek van het WODC.
- Data van de FIOD over het aantal afgeronde tf-onderzoeken van deze opsporingsdienst in de periode 2020-2022. Deze data zijn verkregen naar aanleiding van een dataverzoek van het WODC.

Fase: risico-identificatie

1 Update longlist van tf-dreigingen

Ten behoeve van een update van de longlist van tf-dreigingen die in de tweede NRA Terrorismefinanciering van Van der Veen & Heuts (2020b) is opgesteld, zijn recente (sinds 2020 verschenen) rapporten bestudeerd, waaronder de Europese *Supra National Risk Assessment* (SNRA) door de Europese Commissie (2022) en het *Mutual Evaluation Report* van de FATF met betrekking tot de Nederlandse maatregelen tegen witwassen en terrorismefinanciering (FATF, 2022).³⁴ Dit leidde tot enkele aanvullingen op en nadere specificaties van de dreigingen uit de vorige NRA. Hierdoor steeg het aantal tf-dreigingen op de longlist van 23 tot 28.

2 FANO-enquête

De geactualiseerde longlist is door middel van de zogeheten FANO-enquête (zie toelichting hieronder) *online*³⁵ voorgelegd aan publieke en private partijen met een taak bij de preventie en bestrijding van terrorismefinanciering. De lijst met mogelijk te benaderen organisaties is voorgelegd aan de wetenschappelijke begeleidingscommissie van het onderzoek (zie bijlage 1 voor de samenstelling van deze commissie), wat geleid heeft tot een aanvulling van de lijst met enkele organisaties. De volgende typen organisaties zijn benaderd:

- de toezichthouders in het kader van de Wwft;
- overige overheidsdiensten of aan de overheid gelieerde organisaties die een rol spelen bij de preventie en/of bestrijding van terrorismefinanciering;
- Wwft-poortwachters en branche-/koepelorganisaties van poortwachters.

In de FANO-enquête is aan de respondenten gevraagd om bij de toegestuurde longlist van dreigingen aan te geven of zij vanuit hun eigen werkzaamheden (dus niet via berichten uit de media, via andere organisaties of via andere bronnen) ervaring hebben met feiten/casus van de dreigingen en in hoeverre zij de prevalentie van de dreigingen al dan niet aannemelijk achten op basis van de bij hun organisatie beschikbare informatie. De respondenten werden gevraagd bij iedere dreiging op de longlist van dreigingen één van de volgende letters te plaatsen:

- een **F** indien er volgens een respondent sprake is van deze dreiging en er via de eigen werkzaamheden één of meer Feiten/casus bekend zijn bij zijn of haar organisatie;
- een **A** indien het volgens een respondent Aannemelijk is dat deze dreiging speelt maar er via de eigen werkzaamheden geen feiten/casus bekend zijn bij zijn of haar organisatie;
- een **N** indien het volgens een respondent Niet aannemelijk is dat deze dreiging speelt op basis van de informatie waarover zijn of haar organisatie via de eigen werkzaamheden beschikt;
- een **O** indien het voor een respondent Onbekend is of een dreiging speelt, omdat zijn of haar organisatie hier via de eigen werkzaamheden geen zicht op heeft, of omdat een respondent de dreiging niet kent.

In de FANO-enquête kregen de respondenten de mogelijkheid een korte casusbeschrijving aan te leveren als zij via de eigen werkzaamheden bekend waren met feiten of casus, om de longlist aan te vullen met tf-dreigingen die volgens hen

³⁴ [The Netherlands' measures to combat money laundering and terrorist financing \(fatf-gafi.org\)](https://www.fatf-gafi.org/).

³⁵ De FANO-enquête is uitgezet via de enquêtetool van Onderzoekdoen.nl en is te vinden in Bijlage 4.

onterecht ontbraken in de longlist en om tf-dreigingen te benoemen die in Nederland nog niet gesignaleerd zijn maar in de toekomst actueel zouden kunnen worden.

In totaal werden 39 publieke en private organisaties benaderd, waarvan er 25 de FANO-enquête volledig invulden (zie bijlage 4 voor het responsoverzicht).³⁶ Hiernaast vulden 49 niet direct aangeschreven organisaties de FANO-enquête in.³⁷ Deze organisaties verkregen via hun branche-/koepelorganisatie – buiten het WODC om – de link naar de FANO-enquête.

De toepassing van de FANO-enquête is een eerste stap richting een meer *evidence based* risico-identificatie. De enquête bood inzicht in:

- 1 de mate van (on)bekendheid van publieke en private organisaties met feiten/casus van de dreigingen in de longlist, hetgeen een rol speelde bij het uitnodigingsbeleid voor de expertmeetings (zie box 2.1);
- 2 de deelnemers die in de eerste expertmeeting gevraagd konden worden om een toelichting op feiten/casus te geven;
- 3 de organisaties die op een later moment benaderd dienden te worden voor een verdiepend interview.

Box 2.1 Uitnodigingsbeleid expertmeetings

De resultaten van de NRA worden in belangrijke mate bepaald door de opbrengsten van de expertmeetings. Aan de samenstelling van de expertmeetings is daarom de nodige zorg besteed. Voor een evenwichtige samenstelling is het van belang dat alle relevante invalshoeken op de dreigingen die centraal staan in de expertmeetings zijn vertegenwoordigd.

Aan de expertmeetings namen expertorganisaties deel die, blijkend uit de resultaten van de FANO-enquête, vanuit de eigen werkzaamheden ervaring hebben in het maken van risico-inschattingen over meerdere typen van tf-dreigingen en die dus vanuit deze praktijkervaring beschikken over een breed overzicht op de dreigingen waarop de NRA zich richt. Om belangendiscussies en strategisch opereren zoveel mogelijk te voorkomen werden geen organisaties uitgenodigd die directe belangen zouden kunnen hebben bij de uitkomst van de risicoanalyse. Dit betreft vertegenwoordigers van branche- of belangenorganisaties die zich slechts richten op één enkel type dreiging, betrekking hebbende op de eigen sector. Een uitzondering hierop vormt de bankensector die wél vertegenwoordigd was in de expertmeetings. Banken vormen een belangrijk element in veel tf-constructies. Vanwege de invulling van hun poortwachtersrol werkt de bankensector steeds meer risicogericht. Hierdoor beschikt de bankensector over de nodige expertise in en ervaring met het detecteren van ongebruikelijke financiële transactiepatronen die een grote diversiteit aan dreigingstypen beslaan.

Met het oog op de evenwichtigheid van de discussie konden alle partijen één vertegenwoordiger voor de expertmeetings afvaardigen.

³⁶ Omwille van de anonimiteit van organisaties wordt niet nader gespecificeerd welke organisaties de FANO-enquête niet hebben ingevuld.

³⁷ Het betreft ngo's (n=47) en aanbieders van cryptodiensten (n=2). De opbrengst van de niet aangeschreven maar wel responderende organisaties vormde referentiemateriaal en is daarnaast gebruikt bij het verzamelen van casusbeschrijvingen.

3 Eerste expertmeeting

De resultaten van de FANO-enquête vormden het startpunt voor de eerste expertmeeting waaraan vertegenwoordigers van acht expertorganisaties deelnamen (zie bijlage 3 voor de deelnemende organisaties). In de uitnodigingsmail voor de eerste expertmeeting is aan de expertorganisaties gevraagd de meest aangewezen medewerker af te vaardigen met expertise op het voorkomen en/of tegengaan van terrorismefinanciering waaronder kennis van en ervaring met casuïstiek op dit terrein.

In de expertmeeting is allereerst in gezamenlijkheid de gehele longlist bestaande uit 28 tf-dreigingen besproken. Bij de bespreking van iedere dreiging is de deelnemers gevraagd casus uit de eigen werkzaamheden in te brengen. Door de plenaire bespreking van de dreigingen deden alle deelnemers van de expertmeeting (op z'n minst basale) kennis op van de aard, mechanismen en prevalentie van de dreigingen op de longlist (indien zij hierover nog niet beschikten op basis van de eigen werkzaamheden). Hiermee is beoogd de referentiekaders van de deelnemers zoveel mogelijk gelijk te trekken. De gezamenlijke bespreking van de tf-dreigingen zorgde ervoor dat de longlist op onderdelen is aangepast, omdat experts van mening waren dat twee tf-dreigingen samengevoegd moesten worden. Daarmee bestond de voorlopige longlist uit 27 tf-dreigingen. Vervolgens werden in gezamenlijkheid de tf-dreigingen besproken die experts in de FANO-enquête hadden toegevoegd. Voorafgaande aan de expertmeeting had het WODC deze dreigingen geanalyseerd en geclusterd. Van de toegevoegde dreigingen werd per dreiging besloten om deze al dan niet aan de longlist toe te voegen. De bespreking leidde uiteindelijk tot de herformulering van zes dreigingen, drie samenvoegingen van twee dreigingen, één geschrapte dreiging en vier toegevoegde dreigingen. Zo bestond de definitieve longlist uiteindelijk weer uit 27 tf-dreigingen (zie bijlage 5).

Vervolgens selecteerden de experts uit de longlist de tien dreigingen die naar hun oordeel binnen de Nederlandse context het hoogst scoorden op potentiële impact. Na een plenaire discussie werden de deelnemende experts in gelegenheid gesteld hun eerdere oordelen aan te passen. Daarbij vond ook nog een herformulering van een tf-dreiging plaats plus een combinatie van twee dreigingen. Uiteindelijk leidde dit tot een voorlopige shortlist van 15 tf-dreigingen met de grootste potentiële impact (zie bijlage 5).

In de expertmeeting is evenals bij de daaropvolgende expertmeetings gebruikgemaakt van de Delphi-methode (box 2.2) die wordt toegepast binnen een Group Decision Support System (GDSS) omgeving (box 2.3). Bij de eerdere NRA's bleek dit een vruchtbare benadering te zijn.³⁸

Box 2.2 Delphi-methode

De Delphi-methode is ontwikkeld in de jaren '50 van de vorige eeuw^a, aan het begin van de Koude Oorlog, toen in een project voor de Amerikaanse luchtmacht bleek dat traditionele wetenschappelijke methoden onvoldoende basis vormden voor de ontwikkeling van nieuwe technieken voor internationale oorlogsvoering. In de Delphi-methode worden oordelen van (een groep van) experts gecombineerd bij besluitvorming over onderwerpen waarover geen betrouwbare wetenschappelijk toetsbare inzichten bestaan. Leemtes in de kennis worden gevuld door het samenbrengen, bediscussiëren en onderbouwen van expertoordelen, -ervaringen

³⁸ Zie voor meer informatie de zelfevaluatie van de eerder uitgevoerde NRA's.

en -intuïties. Door deze terugkoppeling worden de experts in de gelegenheid gesteld hun initiële oordeel te herzien. Het proces vindt plaats in een aantal rondes. Voordelen van de Delphi-methode zijn:

- vergroting van de transparantie en systematisering van complexe besluitvormingsprocessen;
- betere benutting van bestaande kennis en informatie, omdat alle experts hun kennis, ervaringen en informatie delen;
- vaak leidt dit tot verhoging van de consensus voor de 'beste' oplossing.

Aan het toepassen van de Delphi-methode is het gevaar van groepsdenken verbonden. Groepsdenken kan ontstaan wanneer de focus binnen een besluitvormingsproces zodanig is gericht op het vinden van consensus dat dit ten koste gaat van de kwaliteit van de besluitvorming.^b Experts kunnen er onterecht van uitgaan dat alle relevante facetten bij de besluitvorming zijn betrokken.

a [Delphi Method | RAND](#).

b Kroon (1992).

Groepsdenken is tegengegaan door een professionele onafhankelijke voorzitter voor de expertmeetings aan te stellen.³⁹ De voorzitter stimuleerde – samen met de onderzoekers – de experts om de oordelen die ze in de GDSS-omgeving (zie box 2.3 voor meer informatie) inbrachten, te onderbouwen, uit te leggen, daarop door te vragen en er casusvoorbeelden voor aan te dragen.

Het GDSS wordt gekenmerkt door een afwisseling van ict – met individuele digitale stemmingen van de experts – en groepsdiscussies. Het GDSS hielp bij het vormgeven en structureren van de expertmeetings. Geprobeerd is binnen de beperkingen van de beschikbare tijd de experts zoveel mogelijk gelegenheid te bieden hun oordelen toe te lichten, elkaar erover te bevragen en te bediscussiëren.⁴⁰

Box 2.3 Group Decision Support System

Evenals in de eerdere NRA's is in de expertmeetings gebruikgemaakt van een GDSS. Een GDSS is een elektronisch vergadersysteem dat de deelnemers in staat stelt in korte tijd een grote hoeveelheid aan ideeën en meningen te genereren door een afwisseling van ict-techniek en plenaire discussies. In de expertmeetings van deze NRA kregen de deelnemers via een laptop-netwerk de mogelijkheid om digitaal te stemmen ten behoeve van de risico-identificatie (eerste expertmeeting), de potentiële impact van de grootste tf-dreigingen in te schatten (tweede expertmeeting) en de weerbaarheid van het beleidsinstrumentarium te beoordelen (derde expertmeeting). Het GDSS zorgde ervoor dat de oordelen van alle deelnemende experts werden meegewogen in de uitkomst van de expertmeeting en niet alleen de oordelen van de meest actief op de voorgrond tredende deelnemers of de deelnemers met een hiërarchische positie. In het GDSS konden de deelnemende experts hun oordelen en inschattingen via de laptop invoeren en werden deze reacties centraal opgeslagen, waarna de geaggregeerde uitkomsten real-time werden gepresenteerd.

³⁹ Drs. P.J.M. Wilms trad, net als bij de vorige NRA's, op als voorzitter van de expertmeetings.

⁴⁰ De GDSS-functionaliteit werd geleverd door het bedrijf Spilter. Het betreft dezelfde functionaliteit die in de eerdere NRA's is gebruikt en toen werd aangeduid als *Group Decision Room* (GDR). Spilter leverde eveneens de technische ondersteuning in de expertmeetings.

4 Verdiepende interviews expertorganisaties

Om meer inzicht in te krijgen in de 15 tf-dreigingen met de grootste potentiële impact die in de eerste expertmeeting zijn geïdentificeerd, zijn verdiepende interviews afgenomen met 52 vertegenwoordigers van 12 publieke en 15 private expertorganisaties (zie bijlage 2 voor een overzicht van de geïnterviewde expertorganisaties).

In de verdiepende interviews is ingegaan op de aard en mechanismen van de grootste tf-dreigingen. Ook is, in het licht van de bepaling van de potentiële impact en de weerbaarheid in de tweede en derde expertmeeting, de wenselijkheid van een nadere specificatie van de dreigingen nagegaan. De interviews hebben ook het zicht op de onderlinge relatie tussen tf-dreigingen vergroot.

5 Tweede expertmeeting (1^e onderdeel)

De verdiepende interviews hebben geleid tot diverse aanpassingsvoorstellen in de voorlopige shortlist van grootste tf-dreigingen die aan het begin van de tweede expertmeeting met de deelnemers is besproken. Uiteindelijk is besloten tot vier samenvoegingen van twee dreigingen, een opsplitsing van een dreiging naar twee dreigingen en een herformulering van drie dreigingen. Dit resulteerde in een aangepaste shortlist bestaande uit 12 tf-dreigingen. Zie bijlage 7 voor deze lijst.

De tweede expertmeeting had een tweeledig doel, namelijk 1. het vaststellen van de definitieve shortlist van de grootste tf-dreigingen en 2. het bepalen van de potentiële impact van deze dreigingen. Aan de tweede expertmeeting namen vertegenwoordigers van de acht expertorganisaties deel (zie bijlage 3), die ook hadden deelgenomen aan de eerste expertmeeting. De shortlist is in het begin van de tweede expertmeeting besproken. Dit leidde tot enkele nieuwe aanscherpingen van tf-dreigingen, viermaal tot een combinatie van twee dreigingen en eenmaal tot een opsplitsing van een dreiging. Na accordering door de deelnemende experts was de definitieve shortlist met de 12 grootste tf-dreigingen vastgesteld en werd de fase van de risico-identificatie afgesloten (zie hoofdstuk 4 en bijlage 5 voor de definitieve shortlist).

Fase: risicoanalyse

6 Tweede expertmeeting (2^e onderdeel)

Nadat de definitieve shortlist van de 12 grootste tf-dreigingen was geïdentificeerd, werd het resterende deel van de tweede expertmeeting besteed aan de bepaling van de potentiële impact van deze dreigingen. Dit gebeurde aan de hand van een MCA (box 2.4).

Box 2.4 Multi Criteria Analyse

Het doel van de NRA voor terrorismefinanciering is beleidsmakers in staat te stellen risicogericht beleid te formuleren, ofwel beleid dat rekening houdt met het risiconiveau van de belangrijkste tf-dreigingen. Hiertoe dienen de tf-dreigingen te worden geprioriteerd. Vanwege het ontbreken van een overkoepelende kwantitatieve dataset die het mogelijk maakt een vergelijkende analyse uit te voeren voor alle huidige en toekomstige tf-dreigingen via dezelfde methode en zo het risiconiveau tegen elkaar af te wegen, wordt in de NRA het risiconiveau van de dreigingen bepaald via expertoordelen. Daarbij wordt de risicoanalyse gezien als een besluitvormingsprobleem. Voor het oplossen van dit besluitvormingsprobleem wordt evenals bij de eerdere NRA's gebruik gemaakt van een MCA. Een MCA is een methode om een rationele ordening aan te brengen in onderling lastig vergelijkbare alternatieven. In het geval van de NRA betreffen deze 'alternatieven' de tf-dreigingen.

In de MCA wordt voor het afwegen van deze alternatieven een set van criteria opgesteld waartegen experts of andere betrokkenen de alternatieven beoordelen en ordenen. De criteria kunnen worden gezien als de effecten waarop alternatieven verschillend kunnen scoren. Hierbij kan worden gedacht aan te maken kosten, het veiligheidsniveau, milieukwaliteit, sociale gevolgen, etc. Voor ieder alternatief en beoordelingscriterium worden door experts of andere betrokkenen wegingsscores toegekend die vervolgens worden gestandaardiseerd. Vervolgens worden per alternatief de scores gesommeerd. Het alternatief met de hoogste score geldt als alternatief dat het meest tegemoetkomt aan de eisen die de specifieke besluitvormingssituatie stelt.

Bijvoorbeeld: als het gaat om de aankoop van een auto, dan kunnen criteria als aankoopkosten, energiezuinigheid en kleur een rol spelen bij de aankoopbeslissing. De besluitvormingsalternatieven bestaan uit de twee auto's die na voorselectie zijn overgebleven: een blauwe Volkswagen en een rode Ford. De criteria kunnen verschillen in de mate waarin ze belangrijk geacht worden voor de aankoopbeslissing. In een MCA krijgen de criteria daartoe een gewicht, (bijvoorbeeld) op een schaal van 1 tot en met 10. In dit voorbeeld krijgen aankoopkosten het gewicht 8, energiezuinigheid krijgt het gewicht 9 en kleur krijgt het gewicht 6. Vervolgens is voor de auto's bepaald hoe ze scoren op de criteria (op een schaal van 0 tot en met 100). Er ontstaat dan een tabel met de volgende vorm:

Criteria	Criteriumgewicht	Volkswagen	Ford
Aankoopkosten	8	60	75
Energiezuinigheid	9	90	60
Kleur	6	80	60

De aankoopkosten van de Volkswagen zijn hoger dan de Ford, maar de Volkswagen is een stuk energiezuiniger en de kopers vinden de kleur van de Volkswagen mooier. De toepassing van een MCA met de bovenstaande data laat zien dat een aankoopbeslissing voor de Volkswagen de meest rationele keuze is.

Criteria	Volkswagen	Ford
Aankoopkosten	48	60
Energiezuinigheid	81	54
Kleur	48	36
Totaalscore	177	150

Met de inzet van een MCA is beoogd te bereiken dat het effect van enkele mogelijke knelpunten van een expert-georiënteerde benadering, namelijk dat de oordelen (deels) subjectief zijn en/of worden bepaald door (organisatie)belangen, wordt verminderd. Door het gebruikmaken van criteria voor het bepalen van de potentiële impact van de tf-dreigingen ontstaat er voor de experts minder ruimte hun eventuele belangenposities te laten meewegen bij het maken van een inschatting.

In de NRA is de MCA toegepast binnen de eerder beschreven GDSS-omgeving (zie box 2.3). In de zelfevaluatie van de vorige NRA voor terrorismefinanciering werd aan het gebruik van een MCA toegevoegde waarde toegekend. De MCA droeg bij aan het structureren van de tweede expertmeeting en vergrootte de transparantie van de resultaten en de wijze waarop de resultaten werden behaald. De gehanteerde criteria worden weergegeven in tabel 2.1.

Tabel 2.1 Criteria MCA

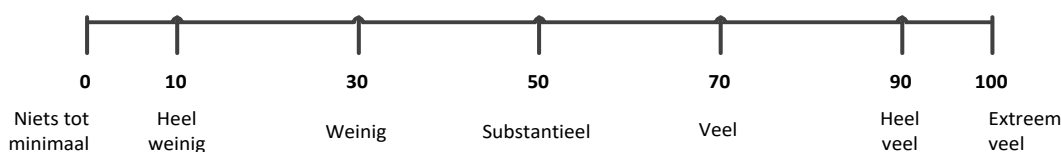
Criteria
Prevalentie terroristische activiteiten in Nederland
Prevalentie terroristische activiteiten in het buitenland
Aantasting financiële sector
Vermindering subjectieve veiligheid
Ondermijning gezag
Aantasting imago Nederland in het buitenland

a De criteria die in de MCA zijn toegepast, zijn gebaseerd op het overzicht over de gevolgen en effecten van terrorismefinanciering in de *FATF Guidance* (2013, pag. 26).

Aan de experts werd gevraagd aan de zes criteria een gewicht op een schaal van 0 tot en met 10 toe te kennen. Daarmee werd duidelijk welke criteria de experts belangrijker en minder belangrijk achtten bij de bepaling van de potentiële impact van de grootste tf-dreigingen. Van de gewichten die de experts toekenden, zijn de gemiddelde waarden bepaald. Deze gemiddelden vormden de toegepaste criteriumgewichten die gebruikt zijn bij de berekening van de potentiële impact.

Vervolgens maakten de experts per dreiging en per criterium een inschatting van de mogelijke gevolgen van de tf-dreigingen op de bovenstaande zes criteria (op een schaal van 0 tot en met 100). Hierbij werd de experts gevraagd om rekening te houden met de Nederlandse context waarbinnen de tf-dreigingen zich kunnen voordoen. Ook is de experts gevraagd om bij hun inschatting van de potentiële impact rekening te houden met de door hen ingeschatte kans dat de dreigingen zich

voordoen. Voor bijvoorbeeld de tf-dreiging 'financiering via girale of contante transacties bij vergunde banken' (zie hoofdstuk 4 voor meer informatie over deze dreiging) en het criterium 'vermindering subjectieve veiligheid' kregen de deelnemers aan de expertmeeting de volgende vraag voorgelegd: 'In welke mate leidt terrorismefinanciering via girale of contante transacties bij vergunde banken tot een vermindering van de subjectieve veiligheid?'. Bij het maken van hun inschattingen konden de experts gebruikmaken van de onderstaande schaal met ijkpunten.



De resultaten⁴¹ van de eerste inschattingsronde zijn vervolgens in gezamenlijkheid besproken. Hierna volgde de tweede en definitieve inschattingsronde waarin de experts de mogelijkheid kregen om – als gevolg van de plenaire bespreking van de resultaten van de eerste ronde – de toegekende scores aan te passen.

7 Derde expertmeeting

De derde expertmeeting richtte zich op 1. het bepalen van de weerbaarheid van het totale pakket aan beschikbare en relevante beleidsinstrumenten ter preventie en/of bestrijding van de grootste tf-dreigingen en 2. het identificeren van mogelijkheden ter verdere vergroting van de weerbaarheid van het beschikbare beleidsinstrumentarium.

Het beschikbare beleidsinstrumentarium omvat alle relevante instrumenten die in juni 2023, de maand waarin de derde expertmeeting plaatsvond, ingezet konden worden bij de preventie en/of repressie van de grootste tf-dreigingen. Het betreft internationale en nationale wet- en regelgeving, wet- en regelgeving op gemeentelijk niveau, sectorale en branchegerichte regelgeving, en regelgeving op organisatieniveau. Ook samenwerkingsverbanden tussen publieke en/of private organisaties, richtlijnen, handreikingen en beleidsplannen van organisaties die een rol spelen bij de preventie en/of bestrijding van tf, worden in deze NRA gezien als beleidsinstrumenten.

Voorafgaand aan de expertmeeting is mede op basis van input van de aanvragers van het onderzoek, het ministerie van Financiën en de NCTV, de lijst van beleidsinstrumenten uit de NRA voor terrorismefinanciering 2019 geactualiseerd. Daarbij is geïnventariseerd welke nieuwe beleidsinstrumenten ter preventie en/of repressie van terrorismefinanciering er sinds 2020 zijn geïmplementeerd en welke aanpassingen er sindsdien zijn doorgevoerd in het al bestaande beleidsinstrumentarium. Dit leidde tot een geactualiseerde lijst van beleidsinstrumenten.

Aan de derde expertmeeting namen vertegenwoordigers van zes van de acht expertorganisaties deel die ook aan de tweede expertmeeting hadden deelgenomen (zie bijlage 3). Op het allerlaatste moment meldden vertegenwoordigers van twee expertorganisaties zich af voor deelname aan de expertmeeting. De geactualiseerde lijst van beleidsinstrumenten vormde de input voor de derde expertmeeting. Tijdens

⁴¹ In de MCA is per dreiging de Potentiële Impact berekend door toepassing van de volgende formule:

$$\text{Potentiële Impact} = \frac{\sum(C_i \times G_i)}{\sum G_i}$$
 waarbij C en G staan voor de expertscores op de Criteria en de Gewichten en i het criterium specificceert.

de plenaire bespreking van de beleidsinstrumenten voegden de experts nog diverse beleidsinstrumenten toe die naar hun mening een belangrijke rol spelen bij de preventie en/of bestrijding van terrorismefinanciering. De bespreking leidde tot een door de experts geaccordeerd overzicht van het beschikbare beleidsinstrumentarium voor de preventie en/of repressie van terrorismefinanciering (zie hoofdstuk 5).

Vervolgens werden de experts gevraagd om voor de 12 tf-dreigingen met de grootste potentiële impact een inschatting te maken van de mate waarin het totale pakket aan beschikbare beleidsinstrumenten ter preventie en/of repressie van terrorismefinanciering deze dreigingen tegengaat. Daarbij werd een schaal van 0 tot en met 100 toegepast, waarbij een score van 0 stond voor 'de dreiging blijft volledig bestaan' en een score van 100 stond voor 'de dreiging wordt volledig weggenomen door het beleidsinstrumentarium'. Na een eerste inschattingsronde werden de resultaten plenair besproken en kregen de experts de mogelijkheid om – in het geval dat de plenaire bespreking tot nieuwe inzichten had geleid – de eerdere inschatting aan te passen in de tweede inschattingsronde.

In het tweede onderdeel van de expertmeeting gingen de experts na of er verbetermogelijkheden zijn met betrekking tot het beleidsinstrumentarium.

8 *Kwantitatieve data*

De methodologie die in de eerdere NRA's is toegepast, vormde onderdeel van de landenevaluatie omtrent het Nederlandse beleid tegen witwassen en terrorismefinanciering die de FATF in 2022 afrondde. Het FATF (2022) oordeelde hierover in het *Mutual Evaluation Report*:

"The methodology of the NRAs is generally sound and based on a structural process to collect and evaluate qualitative inputs from policy, supervisory, law enforcement and private sector authorities through extensive surveys, meetings and interviews. However, inputs into the NRAs can be strengthened by the inclusion of additional quantitative sources."

Met het vergroten van de datagerichtheid werd in de vorige NRA al een aanzet gemaakt. Via de infobox Crimineel en Onverklaarbaar Vermogen (iCOV)⁴² waren destijds bij de relevante dataleveranciers van iCOV toestemmingsprocedures opgestart om toegang tot de benodigde data te krijgen. Helaas bleek de doorlooptijd van het NRA onderzoek te kort om alle benodigde toestemmingen te verkrijgen.⁴³ Hoewel in de nu voorliggende NRA in het contact met alle potentiële dataleveranciers van de start af aan aandacht is gevraagd voor het leveren van kwantitatieve data, bleek het ook nu weer lastig kwantitatieve dataoverzichten te verzamelen die zijn gericht op de grootste tf-dreigingen in de NRA.

Voor de vorige NRA konden data van Justis/TRACK worden betrokken om aanwijzingen te vinden voor en kwetsbaarheden ten aanzien van terrorismefinanciering via stichtingen. In de nu voorliggende NRA zijn deze data ook weer opgevraagd door het

⁴² iCOV is een samenwerkingsverband van de Belastingdienst, de Douane Nederland, de Nationale Politie, het OM, de FIOD, de Rijksrecherche, de FIU-Nederland, bijzondere opsporingsinstanties van de Inspectie Leefomgeving en Transport, de Nederlandse Voedsel- en Warenautoriteit en de Inspectie Sociale Zaken en Werkgelegenheid (SZW). Daarnaast nemen het Centraal Justitieel Incassobureau, DNB en de Autoriteit Consument en Markt deel. Zie: <https://icov.nl/organisatie/>.

⁴³ Voor meer hierover: Van der Veen & Heuts (2020b).

WODC en vervolgens verstrekt door Justis/TRACK. Hiernaast komt deze NRA tegemoet aan de wens van de FATF door het betrekken van andere databronnen.⁴⁴ Eerder werd al genoemd dat voor de contextanalyse kwantitatieve data van de FIU-Nederland (Jaaroverzichten), het OM en DNB zijn gebruikt. Ook heeft de FIOD informatie aangeleverd over het aantal afgeronde tf-onderzoeken van deze organisatie ten aanzien van de grootste tf-dreigingen. Deze verzoeken leverden nadere informatie op die is benut ter ondersteuning van de contextinformatie in hoofdstuk 3 en – in het geval van de FIOD-informatie – over het aantal FIOD-onderzoeken naar de grootste tf-dreigingen in hoofdstuk 4. Verder heeft het WODC een dataverzoek ingediend bij het FEC en de FIU-Nederland.⁴⁵ Deze verzoeken hebben echter niet geleid tot het verstrekken van kwantitatieve data. Redenen voor het niet verstrekken van kwantitatieve data zijn de tijdsinvestering die het vraagt om de kwantitatieve data uit datasystemen te destilleren in combinatie met de beperkte capaciteit bij organisaties om hier tijd voor vrij te maken, knelpunten dan wel onmogelijkheden om bepaalde relevante informatie uit de datasystemen van de organisaties te halen, en/of de vertrouwelijkheid van de betreffende informatie.

De verzamelde dataoverzichten zijn vooral gebruikt ter ondersteuning van de contextinformatie in hoofdstuk 3 en – in beperkte mate – voor een nadere toelichting op de grootste tf-dreigingen in hoofdstuk 4.

9 Validerende en evaluerende interviews

In de eindfase van het onderzoek is de opbrengst van de NRA, de lijst met de grootste tf-dreigingen met een ordening naar potentiële impact en weerbaarheid besproken met vertegenwoordigers van de AIVD, de FIOD, de FIU-Nederland, de Nationale Politie, de NVB en het OM. In de interviews zijn deze opbrengsten nagelopen waarbij gevraagd werd of zij de resultaten van de risicoanalyse herkenden. Ook werd nagegaan welke tf-risico's er naar verwachting in de nabije toekomst actueel gaan worden. Zie bijlage 2 voor een overzicht van de geïnterviewde organisaties.

Ten slotte is er in het kader van het groeimodel van de NRA een evaluerend groepsgebesprek gevoerd met de aanvragers van het onderzoek, het ministerie van Financiën (Directie Financiële Markten) en de NCTV. Het doel hiervan was het bespreken van het onderzoeksproces en een evaluatie van de momenten waarin de contacten van de aanvragers met het veld van onderzoek behulpzaam bleken of – in het geval van het verkrijgen van kwantitatieve data van dataleveranciers – nog beter benut kunnen worden in de toekomst.

⁴⁴ Omdat het WODC geen zicht heeft op de precieze aard en omvang van de data en andere informatie die deze partijen beschikbaar hebben, is een algemene vraag uitgegaan voor het leveren van data en kwalitatieve informatie. Wel zijn daarbij aanwijzingen gegeven voor het type kwantitatieve en kwalitatieve informatie dat voor de NRA behulpzaam zou zijn. Zo werd aangegeven dat de betreffende partij wellicht naar bepaalde dreigingen specifiek onderzoek heeft gedaan, waardoor er cijfermatige overzichten of kwalitatieve beschrijvingen van casuïstiek beschikbaar zijn. Ook is gevraagd uit de datasystemen informatie te leveren die zicht biedt op het jaarlijkse aantal zaken/dossiers per dreiging, achtergrondinformatie over de complexiteit van de zaak en/of een indicatie van de omvang van de zaak (bijvoorbeeld in euro).

⁴⁵ Zie vorige voetnoot.

3 Wat maakt Nederland kwetsbaar voor terrorismefinanciering?

De eerste stap binnen de ISO 31000 standaard voor risicomanagement is het uitvoeren van een contextanalyse. De contextanalyse die in dit hoofdstuk wordt gepresenteerd, is opgebouwd aan de hand van de kenmerken die van invloed kunnen zijn op de prevalentie van terrorismefinanciering, de potentiële impact daarvan en de keuzes van personen voor de door hen in te zetten tf-methoden en te gebruiken tf-bronnen. Het hoofdstuk beschrijft allereerst enkele geografische en demografische kenmerken van Nederland en gaat vervolgens in op verschillende religieuze, sociaal-culturele, politieke, economische en criminologische kenmerken van ons land. Per kenmerk is een box opgenomen waarin de relatie tussen het desbetreffende kenmerk en terrorismefinanciering wordt gelegd. Tot slot gaat het hoofdstuk in op het aantal afgeronde (onherroepelijke) tf-zaken volgens het OM en de aantallen VT's en VT-dossiers volgens de FIU-Nederland die betrekking hebben op terrorisme en/of terrorismefinanciering.

3.1 Geografische en demografische kenmerken

Nederland, een land in het noordwestelijk deel van Europa, is één van de 27 lidstaten van de EU. Op grond van het Verdrag van Schengen kunnen burgers van 27 deelnemende landen in Europa, waaronder Nederland, vrij reizen binnen de Schengenzone; grenscontroles zijn opgeheven tussen landen die lid zijn van Schengen.⁴⁶ Ook maakt Nederland deel uit van de Europese Economische Ruimte (EER). De EU en drie van de landen van de Europese Vrijhandelsassociatie (EVA) – Liechtenstein, Noorwegen en IJsland – vormen samen de EER. In de EER is sprake van vrij verkeer van goederen, personen, diensten en kapitaal.⁴⁷

Eind 2022 telde de Nederlandse bevolking volgens het Centraal Bureau voor de Statistiek (CBS) 17.811.291 mensen.⁴⁸ Na Malta is Nederland met ruim 500 personen per km² het meest dichtbevolkte land van de EU (Eurostat, 2023). In 2022 hadden ongeveer 4,4 miljoen Nederlanders een migratieachtergrond, waarvan circa 1,9 miljoen een westerse en circa 2,5 miljoen een niet-westerse migratieachtergrond. Tabel 3.1 geeft dit weer. De drie grootste groepen Nederlanders met een niet-westerse migratieachtergrond hadden dat jaar een Turkse (429.978), Marokkaanse (419.272) en Surinaamse (359.814) afkomst.⁴⁹

⁴⁶ Niet alle EU-landen behoren tot de Schengenzone. Dit geldt voor Bulgarije, Cyprus, Ierland en Roemenië. Wel tot de Schengenzone behoren de niet-EU-landen Liechtenstein, Noorwegen, IJsland en Zwitserland. [Welke landen zijn Schengenlanden? | Rijksoverheid.nl](#).

⁴⁷ [Welke landen horen bij de Europese Economische Ruimte \(EER\)? | Rijksoverheid.nl](#).

⁴⁸ [StatLine - Bevolkingsontwikkeling; maand en jaar \(cbs.nl\)](#). Geraadpleegd 2-11-2023.

⁴⁹ Bij deze groepen met niet-westerse migratieachtergrond gaat het om het totaal aantal personen met een 1^e en 2^e generatie migratieachtergrond.

Tabel 3.1 Migratieachtergrond Nederlandse bevolking in 2022

Migratieachtergrond ^a	Generatie ^b	Aantal
Westerse migratieachtergrond	1 ^e generatie	996.928
	2 ^e generatie	912.480
<i>Totaal</i>		<i>1.909.408</i>
Niet-westerse migratieachtergrond	1 ^e generatie	1.415.416
	2 ^e generatie	1.114.076
<i>Totaal</i>		<i>2.529.492</i>
Totaal		4.438.900

- a Een westerse migratieachtergrond heeft betrekking op één van de landen in Europa (exclusief Turkije), Noord-Amerika en Oceanië, en Indonesië (circa 19% van het totaal aantal Nederlanders met een westerse migratieachtergrond in 2022) en Japan. Een niet-westerse migratieachtergrond heeft betrekking op één van de landen in Afrika, Latijns-Amerika en Azië (exclusief Indonesië en Japan) of Turkije.
- b Een persoon met een 1^e generatie migratieachtergrond is in het buitenland geboren en heeft ten minste één in het buitenland geboren ouder. Een persoon met een 2^e generatie migratieachtergrond is in Nederland geboren en heeft ten minste één in het buitenland geboren ouder.

Bron: CBS Statline (2023). Geraadpleegd op 2-11-2023.

Box 3.1 Relatie geografische en demografische kenmerken met terrorismefinanciering

Het zonder grenscontroles reizen van personen in de Schengenzone en vrij verkeer van personen, goederen, diensten en kapitaal tussen de EER-landen maken verhulling van een criminele oorsprong van vermogen mogelijk, omdat dit het volgen van de *paper trail* van transacties bemoeilijkt dan wel onmogelijk maakt. Ook maakt het fysieke verplaatsing over land van contant geld en grootwaardeproducten zonder grenscontroles binnen de EER mogelijk.

Volgens de AIVD en de NCTV is de internationale jihadistische beweging één van de belangrijkste terroristische dreigingen in Nederland (zie ook paragraaf 3.6). Het jihadisme is een militante, extremistische en revolutionaire ideologische stroming die zich beroept op de islam^a en die oproept tot het voeren van een 'heilige oorlog' tegen 'ongelovigen'. Jihadisten claimen de islam om hun overtuigingen en manier van leven met geweld op te leggen aan anderen.^b Ten tijde van de vorige NRA Terrorismefinanciering meldde de AIVD dat er verhoudingsgewijs veel Nederlandse jihadististen van onder meer Marokkaanse en Turkse afkomst waren (Van der Veen & Heuts, 2020b). Om deze reden is in deze NRA ook een beschrijving gegeven van het aantal Nederlanders met een westerse en niet-westerse migratieachtergrond. Ongeveer één op de zeven Nederlanders heeft een niet-westerse migratieachtergrond, waarvan circa 34% een Turkse of Marokkaanse afkomst heeft (in totaal 849.250 personen per 1 januari 2022¹). Gezien het feit dat er in Nederland naar schatting zo'n 500 aanhangers van het jihadistisch gedachtegoed zijn (zie ook paragraaf 3.6), betreft dit – in het geval dat zij allen een niet-westerse migratieachtergrond zouden hebben – slechts een zeer klein deel van de Nederlanders met een niet-westerse migratieachtergrond (namelijk 0,02%).

- a [Jihadistische dreiging tegen Nederland | Terrorisme | AIVD](#).
- b [Jihadisme tegengaan | Terrorismebestrijding | Rijksoverheid.nl](#).
- c [Bevolking; geslacht, lft, generatie en migr.achtergrond, 1 jan; 1996-2022 | CBS](#).

3.2 Religieuze kenmerken

Ongeveer 57% van de Nederlandse bevolking (vanaf 15 jaar) rekent zich niet tot een bepaalde kerkelijke gezindte (zie tabel 3.2). Bijna één op de vijf is Rooms-Katholiek, zo'n 13% is protestants en ongeveer zes% is islamitisch. Tabel 3.2 laat verder zien dat circa vier op de vijf Nederlanders (vanaf 15 jaar) zelden of nooit een religieuze dienst bezoekt. Wat betreft het bezoeken van religieuze diensten bestaan er grote verschillen tussen de geloofsgroepen (dit wordt niet weergegeven in de tabel): circa 31% van de protestanten gaat ten minste één keer per week naar de kerk. Wat moslims betreft bezoekt zo'n 22% minstens eenmaal per week de moskee. Van de katholieken woont ongeveer 4% ten minste één keer per week een religieuze dienst bij.⁵⁰

Tabel 3.2 Kerkelijke gezindte en bezoek aan religieuze dienst in 2022

Kerkelijke gezindte <i>(personen van 15 jaar of ouder)</i>	Aandeel	Bezoek religieuze dienst <i>(personen van 15 jaar of ouder)</i>	Aandeel
Geen kerkelijke gezindte	57%	1 keer per week of vaker	7%
Rooms-Katholiek	18%	2-3 keer per maand	3%
Protestants	13%	1 keer per maand	3%
Islam	6%	Minder dan 1 keer per maand	5%
Andere gezindte	6%	Zelden of nooit	83%

Bron: [Religieuze betrokkenheid in Nederland \(cbs.nl\)](#).

Box 3.2 Relatie religieuze kenmerken met terrorismefinanciering

In box 3.1 kwam al aan bod dat de internationale jihadistische beweging door de AIVD en de NCTV gezien wordt als één van de belangrijkste terroristische dreigingen in Nederland en dat er in Nederland zo'n 500 aanhangers van het jihadistisch gedachtegoed zijn. Om deze reden werd in deze paragraaf ingegaan op de kerkelijke gezindte van Nederlanders en de frequentie van hun bezoek aan religieuze diensten. Circa één op de twintig Nederlanders is islamitisch en daarvan is één op de vijf dermate religieus dat zij ten minste eenmaal per week de moskee bezoeken. Het geschatte aantal van 500 aanhangers van het jihadistisch gedachtegoed betreft slechts een zeer klein deel (0,2%)^a van de Nederlandse moslims die ten minste eenmaal per week naar de moskee gaan.

- a Daarbij is uitgegaan van de totale Nederlandse bevolking eind 2022 (17.811.291), maar is er geen onderscheid gemaakt naar leeftijd (terwijl tabel 3.2 betrekking heeft op personen van 15 jaar en ouder).

3.3 Sociaal-culturele en politieke kenmerken

Nederland kan worden gekenmerkt als een modern, dichtbevolkt, internationaal georiënteerd land met een veelheid aan buitenlandse handelsbetrekkingen, migratiebewegingen, culturele uitwisselingen, netwerken, allianties en samenwerkingsverbanden (Besamusca & Verheul, 2010). Nederland is een constitutionele monarchie met een lange democratische traditie, een internationaal georiënteerde economie met een uitgebreid welvaartsysteem en een op consensus gerichte politieke cultuur. Besamusca & Verheul (2010) zien de onderling samenhangende begrippen tolerantie, verzuiling en het Poldermodel als kernelementen voor de Nederlandse cultuur en maatschappij (Besamusca & Verheul, 2010). Wat

⁵⁰ [Religieuze betrokkenheid in Nederland \(cbs.nl\)](#).

betreft politieke kenmerken waren er de afgelopen decennia enkele belangrijke ontwikkelingen in de Nederlandse samenleving, te weten een polarisatie, versplintering van het politieke stelsel en afnemend vertrouwen in de politiek. Hieronder worden deze onderling samenhangende elementen en hun uitwerking besproken.

Tolerantie

Nederland staat bekend als een tolerant land. In de 16^e eeuw was de Republiek der Verenigde Nederlanden het eerste land ter wereld met een vorm van godsdienstvrijheid (Mijnhardt, 2010). Dit leidde tot een grote instroom van religieuze vluchtelingen uit andere landen die in Nederland relatief ongestoord hun godsdienst konden belijden. Vanaf de jaren '60 van de vorige eeuw, ten tijde van de ontkerkelijkking, ontstond in Nederland een nieuw, meer op het individu georiënteerd mensbeeld met een nadruk op persoonlijke ontwikkeling, ondernemerschap, creativiteit en zelfexpressie. Deze culturele revolutie rekende af met de oude waarden van conformiteit en vormde de basis voor een nieuwe periode van gedogen en tolerantie, met name op terreinen als homoseksualiteit, emancipatie, abortus, homohuwelijk, softdrugs en euthanasie.

In 2022 waren er, zo werd al in paragrafen 3.1 en 3.2 aangegeven, ongeveer 2,5 miljoen Nederlanders met een niet-westerse migratieachtergrond en was circa 6% van de Nederlanders moslim. Na de 9/11 aanslagen in New York en de dodelijke aanslag op Pim Fortuyn door een links-extremist in 2002 werden in het voordien tolerante Nederland vanaf dan scherpe(re) standpunten ingenomen op thema's als immigratie en de Europese eenwording, niet alleen door de dan opgerichte anti-immigratiepartijen, zoals de PVV,⁵¹ maar ook door middenpartijen. Deze ontwikkeling vond in dezelfde periode ook plaats in andere Europese landen. Na de 9/11 aanslagen en andere aanslagen in Europa nam in Nederland de tolerantie en het gedogen ten opzichte van moslims af. Mede als reactie daarop ontstonden aan de andere kant van het politiek spectrum politieke partijen die zich speciaal richtten op het behartigen van de belangen van bevolkingsgroepen met een migratieachtergrond.⁵² Deze partijen hebben inmiddels vaste voet aan de grond gevonden en zijn vertegenwoordigd in het parlement.

Poldermodel

Tot het midden van de jaren '60 was Nederland voornamelijk verzuild georganiseerd, volgens de lijnen van de religieuze en politieke denominaties. Naar denominatie onderscheiden instituties zoals scholen, verenigingen, vakbonden, omroeporganisaties en politieke partijen bestonden naast en los van elkaar. In de jaren '60 ontkerkelijkte Nederland en nam de verzuiling langzamerhand af. Desalniettemin bevat de huidige Nederlandse maatschappij nog veel sporen uit het verzuilde verleden, bijvoorbeeld in politieke partijen, omroepen, werknemersorganisaties en onderwijsinstellingen.

Het Poldermodel wordt gekenmerkt door het samenwerken van partijen met verschillende belangen, waarbij wordt gezocht naar consensus en compromissen (Van Zanden, 2010). Hoewel de toepassing van het Poldermodel tijdsintensief is, is het een groot voordeel dat alle relevante partijen betrokken worden en dat bij de besluitvorming rekening kan worden gehouden met hun belangen. Besluiten die via het Poldermodel worden genomen, mogen dan ook op draagvlak rekenen. Het

⁵¹ In november 2023 was de PVV de grote winnaar van de Tweede Kamer-verkiezingen. Deze politieke partij heeft in haar verkiezingsprogramma verschillende anti-islam standpunten opgenomen.

⁵² [Aanbod aan migrantenpartijen sterk toegenomen \(nos.nl\)](#).

Poldermodel wordt breed toegepast, bijvoorbeeld bij onderhandelingen over arbeidsvoorwaarden en lonen tussen overheid, vakbonden en werkgeversorganisaties en bij besluitvorming over zorg en onderwijs. Ook bij de vorming van Nederlandse regeringen komt de Poldermodel-benadering terug. Bij Nederlandse verkiezingen kan geen van de politieke partijen rekenen op een meerderheid van stemmen. Om een regering te kunnen vormen moeten partijen samenwerken en coalities sluiten met andere partijen. Omdat bij het Poldermodel conflicten zoveel mogelijk worden vermeden, is in Nederland een stabiele politieke constellatie ontstaan.

Vanuit de cultuur van het Poldermodel zijn er voor de preventie en bestrijding van terrorismefinanciering in Nederland in vergelijking met de meeste andere landen relatief veel initiatieven ontplooid waarbij organisaties samenwerking met andere organisaties zoeken om op effectievere manier terrorismefinanciering tegen te gaan. Onder meer ter bestrijding van terrorisme nam de Nederlandse krijgsmacht de afgelopen jaren deel aan een groot aantal militaire vredesmissies dat wereldwijd wordt of werd uitgevoerd. Het gaat om grote en kleinere missies, onder meer in Irak, Afghanistan, Bahrein, Libië en Mali.

Politieke versplintering, polarisatie en afnemend vertrouwen in de politiek

Naast de opkomst van nieuwe politieke partijen waren er de afgelopen decennia diverse afsplitsingen binnen partijen die al in de Tweede Kamer waren vertegenwoordigd. Als gevolg hiervan bestaat de Tweede Kamer inmiddels uit 15 fracties.⁵³ In dit verband wordt wel gesproken over versplintering.⁵⁴ De versplintering in de politiek gaat gepaard met verslechterde omgangsvormen in het Nederlandse parlement, waarin polarisatie, extreme uitingen en verharding in politieke debatten in toenemende mate als problematisch worden gezien.⁵⁵

De gevolgen van de polarisatie werken ook door in de Nederlandse samenleving. Eind 2022 maakte circa driekwart van de Nederlandse bevolking zich zorgen over toenemende tegenstellingen in de Nederlandse samenleving en conflicten en meningsverschillen tussen burgers met verschillende politieke opvattingen (Verbeek-Oudijk et al., 2023). Als redenen hiervoor wordt gewezen op de katalyserende rol van de Corona-pandemie-crisis in de periode van maart 2020 tot begin 2022, de verharding van het politieke debat en de extreme uitingen in sociale media (Snel et al., 2023). In sociale media zoeken mensen naar bevestiging van hun eigen overtuigingen en eigen gelijk. Ook graven zij zich daar in 'echokamers' in, waarin geen ruimte is voor afwijkende meningen (Miltenburg et al., 2022).

⁵³ [Fracties | Tweede Kamer der Staten-Generaal](#). Stand van zaken december 2023.

⁵⁴ [Versplintering - Parlement.com](#).

⁵⁵ Dit gaf aanleiding om op 9 maart 2022 een debat in de Tweede Kamer te voeren over parlementaire omgangsvormen. Het doel was grenzen te stellen aan verruwing in het debat.

Box 3.3 Relatie sociaal-culturele kenmerken met terrorismefinanciering

In de afgelopen twee decennia worden in Nederland steeds scherpe(re) standpunten ingenomen op thema's als immigratie. Na de 9/11 aanslagen en andere aanslagen in Europa is in Nederland de tolerantie en het gedogen ten opzichte van moslims afgenomen. Enerzijds kan deze verminderde tolerante houding leiden tot rechtsextremistische acties – en in zijn uiterste vorm terroristische daden – gericht op moslims. Anderzijds kan de verminderde tolerante houding ten opzichte van moslims aanleiding zijn voor jihadisten om terroristische activiteiten in ons land te plegen. Paragraaf 3.6 gaat nader in op de terroristische dreiging vanuit jihadistische en rechtsextremistische hoek.

De deelname van de Nederlandse krijgsmacht aan een groot aantal militaire vredesmissies dat wereldwijd wordt of werd uitgevoerd, kan er mogelijk toe leiden dat terroristische groeperingen besluiten financiële of andere middelen vrij te maken voor het plegen van aanslagen in Nederland (of tegen Nederlandse belangen in het buitenland).

De versplintering in de Nederlandse politiek gaat gepaard met verslechterde omgangsvormen in het parlement, waarin polarisatie, extreme uitingen en verharding in politieke debatten in toenemende mate als problematisch worden gezien.^a Dit kan leiden tot vormen van extremisme, hetgeen op zijn beurt in zijn uiterste vorm volgens de AIVD tot terrorisme kan leiden.^b

a [Burgerperspectieven bericht 2 2022 | Publicatie | Sociaal en Cultureel Planbureau \(scp.nl\)](#).

b [Extremisme | AIVD](#).

3.4 Economische kenmerken

Bancaire financiële dienstverlening

Nederland kent een relatief grote en internationaal georiënteerde bankensector die medio oktober 2023 93 vergunde banken omvatte (zie tabel 3.3). Hieronder vallen 39 banken met een DNB-vergunning, 49 banken met een buitenlandse bankvergunning en vijf 'online banken' (zie hieronder voor meer informatie) met een DNB- dan wel buitenlandse bankvergunning.

Tabel 3.3 Aantal vergunde banken in Nederland

Sector	Aantal instellingen
Banken met een DNB-vergunning	39
Banken met een buitenlandse bankvergunning	49
Online banken met een DNB-vergunning ^a	3
Online banken met een buitenlandse bankvergunning ^a	2
Totaal	93

a Hierbij is DNB uitgegaan van de definitie van 'online banken' die het WODC heeft aangedragen. 'Online banken' zijn banken die alleen via *online* platforms hun diensten aanbieden en dus geen fysieke kantoren hebben.

Bron: data voor deze NRA aangeleverd door DNB op 18 oktober 2023.

De totale bankensector had in het laatste kwartaal van 2022 een balanstotaal van 2.625 miljard euro, circa 330% van het bruto binnenlands product (bbp).⁵⁶ ING, de Rabobank en ABN AMRO zijn veruit de grootste banken van Nederland. Respectievelijk hadden deze consumentenbanken in die periode een balanstotaal van 968 miljard euro, 628 miljard euro en 380 miljard euro. Van de dertien grootste banken in Nederland hadden deze drie grootbanken in 2022 een gezamenlijk marktaandeel van 84%.⁵⁷ Ook de Volksbank is een consumentenbank die eveneens wordt aangemerkt als grootbank. Wel viel het balanstotaal van de Volksbank met 73 miljard euro in het vierde kwartaal van 2022 veel lager uit dan de drie andere grootbanken. Naast de vier grootbanken kende het Nederlandse bankenlandschap eind 2022 in totaal 35 kleine of middelgrote banken met een DNB-vergunning. De 49 in Nederland actieve banken met een buitenlandse bankvergunning betreffen dochters en branches met relatief lage balanstotalen, en vormen dus een klein aandeel in de Nederlandse bankensector.⁵⁸

Sinds de jaren '10 ontstaan er volledig digitale banken. Deze opereren in tegenstelling tot de traditionele banken zonder fysieke kantoren en verlenen hun diensten uitsluitend via *online* platforms en apps en tegen relatief lage kosten. Digitale banken worden ook wel aangeduid als neobanken, virtuele banken, *online* banken en internetbanken. In het afgelopen decennium zijn de digitale banken snel gegroeid.⁵⁹ Aanjagers hiervoor zijn de snelle opkomst van mobiele telefonie, ondersteunende regelgeving (zoals de inwerkingtreding van de Europese *Payment Service Directive 2, PSD2*⁶⁰) en de Corona-pandemie (Nanaeva et al., 2021). De meeste van deze digitale banken opereren met een buitenlandse bankvergunning. In Nederland zijn volgens opgave van DNB vijf digitale banken actief: Brand New Day, Bunq, Revolut, FlatexdeGiro en Knab.

De hierboven vermelde banken beschikken over een Nederlandse of buitenlandse bankvergunning. Een niet-vergunde vorm van bankieren betreft ondergronds bankieren. De Minister van JenV definieert ondergronds bankieren als 'het verlenen van betaaltransacties buiten de wettelijk gereguleerde financiële instellingen om, oftewel bankieren zonder vereiste vergunning' (Minister van JenV, 2022). In hoofdstuk 4 wordt nader ingegaan op verschillende vormen van ondergronds bankieren.

Niet-bancaire financiële dienstverlening

Personen die terrorisme financieren, maken veelal ook gebruik van de diensten van niet-bancaire financiële dienstverleners. Het kan dan bijvoorbeeld gaan om betaaldienstverleners⁶¹ als *Payment Service Providers* (PSP's) en geldtransactiekantoren, en aanbieders van cryptodiensten. Hieronder worden de niet-

⁵⁶ [THE NETHERLANDS - EBF](#).

⁵⁷ [Balanstotaal van Nederlands grootste banken met 2% gekrompen](#).

⁵⁸ De cijfers die DNB over buitenlandse banken in Nederland publiceert, zijn niet concludent. Volgens DNB wordt dit "veroorzaakt door de zgn. *Opt-in* banken. *Opt-in* banken zijn banken waarvan de vergunning niet langer kwalificeert als vergunning volgens art. 2.11 van Wft, maar waarvan de vergunning onder 'opt-in' valt. *Opt-in* banken zijn inbegrepen in het totaal, maar behoren niet tot de gepresenteerde classificaties." Zie: [Data zoeken - DNB](#).

⁵⁹ [Europe Neobanking Market Size & Share Analysis - Industry Research Report - Growth Trends \(mordorintelligence.com\)](#). Geraadpleegd op 2-11-2023.

⁶⁰ PSD2 is een Europese wet voor het betalingsverkeer van consumenten en bedrijven die in februari 2019 in Nederland is ingevoerd.

⁶¹ PSD2 onderscheidt acht betaaldiensten waarvoor een vergunning nodig is. Het behandelen van al deze typen valt buiten het bestek van deze NRA.

bancaire financiële dienstverleners behandeld die gerelateerd kunnen worden aan de tf-dreigingen in deze NRA (zie hoofdstuk 4).

PSP's

PSP's zijn betaaldienstverlenende bedrijven die ondernemingen, bijvoorbeeld webwinkeliers, in staat stellen *online* betaalmethoden te accepteren. Hierbij kan worden gedacht aan bankoverschrijvingen via iDeal en betalingen via creditcards, debetcards, e-wallets etc. Binnen de EU dienen PSP's tegemoet te komen aan de richtlijnen van de PSD2. PSP's dienen te beschikken over een vergunning die wordt verstrekt door de toezichthouder in het EU-land van vestiging van de PSP. Voor in Nederland gevestigde PSP's is DNB de toezichthouder. PSP's met een vergunning uit een ander EU-land kunnen via een zogenaamd EU-paspoort ook in alle andere EER-landen betaaldiensten aanbieden. Medio oktober 2023 beschikten 68 PSP's over een DNB-vergunning en negen PSP's over een buitenlandse vergunning (zie tabel 3.4).

Geldtransactiekantoren

Geldtransactiekantoren (of *money transfer organisations*) zijn betaaldienstverleners die zich bezighouden met het bedrijfsmatig uitvoeren van geldtransacties of het verrichten van werkzaamheden gericht op de totstandkoming van zulke transacties. Volgens DNB is van geldtransacties sprake als een betaalinstelling van een betaler geld ontvangt met als enig doel het daarmee corresponderende bedrag rechtstreeks over te maken aan een begunstigde of aan een andere betalingsdienstverlener die de gelden aan de uiteindelijk begunstigde uitkeert. Geldtransacties hebben in de praktijk vooral betrekking op het overmaken van geld naar begunstigden in het buitenland, met name naar landen met een minder ontwikkeld banksysteem en waar het gebruik van bankrekeningen minder voorkomt. Ook voor onverwachte spoedbetalingen wordt van geldtransactiekantoren gebruikgemaakt.⁶² Transacties kunnen zowel contant als giraal plaatsvinden.

Geldtransactiekantoren vallen net als PSP's onder de Wwft en moeten op basis van de Wet op het financieel toezicht (Wft) over een door DNB verstrekte vergunning beschikken om hun diensten te verlenen of moeten beschikken over een buitenlandse vergunning. Medio oktober 2023 beschikten acht geldtransactiekantoren over een DNB-vergunning en zes geldtransactiekantoren over een buitenlandse vergunning (zie tabel 3.4).

In Nederland zijn ook betaaldienstagenten van geldtransactiekantoren actief. Deze moeten genotificeerd zijn bij DNB door het geldtransactiekantoor waarvan zij agent zijn (en dat geldtransactiekantoor moet weer een DNB- of buitenlandse vergunning hebben). Deze betaaldienstagenten staan onder toezicht van DNB, die daar ter plekke onderzoek kan doen. Tabel 3.4 geeft weer dat er in april 2023 104 betaaldienstagenten actief waren, waarvan er 99 over een DNB-vergunning en vijf over een buitenlandse vergunning beschikten.

⁶² [Betaaldiensten waarvoor een vergunning nodig is \(dnb.nl\)](https://www.dnb.nl/nl/over-dnb/vergunningen/vergunningen-voor-betaaldiensten).

Tabel 3.4 Aantallen vergunde PSP's en geldtransactiekantoren (per medio oktober 2023) en vergunde betaaldienstagenten (per april 2023)

Sector	Aantal
PSP's met een DNB-vergunning	68
PSP's met een buitenlandse vergunning	9
Geldtransactiekantoren met een DNB-vergunning	8
Geldtransactiekantoren met een buitenlandse vergunning	6
Betaaldienstagentschappen met een DNB-vergunning	99
Betaaldienstagentschappen met een buitenlandse vergunning	5

Bron: data voor deze NRA aangeleverd door DNB op 18 oktober 2023.

Cryptodienstverlening

Tot op heden zijn er bijna 8.000 *crypto currencies* (virtuele valuta of crypto's) gecreëerd. Een groot deel daarvan is inmiddels echter alweer verdwenen. Naar schatting zijn er op dit moment 4.000-5.000 crypto's in omloop, waarvan Bitcoin en Ethereum *het meest bekend zijn*. De top 5 crypto's is samen goed voor ongeveer 80% van de markt.⁶³ Medio 2022 had volgens DNB naar schatting 14% van de Nederlanders crypto's.⁶⁴

Sinds mei 2020 vallen bedrijven die diensten aanbieden voor het wisselen tussen crypto's en regulier geld evenals bedrijven die cryptobewaarpotemonnees aanbieden, onder het toezicht van DNB. Aanbieders van cryptodiensten die in of vanuit Nederland actief willen worden, moeten een inschrijving in het openbaar register van DNB aanvragen. Daarvoor moeten ze kunnen aantonen dat ze voldoen aan de Wwft en de Sanctiewet 1977 (zie hoofdstuk 5 voor meer informatie hierover).⁶⁵ Voor entiteiten die enkel wisselen tussen crypto's, geldt voornamelijk geen registratieplicht.⁶⁶ Tabel 3.5 laat zien dat er medio oktober 2023 36 wisseldienst-aanbieders en 31 aanbieders van een bewaarpotemonnee waren geregistreerd bij DNB.

Tabel 3.5 Aantal geregistreerde aanbieders van cryptodiensten

Sector	Aantal
Aanbieders van diensten voor het wisselen tussen crypto's en regulier geld	36
Aanbieders van een bewaarpotemonnee	31

Bron: data voor deze NRA aangeleverd door DNB op 18 oktober 2023.

Export

Nederland was in 2022 met US\$ 966 miljard de op drie na grootste exporteur ter wereld van goederen. Alleen China, de Verenigde Staten (VS) en Duitsland exporteerden in 2022 meer goederen dan Nederland. Naast goederen exporteert Nederland ook veel diensten. In 2022 nam Nederland met een export van diensten ter waarde van US\$ 270 miljard de negende plaats in op het jaarlijks verschijnende *World Trade Statistical Review* van de *World Trade Organization* (WTO, 2023).

⁶³ [Hoe werken Cryptocurrencies? Wij leggen het je uit! \(techopedia.com\)](#).

⁶⁴ [Wat u moet weten over crypto's \(dnb.nl\)](#).

⁶⁵ [Register van aanbieders van cryptodiensten \(dnb.nl\)](#).

⁶⁶ [Geen registratieplicht bij DNB voor aanbieders van crypto-to-crypto omwisseldiensten](#).

In 2021 maakte de toegevoegde waarde van de export van producten en diensten 32,6% uit van het bbp.⁶⁷ Van de in 2021 geëxporteerde producten was 77% gericht op Europa, voornamelijk Duitsland, België, Frankrijk en het Verenigd Koninkrijk (VK). De belangrijkste exportproducten in 2021 waren machines en apparaten, fabricaten (zoals kleding, papier en karton en ijzer- en metaalproducten) en chemische producten. Tezamen hadden deze een aandeel in de export van producten van circa 64%. Bij de export van diensten in 2021 vormden zakelijke diensten en vervoersdiensten de grootste categorieën. Samen maakten deze circa 52% uit van de export van diensten (CBS, 2023).

Luchthavens en zeehavens

Nederland heeft met Schiphol één van de grootste luchthavens ter wereld. Volgens de *Airports Council International* stond Schiphol in 2022 qua passagiersaantallen met bijna 53 miljoen passagiers op de dertiende plaats in de lijst van grootste luchthavens.⁶⁸ Binnen West-Europa namen alleen de luchthavens van Londen en Parijs nog hogere posities in. Naast Schiphol kent Nederland nog enkele kleinere luchthavens met internationale vluchten: Eindhoven *Airport*, Rotterdam *The Hague Airport*, Maastricht Aachen *Airport* en Groningen *Airport* Eelde.

De haven van Rotterdam was in 2022 de grootste overslaghaven van Europa, gevolgd door de havens van Antwerpen, Hamburg en Valencia.⁶⁹ Tot het havengebied Rotterdam behoren ook de havens van Moerdijk, Dordrecht en Vlaardingen. In 2021 werd hier 457 miljoen ton aan goederen overgeslagen (van de in totaal 593 miljoen ton aan goederen die werden overgeslagen in de Nederlandse zeehavens). Andere belangrijke zeehavens in Nederland zijn Amsterdam (inclusief Velsen/IJmuiden, Beverwijk en Zaanstad), *North Sea Port* (Vlissingen en Terneuzen, exclusief Gent) en Groningen *Seaports* (Delfzijl en Eemshaven).⁷⁰

Box 3.4 Relatie economische kenmerken met terrorismefinanciering

Nederland kenmerkt zich door een grote en internationaal georiënteerde financiële sector. Personen, groepen personen of organisaties die terrorisme financieren, kunnen op verschillende manieren gebruikmaken van het financiële stelsel in Nederland. Geldtransacties kunnen contant of op girale wijze via vergunde banken of (on)vergunde betaaldienstverleners plaatsvinden. Verder bieden crypto's (groepen) personen of organisaties de mogelijkheid om terrorisme te financieren. Het feit dat Nederland een open, op handel gerichte economie heeft en één van de grootste exporteurs ter wereld is, kan van invloed zijn op de prevalentie van terrorismefinanciering via fysieke verplaatsing van contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland. De toegangshavens tot Nederland kunnen worden gebruikt bij de import en export van legale goederen en illegale goederen als verboden wapens en drugs, waarbij de op die wijze verkregen middelen gebruikt kunnen worden voor terrorismefinanciering.

⁶⁷ [StatLine - Verdiensten en arbeidsvolume; uitvoerstromen \(cbs.nl\)](#). Geraadpleegd op 2-11-2023.

⁶⁸ [ACI World confirms top 20 busiest airports worldwide | ACI World](#).

⁶⁹ [Top-15 container ports in European Union in 2022 – PortEconomics](#).

⁷⁰ [Welke zeehavens zijn er in Nederland? \(cbs.nl\)](#).

3.5 Criminologische kenmerken

Eerder werd al genoemd dat de financiële middelen die gebruikt worden voor terrorismefinanciering, zowel een legale als een criminele herkomst kunnen hebben. Vanwege de potentiële criminele herkomst van middelen bedoeld voor terrorismefinanciering beschrijft deze paragraaf enkele criminologische kenmerken van Nederland.

Algemeen

In Nederland vonden in de periode 2019-2022 volgens het CBS jaarlijks rond de 800.000 geregistreerde⁷¹ misdrijven plaats (zie tabel 3.6). Daarbij gaat om een breed palet aan misdrijven: vermogensmisdrijven waaronder vormen van fraude maar ook diefstal/verduistering en inbraak, drugsmisdrijven, vuurwapenmisdrijven, misdrijven met betrekking tot mensenhandel en mensensmokkel en cybercriminaliteit.

Tabel 3.6 Geregistreerde misdrijven in Nederland in 2019-2022

	2019	2020	2021 ^a	2022 ^a
Aantal misdrijven	821.905	813.150	757.795	806.210

a Voor 2021 en 2022 gaat het om voorlopige resultaten.

Bron: CBS Statline. Geraadpleegd op 2-11-2023.

Onderstaande subparagrafen beschrijven wat er bekend is over de prevalentie van de verschillende criminaliteitsvormen waarmee illegaal geld verkregen wordt dat gebruikt kan worden voor de financiering van terrorisme.

Fraude

Het OM omschrijft fraude als 'opzettelijke misleiding om onrechtmatig voordeel te verkrijgen'.⁷² Fraude is in feite een containerbegrip waaronder veel verschillende fraudevormen vallen, zoals belastingfraude, faillissementsfraude, sociale fraude en identiteitsfraude die in fysieke en/of *online* vorm kunnen plaatsvinden. Er bestaat een onderscheid tussen 'horizontale fraude' waarbij burgers, bedrijven of instellingen het slachtoffer zijn, en 'verticale fraude' waarbij de overheid het slachtoffer is.⁷³

Uit onderzoek van Junger et al. komt naar voren dat in 2020 circa 16% van de Nederlanders van 16 jaar en ouder slachtoffer waren van fraude. Grofweg 70% van de fraude vond geheel *online* plaats en ongeveer 18% was een combinatie van offline en *online*. Een deel van de Nederlanders (circa 6%) was vaker dan één keer slachtoffer. Aankoopfraude (bestelde en betaalde producten of diensten worden niet geleverd) maakte in 2020 de meeste slachtoffers (ongeveer 11%), slachtofferschap van andere onderzochte fraudevormen lag rond de 1-2% (Junger et al., 2022).⁷⁴ Wat betreft *online* fraude en oplichting geeft het CBS aan dat in 2022 8% van de Nederlanders van 15 jaar en ouder slachtoffer hiervan was. Net als in de studie van Junger et al. ging

⁷¹ Volgens het CBS is een 'geregistreerd misdrijf' dat alleen door de politie is vastgelegd in een proces-verbaal van aangifte of in een ambtshalve opgemaakt proces-verbaal.

⁷² [Fraude | Openbaar Ministerie \(om.nl\)](#).

⁷³ [Van bankrekeningfraude tot hulpvraagfraude - Het CCV](#).

⁷⁴ In dit onderzoek werden 12 fraudecategorieën gemeten: 1. investeringsfraude, 2. aankoopfraude, 3. baanfraude, 4. prijsfraude, 5. schuldfraude, 6. goede-doelenfraude, 7. datingfraude, 8. vriend-in-noodfraude (waaronder Whatsapp-fraude), 9. phishing, 10. identiteitsfraude, 11. spoofing (waaronder helpdeskfraude) en 12. overige fraudevormen.

het daarbij in de meeste gevallen om aankoopfraude, maar het CBS meldt ook dat verkoopfraude (het slachtoffer verkoopt iets maar wordt niet betaald), fraude in het betalingsverkeer (een crimineel krijgt toegang tot de creditcard of bankrekening van het slachtoffer en boekt daar geld vanaf), identiteitsfraude (een crimineel maakt illegaal gebruik van iemands persoonsgegevens) en *phishing* (het slachtoffer raakt geld kwijt aan een crimineel die zich voordoeft als iemand anders of als een vertrouwde instantie) voorkwamen.⁷⁵

Tabel 3.7 Geregistreeerde vormen van fraude in 2019-2022

	2019	2020	2021 ^a	2022 ^a
Bedrog	53.005	60.375	52.895	43.360
<i>Oplichting</i>	51.045	58.460	51.115	41.835
<i>Bedrog (overig)</i>	1.955	1.915	1.775	1.520
Valsheidsmisdrijf	36.225	70.665	69.340	45.675
<i>Muntmisdrijf</i>	1.540	1.130	725	400
<i>Valsheid in zegels en merken</i>	170	200	240	180
<i>Valsheid in geschriften</i>	34.515	69.335	68.375	45.100
Bankbreuk	110	110	60	45
Totaal	89.340	131.150	122.295	89.080

a Voor 2021 en 2022 gaat het om voorlopige resultaten.

Bron: CBS Statline. Geraadpleegd op 2-11-2023.

Het CBS onderscheidt enkele vormen van vermogenscriminaliteit die onder de noemer 'fraude' geschaard kunnen worden (zie tabel 3.7): bedrog, valsheidsmisdrijven en bankbreuk (een juridische term voor faillissementsfraude). In 2022 ging het in totaal om circa 89.000 geregistreeerde misdrijven. Dit is ongeveer hetzelfde aantal als in 2019, maar een stuk minder dan in de jaren van het hoogtepunt van de Corona-pandemie in 2020 en 2021. In die jaren lag het aantal misdrijven met betrekking tot valsheid in geschriften veel hoger dan in 2019 en 2022.

Vermogenscriminaliteit

Ook de opbrengsten van andere vormen van vermogenscriminaliteit (dan fraude) kunnen gebruikt worden voor de financiering van terrorisme, namelijk diefstal/verduistering en inbraak, heling, en afpersing en afdreiging. In 2022, toen de Corona-pandemie op zijn eind liep, hadden bijna 360.000 geregistreeerde misdrijven betrekking op diefstal/verduistering en inbraak. Dat is een stuk hoger dan in 2020 en 2021 maar lager dan in 2019. Het aantal geregistreeerde misdrijven met betrekking tot heling, afpersing en afdreiging was in de periode 2019-2022 veel kleiner dan het aantal geregistreeerde misdrijven wat betreft diefstal/verduistering en inbraak. Tabel 3.8 geeft het een en ander weer.

⁷⁵ [4. Online oplichting en fraude \(cbs.nl\)](#).

Tabel 3.8 **Geregistreeerde andere vormen van vermogenscriminaliteit in 2019-2022**

	2019	2020	2021 ^a	2022 ^a
Diefstal/verduistering en inbraak	374.790	330.095	287.045	349.035
Heling	6.410	6.130	5.545	6.550
Afpersing en afdreiging	1.785	2.260	2.220	2.105
Totaal	382.985	338.485	294.810	357.690

a Voor 2021 en 2022 gaat het om voorlopige resultaten.

Bron: CBS Statline. Geraadpleegd op 2-11-2023.

Drugsmisdrijven

De Opiumwet regelt in Nederland de opsporing, vervolging en berechting van handelingen die te maken hebben met (verboden) drugsbezit en drugshandel. Op grond van deze wet geldt een verbod op het bereiden, bewerken, verwerken, verkopen, afleveren, verstrekken, vervoeren of aanwezig hebben van middelen die genoemd worden op de zogeheten lijst I (harddrugs) en lijst II (softdrugs). Voorbeelden van de hier bedoelde stoffen zijn cocaïne, heroïne, methadon, morfine, opium en hennep. De Opiumwet maakt onderscheid tussen misdrijven en overtredingen. De genoemde aantallen in tabel 3.9 hebben uitsluitend betrekking op misdrijven.

Het totaal aantal geregistreeerde drugsmisdrijven is volgens het CBS in de periode 2019-2022 gedaald van bijna 15.000 tot ruim 12.000 misdrijven. Die daling komt met name doordat het aantal softdrugsmisdrijven in die periode ieder jaar steeds verder afnam. Het aantal harddrugsmisdrijven lag in 2022 juist hoger dan in 2020 en 2021 (maar wel lager dan in 2019), wat naar verwachting te maken heeft met de Coronapandemie in de jaren 2020 en 2021.

Tabel 3.9 **Geregistreeerde drugsmisdrijven in 2019-2022**

	2019	2020	2021 ^a	2022 ^a
Drugsmisdrijven harddrugs	7.820	6.960	6.530	7.295
Drugsmisdrijven softdrugs	6.690	6.160	5.535	4.715
Drugsmisdrijven (overig)	195	165	135	190
Totaal	14.700	13.285	12.205	12.200

a Voor 2021 en 2022 gaat het om voorlopige resultaten.

Bron: CBS Statline. Geraadpleegd op 2-11-2023.

In diverse onderzoeken wordt Nederland aangemerkt als grote producent en handelaar van diverse soorten drugs. Volgens het *Bureau of International Narcotics and Law Enforcement Affairs* van het Amerikaanse ministerie van Buitenlandse Zaken is Nederland een belangrijk land in de Europese en mondiale illegale drugsindustrie vanwege de 'historisch lakse' handhaving van drugsgerelateerde delicten, relatief lichte straffen en haar positie als doorvoerland en digitale toegangspoort voor Europese drugsgebruikers en -leveranciers. Nederland is ook de thuisbasis van een groeiende *pool* van specialisten met diepgaande expertise in de productie van illegale chemicaliën, evenals van een toenemend aantal exploitanten die criminele marketing- en distributiebedrijven bouwen/beheren op illegale *darkweb*-technologieplatforms. Volgens het *Bureau of International Narcotics and Law Enforcement Affairs* biedt Nederland onderdak aan een groot aantal criminele ondernemingen en actoren die zich

met behulp van *online* technologie, zoals het gebruik van berichtenverkeer met *end-to-end* encryptie, bezighouden met drugshandel. Nederland blijft een belangrijke locatie voor de wereldwijde productie en distributie van synthetische drugs, waaronder meerdere stimulerende middelen van het amfetamine-type (US Department of State, 2022).

In *The World Factbook* van de Amerikaanse *Central Intelligence Agency* (CIA) wordt Nederland in 2023 omschreven als een belangrijk doorvoerknooppunt voor illegale stoffen, met name cocaïne uit Zuid- en Midden-Amerika en methamfetamine uit Mexico. De zeehavens van Nederland dienen als belangrijke doorvoerknooppunten voor illegale drugs, met name cocaïne uit Zuid-Amerika. De haven van Rotterdam, de grootste haven van Europa, dient als belangrijk kanaal tussen leveranciers van verdovende middelen en Europese consumenten.⁷⁶

Mensenhandel en mensensmokkel

In artikel 273f WvSr is mensenhandel strafbaar gesteld. Menschenhandel heeft onder meer betrekking op het werven, vervoeren of opnemen en huisvesten van mensen met gebruik van dwang, waarbij de uitbuiting van een persoon het doel is van de mensenhandelaar. Er zijn verschillende vormen van mensenhandel:⁷⁷

- arbeidsuitbuiting: als iemand werkt en de inkomsten (gedeeltelijk) moet afdragen en/of in mensonterende omstandigheden moet werken.
- seksuele uitbuiting: als iemand gedwongen wordt om seks te hebben tegen betaling van geld, kleding of eten en dat moet afdragen aan de uitbouter.
- criminele uitbuiting: als iemand gedwongen wordt om te bedelen, stelen of andere criminele activiteiten uit te voeren en de buit moet afdragen aan de uitbouter.
- gedwongen orgaanverwijdering: hierbij wordt iemand gedwongen om zijn of haar organen af te staan.

Het aantal slachtoffers van mensenhandel dat gemeld wordt bij het Coördinatiecentrum tegen Menschenhandel (CoMensha), laat over de afgelopen jaren een dalende trend zien. In 2021 waren er circa 800 meldingen, terwijl er in 2019 nog ongeveer 1.400 meldingen waren. In 2021 was arbeidsuitbuiting de meest gemelde vorm van mensenhandel, gevolgd door grensoverschrijdende en binnenlandse seksuele uitbuiting (Nationaal Rapporteur Menschenhandel en Seksueel Geweld tegen Kinderen, 2022a). Zoals bij alle vormen van criminaliteit blijft ook bij mensenhandel een groot deel verborgen. Dit *'dark number'* komt niet terug in de registratiecijfers. Om een beter zicht te krijgen op de werkelijke omvang is in 2021 op basis van de CoMensha-registratie een *dark number*-schatting uitgevoerd van het aantal slachtoffers van mensenhandel in Nederland. Voor 2019 kwam de schatting uit op ongeveer 5.000 slachtoffers (Van Dijk et al., 2021).

Mensensmokkel betreft het bieden van hulp en transport aan mensen met als doel hen de grens over te smokkelen. Mensensmokkelaars smokkelen voor veel geld migranten Nederland of de EU binnen. Daarbij komt vaak het leven of de gezondheid van de migranten in het geding, maar in tegenstelling tot mensenhandel is bij mensensmokkel uitbuiting geen primair doel.⁷⁸ Mensensmokkel en mensenhandel kunnen wel in

⁷⁶ [Netherlands - The World Factbook \(cia.gov\)](#).

⁷⁷ [Bestrijden van mensenhandel | Menschenhandel en mensensmokkel | Rijksoverheid.nl](#).

⁷⁸ [Bestrijden van mensensmokkel | Menschenhandel en mensensmokkel | Rijksoverheid.nl](#).

combinatie met elkaar voorkomen. Zo komt mensensmokkel vaak voor bij grensoverschrijdende seksuele uitbuiting en arbeidsuitbuiting.⁷⁹

In 2022 lag het aantal geregistreerde misdrijven met betrekking tot mensenhandel en mensensmokkel⁸⁰ op 835 misdrijven. Dit is een lichte stijging ten opzichte van de jaren 2020 en 2021, maar in 2019 lag dit aantal een stuk hoger (1.360 misdrijven). Tabel 3.10 geeft dit weer.

Tabel 3.10 Geregistreerde mensenhandel en mensensmokkel in 2019-2022

	2019	2020	2021 ^a	2022 ^a
Mensenhandel en mensensmokkel	1.360	765	800	835

a Voor 2021 en 2022 gaat het om voorlopige resultaten.

Bron: CBS Statline. Geraadpleegd op 2-11-2023.

Wapenhandel en wapensmokkel

Volgens Ferwerda et al. (2020) komen illegale vuurwapens in Nederland in de regel uit het buitenland. Als 'bronlanden' voor de illegale vuurwapens in Nederland noemt dit rapport onder meer de voormalige Sovjet-Unie, Bosnië en Herzegovina, Kroatië, Servië en landen uit Noord-Afrika. Illegale vuurwapenhandel is één van de nevenactiviteiten van de handel in drugs. Daarbij wordt de opbrengst van de illegale wapenhandel benut voor het aankopen van drugs, die vervolgens in het buitenland tegen relatief hoge prijzen worden verkocht (Bruinsma & Spapens, 2018). Een relatief kleine groep handelaars is betrokken bij de smokkel van illegale vuurwapens. Deze maakt gebruik van leveranciers uit hun buitenlandse contactenkring (familie, etnische gemeenschappen). Eenmaal in Nederland zijn verschillende 'partijen' betrokken bij de tussenhandel van de wapens, zoals woonwagenbewoners, leden van *Outlaw Motorcycle Gangs* en (doorgegroeide) criminele jeugdgroepen (voornamelijk van Antilliaanse en voormalig-Joegoslavische origine) (Boerman et al., 2017).

Volgens het CBS lag het aantal geregistreerde vuurwapenmisdrijven in 2022 op ruim 7.000. De afgelopen jaren is het aantal vuurwapenmisdrijven steeds iets verder toegenomen (zie tabel 3.11). Bij 'vuurwapenmisdrijven' gaat het bij het CBS om misdrijven zoals omschreven in artikel 55 van de Wet wapens en munitie die de opsporing, vervolging en berechting regelt van handelingen die te maken hebben met (verboden) wapenbezit en wapenhandel. Welk aandeel van de vuurwapenmisdrijven betrekking heeft op wapenhandel/-smokkel – de criminaliteitsvorm waarvan de opbrengsten gebruikt kunnen worden voor terrorismefinanciering – kan op basis van de CBS-data niet worden vastgesteld.

Tabel 3.11 Geregistreerde vuurwapenmisdrijven in 2019-2022

	2019	2020	2021 ^a	2022 ^a
Vuurwapenmisdrijven	6.580	6.820	7.005	7.105

a Voor 2021 en 2022 gaat het om voorlopige resultaten.

Bron: CBS Statline. Geraadpleegd op 2-11-2023.

⁷⁹ Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen (2022b).

⁸⁰ Dit betreft misdrijven omschreven in artikel 197a en artikel 273f van het WvSr. Hoewel artikel 197a WvSr een misdrijf tegen het openbaar gezag is, wordt het door het CBS meegeteld omdat in de politieregistratie het onderscheid tussen mensenhandel en mensensmokkel niet goed te maken is.

Box 3.5 Relatie criminologische kenmerken met terrorismefinanciering

In Nederland wordt een breed palet aan misdrijven gepleegd, waarvan de criminele opbrengsten gebruikt kunnen worden voor de financiering van terrorisme. Het gaat om vermogensmisdrijven waaronder vormen van fraude maar ook diefstal/verduistering en inbraak, drugsmisdrijven, vuurwapenmisdrijven, en misdrijven met betrekking tot mensenhandel en mensensmokkel.

3.6 Terrorisme en terrorismefinanciering

Terrorisme

De laatste keer dat in Nederland een terroristische aanslag werd gepleegd met dodelijke afloop was in 2019. In maart van dat jaar vond een aanslag plaats in een tram in Utrecht met vier dodelijke en twee zwaargewonde slachtoffers.⁸¹ In 2020 is de man veroordeeld tot een levenslange gevangenisstraf voor de schietpartij met terroristisch oogmerk. Hij was schuldig bevonden aan moord op vier mensen, poging tot moord op drie mensen en bedreiging met een terroristisch misdrijf van zeventien mensen.⁸² Hoewel er sindsdien geen terroristische aanslag heeft plaatsgevonden in ons land, is er nog steeds sprake van een terroristische dreiging. De NCTV heeft in december 2023 het dreigingsniveau in Nederland vastgesteld op niveau vier van vijf, wat betekent dat er een reële kans op een aanslag in Nederland is (NCTV, 2023b).

Volgens de AIVD (2023) en NCTV (2023b) vormt het jihadisme nog steeds de belangrijkste terroristische dreiging tegen Nederland. De overgrote meerderheid van meldingen en *leads* die de AIVD (2023) krijgt, gaat nog altijd over (mogelijk) jihadisme. Volgens de NCTV (2023b) neemt de terroristische dreiging vanuit jihadistische hoek toe. Daarnaast komt er een geweldsdreiging voort vanuit de soms zeer jonge personen die actief zijn binnen een rechtsextremistisch *online* milieu.

Hieronder wordt nader ingegaan op de terroristische dreigingen vanuit jihadistische en rechts-extremistische hoek die volgens de NCTV in december 2023 bestaan.

Terroristische dreiging vanuit jihadistische hoek

Sinds oktober 2023 woedt een oorlog tussen Israël en Hamas. Hamas bestuurt sinds 2007 de Gaza-strook. Volgens de NCTV heeft dit een polariserend effect op delen van de Nederlandse samenleving. Het is voorstelbaar dat de daaruit voortvloeiende spanningen leiden tot geweld tegen Joodse of islamitische instellingen. Ook proberen jihadistische groeperingen volgens de NCTV de Gaza-oorlog te gebruiken om sympathisanten aan te sporen aanslagen te plegen tegen het Westen. De NCTV geeft verder aan dat koranschendingen door extreemrechtse en anti-islamactivisten sinds begin 2023 in Zweden, Denemarken en in mindere mate Nederland de jihadistische dreiging richting Europa verhogen. Terroristische organisaties als ISIS en Al Qa'ida roepen op om uit wraak aanslagen te plegen in deze landen. Door de ontwikkelingen rond de oorlog in Gaza en koranschendingen kunnen volgens de NCTV enkelingen of kleine groepen binnen de jihadistische beweging eerder geneigd zijn om over te gaan tot geweld. Ook hebben deze gebeurtenissen een mobiliserende werking voor Nederlandse jihadisten en radicaalislamitische personen buiten de jihadistische beweging. De NCTV (2023b) verwacht niet dat deze verhoogde dreiging snel afneemt.

⁸¹ [GTI-2020-web-1.pdf \(visionofhumanity.org\)](#).

⁸² [Levenslang voor schietpartij in tram op 24 Oktoberplein Utrecht | Nieuws | Rechtspraak](#).

Box 3.6 Jihadistische beweging^a

Volgens de NCTV is het beeld van de Nederlandse jihadistische beweging, bestaande uit ongeveer 500 personen, al enkele jaren onveranderd:

- in verschillende steden van Nederland bevindt zich een aantal kleinere of grotere netwerken dat het jihadistisch gedachtegoed aanhangt;
- tussen de netwerken zijn er contacten, vindt uitwisseling van ideeën plaats en zoekt men elkaar;
- de beweging is ideologisch versnipperd en sociaal gefragmenteerd waardoor ze er niet in slaagt om effectief te opereren en haar invloed te vergroten.

a NCTV (2023b).

Ook is er volgens de NCTV een terroristische dreiging vanuit jihadistische hoek van personen en transnationale netwerken die zijn geïnspireerd of worden aangestuurd door Islamitische Staat in Syrië en Irak (ISIS) en haar Afghaanse afdeling, Islamitische Staat Khorasan Provincie (ISKP). De dreiging voor het Westen wordt vooral gevormd door relatief autonome, transnationale netwerken die zijn verbonden aan ISKP. De NCTV (2023b) geeft aan dat ISKP via *online* berichten moslims in het Westen oproept om aanslagen te plegen en dat personen die in Europa zijn geradicaliseerd, contact zoeken met ISIS-netwerken buiten Europa voor het uitvoeren van een aanslag.

Tot slot geeft de NCTV aan dat terugkeerders uit conflictgebieden in Syrië en Irak in theorie in Nederland een geweldsdreiging kunnen vormen vanwege hun verblijf bij jihadistische organisaties in de regio en daar opgedane training of gevechtservaring. Ook zouden ze na hun vrijlating uit detentie een impuls kunnen geven aan netwerken binnen de Nederlandse jihadistische beweging. Verder is het volgens de NCTV (2023a) voorstelbaar dat ex-gedeteneerde terrorismeveroordeelden met jihadistisch gedachtegoed in vreemdelingenbewaring proberen hun overtuigingen over te brengen op andere vreemdelingen. In het Jaarverslag 2022 geeft de AIVD (2023) echter aan dat zij bij terugkeerders en veroordeelde jihadisten die in detentie zitten op de terroristenafdeling van de Dienst Justitiële Inrichtingen (DJI), niet heeft waargenomen dat ze in 2022 een significante, dreigingsverhogende impact hadden op de jihadistische beweging in Nederland.⁸³

Terroristische dreiging vanuit rechts-extremistische hoek

De afgelopen jaren waren er in Nederland geen terroristische aanslagen vanuit de rechts-extremistische hoek. Volgens de AIVD (2023) en NCTV (2023a) is er wel sprake van een dreiging van rechts-terrorisme.

Volgens de NCTV schuilt de dreiging in de mogelijkheid dat een enkeling die is geradicaliseerd binnen het rechts-extremistische *online* milieu, overgaat tot geweld. Binnen dit milieu bevinden zich bijvoorbeeld aanhangers van het zogeheten accelerationisme, die met terroristisch geweld een rassenoorlog willen bespoedigen om het huidige politieke bestel te kunnen vervangen door een witte etnostaat. In 2023 zijn in Nederland personen uit dit *online* milieu aangehouden, op verdenking van een terroristisch misdrijf, het dreigen met een aanslag, rekrutering, haatzaaien, discriminatie en groepsbelediging. In Nederland zijn waarschijnlijk een paar honderd

⁸³ De AIVD plaatst daarbij wel een voorbehoud. De druk die de jihadistische beweging ervaart van terrorismebestrijding lijkt de beweging te verzwakken maar vergroot tegelijk het bewustzijn binnen de beweging van hoe inlichtingen- en veiligheidsdiensten en de (rest van de) strafrechtketen werken. Dit kan ertoe leiden dat activiteiten van jihadisten minder zichtbaar worden.

personen actief in dit rechtsextremistische *online* milieu, meestal minderjarigen of jongvolwassenen. *Online* delen zij berichten met een nazistische inhoud, verheerlijken geweld of roepen op tot het ontketenen van een rassenoorlog. Verder bestaat de Nederlandse rechtsextremistische *scene* volgens de NCTV uit 'klassieke neonazi's, nationaalsocialisten, *alt-right*, identitaire groepen en volksnationalisten'. Zij richten zich voornamelijk op de normalisering van hun rechtsextremistisch gedachtegoed en beschouwen geweld doorgaans als contraproductief (in ieder geval richting de buitenwereld). Zij houden zich volgens de NCTV wel uit oogpunt van 'zelfverdediging' bezig met gevechts- en survivaltrainingen en hebben interesse in wapens.

In 2022 heeft de AIVD een aantal keer een mogelijke rechts-terroristische dreiging voorkomen door die actief te verstoren, bracht de dienst over het onderwerp vijf ambtsberichten uit aan het OM en arresteerde de politie een aantal mensen op verdenking van activiteiten die aan rechts-terrorisme zijn gelinkt. Bovendien heeft de AIVD (2023) meerdere keren collega-diensten in het buitenland op de hoogte gebracht van (mogelijke) dreigingen, zodat zij actie konden ondernemen.

Terrorismedinanciering

Terrorismedinanciering in, vanuit of naar Nederland kan betrekking hebben op het verstrekken van middelen aan individuen, kleine groepen personen of organisaties. In het geval van jihadistisch terrorisme kan het bijvoorbeeld gaan om verstrekte middelen ten behoeve van activiteiten van ISIS, ISKP of Al Qa'ida en/of van individuen of groepen personen die in naam van deze organisaties een terroristische aanslag plegen of meevechten in strijdgebieden. Verder kunnen vanuit Nederland ook middelen worden verstrekt aan buitenlandse islamitische organisaties die door de EU als terroristisch zijn aangemerkt maar niet onder de noemer 'jihadisme' geschaard kunnen worden. Het gaat dan bijvoorbeeld om organisaties als Hamas en Hezbollah, een politieke partij in Libanon en militante beweging van sjiiitische moslims.⁸⁴

De bedragen die gemoeid zijn met terrorismedinanciering evenals de *tf*-methoden die gehanteerd worden, kunnen verschillen tussen enerzijds de financiering van individuen en kleine groepen personen en anderzijds de financiering van organisaties. Individen en kleine groepen hebben relatief weinig middelen nodig voor het plegen van een terroristische aanslag, en kunnen daardoor ook verhoudingsgewijs eenvoudigere financieringsmethoden aanwenden. Aan het in stand houden van terroristische organisaties zijn echter hoge kosten verbonden. De kosten omvatten onder meer de rekrutering van terroristische strijders, het plannen van terroristische daden, het verzorgen van training, levensonderhoud, reiskosten, het onderhoud van het terroristische netwerk, de aanschaf van wapens, *public relations* en propaganda. De verscheidenheid in de organisatiegraad van terroristische organisaties is van invloed op de omvang van de benodigde financiering.

Over de financiering van de (hoge) kosten van terroristische organisaties is volgens Wesseling en De Goede (2018) bekend dat voor Al Qa'ida internationale donaties belangrijk waren en dat ISIS zich voornamelijk financierde door het exploiteren van haar grondgebied (smokkel van olie en gas, diefstal en plundering van publieke goederen, verkoop van kunstschaten) en de daar woonachtige bevolking (belastingheffingen en diefstal) (Jonsson, 2015). De NCTV kennisbank terroristische organisaties vermeldt dat de militaire vleugel van Hezbollah (die op de EU-sanctielijst

⁸⁴ [Publications Office \(europa.eu\)](https://publications-office.europa.eu). De EU zie alleen de militaire vleugel van Hezbollah als terroristisch.

is geplaatst⁸⁵) bij haar fondsenwerving gebruikmaakt van wapen- en drugshandel, witwassen, fraude en vervalsing.⁸⁶ Van Hamas is bekend dat deze organisatie gebruikmaakt van cryptodiensten. Sinds 2021 zou er circa 41 miljoen dollar zijn overgemaakt naar *cryptowallets* die aan Hamas gelinkt worden.⁸⁷ Daarnaast hebben Israëlische autoriteiten in samenwerking met cryptobeurs Binance verschillende cryptoaccounts bevroren omdat ze aan Hamas konden worden gelinkt.⁸⁸ Reuters meldde in mei 2023 al dat Israël al ongeveer 190 cryptorekeningen in beslag had genomen, onder meer van Palestijnse bedrijven met een connectie met Hamas.⁸⁹ In haar periodieke updates van oktober 2022 en februari 2023 gaf de FATF (2023) het signaal af dat er bij ISIS en Al Qa'ida een verschuiving plaatsvindt van de meer traditionele financieringsmethoden naar het gebruik van cryptodiensten, bijvoorbeeld het werven van fondsen in Monero's.

Volgens De Goede (2007) zijn de kosten voor het plegen van terroristische daden beperkt, zeker in het licht van de schadeomvang die terrorisme veroorzaakt. Als hoogste worden de kosten van de 9/11 aanslagen in New York en Washington geschat, op US\$ 400.000 tot US\$ 500.000. De meeste aanslagen na 2001 lijken te zijn gefinancierd via beperkte en lokaal beschikbare middelen. Voor de aanslagen in Madrid in 2004 zijn de berekende kosten € 54.271 en voor de aanslagen in Londen in 2005 UK£ 8.000. Voor de aanslagen in Parijs in 2015 lopen de kostenberekeningen uiteen, afhankelijk van wat er in meegenomen wordt, van €30.000 tot €82.000. Een onderzoek naar de kosten van zeven aanslagen in Europa met een grote impact in de periode 2015-2017 wees uit dat deze aanslagen in de meeste gevallen zijn gefinancierd met minder dan € 10.000 (Wesseling & De Goede, 2018).

Aantal tf-zaken, tf-onderzoeken en tf-gerelateerde VT-dossiers

Sinds de vorige NRA is er één afgeronde onherroepelijke zaak met betrekking tot terrorismefinanciering volgens het OM geweest (ECLI:NL:GHDHA:2023:1268). In de periode 2020-2022 is het OM circa tien onderzoeken naar terrorismefinanciering gestart.⁹⁰ De FIOD heeft aan het WODC laten weten dat zij in deze periode in totaal zeven onderzoeken naar terrorismefinanciering heeft afgerond.

In Nederland verplicht de Wwft een groot aantal instellingen OT's te melden bij de FIU-Nederland. Deze instellingen worden ook wel aangeduid als poortwachters. Er zijn momenteel 29 verschillende soorten poortwachters in het kader van de Wwft. De FIU-Nederland geeft in haar jaaroverzichten weer hoeveel VT-dossiers (zie ook box 4.1) in 2021 en 2022 zijn opgestart op aanwijzing van terrorisme dan wel terrorismefinanciering. In 2022 was een daling zichtbaar in het aantal dossiers m.b.t. terrorismefinanciering, namelijk van 283 in 2021 naar 213 in 2022. Wel was er in die jaren sprake van een sterke toename van het aantal VT's, zo blijkt ook uit tabel 3.12.

⁸⁵ [EUR-Lex - 32023D1514 - EN - EUR-Lex \(europa.eu\)](#)

⁸⁶ [Hezbollah Military Wing \(nctv.nl\)](#).

⁸⁷ [Hamas kreeg 41 miljoen dollar in cryptomunten in aanloop naar aanval | De Standaard](#).

⁸⁸ [Israel freezes crypto accounts seeking Hamas donations, police say | Reuters](#).

⁸⁹ [Exclusive: Israel seized Binance crypto accounts to 'thwart' Islamic State, document shows | Reuters](#).

⁹⁰ Het OM heeft op 30 oktober 2023 richting het WODC aangegeven dat het om ongeveer tien gestarte tf-onderzoeken gaat, met daarbij de opmerking dat dit niet het volledige aantal onderzoeken betreft. Wat het precieze aantal gestarte tf-onderzoeken in de periode 2020-2022 is, is onbekend bij het WODC. In hoeverre deze onderzoeken betrekking hebben op de financiering van jihadistisch terrorisme, is op basis van de door het OM verstrekte informatie onbekend.

Tabel 3.12 Afgeronde dossiers die waren gestart op aanwijzing van terrorisme/terrorismedinanciering in 2021 en 2022

	2021		2022	
	Aantal dossiers	Aantal VT's	Aantal dossiers	Aantal VT's
Terrorisme(financiering) ^a	214	1.712	149	1.614
Terrorisme(financiering) + Anders ^b	69	1.492	86	3.294
Anders ^c	103	613	64	919

- a Dit zijn dossiers die gestart zijn op basis van een indicatie van terrorisme(financiering) en waarbij, na analyses van de FIU-Nederland, bleek dat deze daar inderdaad mogelijk aan gerelateerd zijn.
- b Dit zijn dossiers die gestart zijn op basis van een indicatie van terrorisme(financiering) maar waar, na analyses van de FIU-Nederland, ook een link met een mogelijk ander delict aan het licht kwam.
- c Dit zijn dossiers die gestart zijn op basis van een indicatie van terrorisme(financiering) maar waar, na analyses van de FIU-Nederland, alleen een link met een mogelijk ander delict aan het licht kwam

Bron: FIU-Nederland (2022 en 2023).

De FIU-Nederland geeft aan dat de sterke toename van het aantal VT's wordt veroorzaakt door een beperkt aantal dossiers met uitzonderlijk veel transacties. Deze complexe dossiers hadden bijvoorbeeld betrekking op internationale netwerken rondom ondergronds bankieren en een omvangrijk internationaal witwasnetwerk met daarin ook indicaties van terrorismedinanciering. Van de dossiers met indicaties van terrorismedinanciering heeft het merendeel betrekking op jihadistisch terrorisme. Op het gebied van extreemrechts en accelerationisme werden dossiers gegenereerd die hoofdzakelijk betrekking hebben op potentieel gewelddadige eenlingen en personen die mogelijk extreem rechts gedachtengoed aanhangen en betrokken bleken te zijn bij transacties m.b.t. de aankoop van (vuur)wapens.

Box 3.7 Ongebruikelijke en Verdachte Transacties^a

Op grond van de Wwft is een groot aantal instellingen verplicht OT's te melden bij de FIU-Nederland. De FIU-Nederland analyseert OT's, kan deze verdacht verklaren en stelt deze daarna beschikbaar aan de diverse (bijzondere) opsporings-, inlichtingen- en veiligheidsdiensten die de VT's kunnen gebruiken voor verschillende doeleinden:

- de VT's worden, al dan niet gebundeld in dossiers, gebruikt als (onderdeel van) startinformatie voor een opsporingsonderzoek;
- de VT's kunnen direct onderdeel uitmaken van het bewijs in een strafzaak;
- de VT's worden gebruikt als sturingsinformatie voor de diverse (bijzondere) opsporings-, inlichtingen- en veiligheidsdiensten;
- indien het OM strafrechtelijke interventies niet opportuun acht en de transacties ter beschikking stelt aan andere overheidsdiensten, kunnen de VT's een bijdrage leveren aan een ander type interventie, bijvoorbeeld bestuursrechtelijk of fiscaal.

De FIU-Nederland werkt met VT-dossiers omdat niet alle individuele transacties even informatief zijn als ze zonder context of onderling verband worden bekeken. Een dossier is een samenhangend geheel van informatie dat volgens de FIU-Nederland van belang kan zijn voor de diverse (bijzondere) opsporings-, inlichtingen- en veiligheidsdiensten. Dossiers geven zicht op witwasconstructies, criminele of terroristische netwerken, terrorismedinanciering of andere criminele activiteiten zoals fraude of uitbuiting. Een dossier kan één transactie bevatten, maar ook duizenden.

- a De informatie in deze subparagraaf komt uit: FIU-Nederland (2023).

3.7 Tot slot

In dit contexthoofdstuk is ingegaan op een aantal specifieke kenmerken van Nederland die in relatie kunnen staan met de prevalentie van terrorismefinanciering, de potentiële impact daarvan en de keuzes van personen voor de door hen in te zetten financieringsmethoden en te gebruiken financieringsbronnen. Het betreft geografische, demografische, religieuze, sociaal-culturele, politieke, economische en criminologische kenmerken die veelal vaststaan en via beleidsmaatregelen niet of slechts beperkt en/of op de langere termijn beïnvloedbaar zijn.

Volgens de AIVD en de NCTV is de internationale jihadistische beweging één van de belangrijkste terroristische dreigingen tegen Nederland. Jihadisten claimen de islam om hun overtuigingen en manier van leven met geweld op te leggen aan anderen. Naar schatting hangen in Nederland zo'n 500 mannen en vrouwen het jihadistisch gedachtegoed aan. Vanwege deze relatie tussen de islam, terrorisme en de financiering daarvan is ingegaan op enkele religieuze kenmerken van Nederland. Circa één op de twintig Nederlanders is islamitisch en daarvan is één op de vijf dermate religieus dat zij ten minste eenmaal per week de moskee bezoeken. Ten tijde van de vorige NRA Terrorismefinanciering meldde de AIVD dat er verhoudingsgewijs veel Nederlandse jihadisten van onder meer Marokkaanse en Turkse afkomst waren. Ongeveer één op de zeven Nederlanders heeft een niet-westerse migratieachtergrond, waarvan een groot deel een Turkse of Marokkaanse afkomst heeft. Na de 9/11 aanslagen en andere aanslagen in Europa is in Nederland de tolerantie en het gedogen ten opzichte van moslims afgenomen. Enerzijds kan deze verminderde tolerante houding leiden tot rechtsextremistische acties – en in zijn uiterste vorm terroristische daden – gericht op moslims. Anderzijds kan de verminderde tolerante houding ten opzichte van moslims aanleiding zijn voor jihadisten om terroristische activiteiten in ons land te plegen.

Nederland kenmerkt zich door een grote en internationaal georiënteerde financiële sector. Personen, groepen personen of organisaties die terrorisme financieren, kunnen op verschillende manieren gebruikmaken van het financiële stelsel in Nederland. Geldtransacties kunnen contant of op girale wijze via vergunde banken of betaaldienstverleners (geldtransactiekantoren of internet betaaldiensten) plaatsvinden. Ook crypto's bieden mogelijkheden voor terrorismefinanciering. Het zonder grenscontroles reizen van personen in de Schengenzone en vrij verkeer van personen, goederen, diensten en kapitaal tussen de EER-landen maken verhulling van een criminele oorsprong van vermogen mogelijk, omdat dit het volgen van de *paper trail* van transacties bemoeilijkt dan wel onmogelijk maakt. Ook maakt het fysieke verplaatsing over land van contant geld en grootwaardeproducten zonder grenscontroles binnen de EER mogelijk.

Het feit dat Nederland een open, op handel gerichte economie heeft en één van de grootste exporteurs ter wereld is, kan van invloed zijn op de prevalentie van terrorismefinanciering via fysieke verplaatsing van contant geld of grootwaardeproducten binnen, via, vanuit of naar Nederland. De toegangshavens tot Nederland kunnen worden gebruikt bij de import en export van legale goederen en illegale goederen als drugs. In Nederland is sprake van een breed palet aan misdrijven, waarvan de criminele opbrengsten gebruikt kunnen worden voor de financiering van terrorisme. Het gaat om vermogensmisdrijven waaronder vormen van fraude maar ook diefstal/verduistering en inbraak, drugsmisdrijven,

vuurwapenmisdrijven, misdrijven met betrekking tot mensenhandel en mensensmokkel en cybercriminaliteit.

Tot slot is er de afgelopen jaren sprake van een versplintering in de Nederlandse politiek die gepaard gaat met verslechterde omgangsvormen in het parlement, waarin polarisatie, extreme uitingen en verharding in politieke debatten in toenemende mate als problematisch worden gezien. De gevolgen van deze polarisatie werken door in de Nederlandse samenleving. Eind 2022 maakte circa drie kwart van de Nederlandse bevolking zich zorgen over toenemende tegenstellingen en meningsverschillen tussen burgers met verschillende politieke opvattingen. Deze toenemende onenigheid kan extremisme aanwakkeren. Volgens de AIVD kan extremisme in zijn uiterste vorm tot terrorisme leiden.

Het hoofdstuk sloot af met een toelichting op het onderscheid tussen de financiering van enerzijds terroristische individuen en kleine groepen, en anderzijds terroristische organisaties. Hierna werd een overzicht gegeven van het aantal afgeronde onherroepelijke zaken met betrekking tot terrorismefinanciering volgens het OM in de periode 2020 tot heden, het aantal FIOD-onderzoeken naar terrorismefinanciering in die periode en het aantal VT's en VT-dossiers dat de FIU-Nederland heeft geregistreerd dat gekoppeld kan worden aan terrorisme en terrorismefinanciering.

4 Grootste dreigingen terrorismefinanciering

Dit hoofdstuk geeft een nadere toelichting op de 12 dreigingen die in de tweede expertmeeting uit de longlist van 27 tf-dreigingen (zie bijlage 5) zijn geïdentificeerd als de grootste tf-dreigingen in Nederland (zie paragraaf 2.3 voor een nadere toelichting hierop). Zoals in hoofdstuk 1 al is benoemd, legt deze derde NRA Terrorismefinanciering – net als de eerdere NRA's op dit terrein – de focus op de financiering van jihadistisch terrorisme. Ook kwam in hoofdstuk 1 aan bod dat het bij terrorismefinanciering om meer kan gaan dan alleen het verwerven van financiële middelen ten behoeve van terrorismefinanciering en het daadwerkelijk verstrekken van financiële middelen ten behoeve van terrorisme. De grootste tf-dreigingen die in dit hoofdstuk worden beschreven, betreffen echter uitsluitend financieringsmethoden en -bronnen, omdat tf-experts alleen deze typen dreigingen noemden in de FANO-enquête, interviews en expertmeetings. Tabel 4.1 geeft een overzicht van de 12 grootste tf-dreigingen. De tf-dreigingen kunnen zich zelfstandig voordoen maar kunnen ook elementen vormen waarmee tf-constructies worden opgebouwd.

Tabel 4.1 De 12 grootste tf-dreigingen in Nederland

Dreiging
Financiering via girale of contante transacties bij vergunde banken
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren
Financiering via internetbetaaldiensten (<i>Payment Service Providers</i>)
Financiering via aanbieders van cryptodiensten
Financiering via onvergunde betaaldienstverleners en hawala-bankieren
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland
Financiering met legaal verkregen eigen middelen
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media
Financiering met middelen verkregen via horizontale/verticale fraude
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude

Dit hoofdstuk beschrijft de aard en mechanismen van deze dreigingen, mede aan de hand van recente casuïstiek en – voor zover beschikbaar – relevante kwantitatieve data. De dreigingen worden zoveel mogelijk per paragraaf afzonderlijk besproken.⁹¹ Bij de beschrijvingen is gebruikgemaakt van openbare data van de FIU-Nederland en het Centraal Bureau Fondsenwerving (CBF), een onafhankelijke stichting die toezicht houdt op de inzameling van geld voor goede doelen, en door de FIOD en Justis/TRACK verstrekte data. Voor deze grootste 12 tf-dreigingen hebben experts aan de hand van

⁹¹ Om dubbelingen in de tekst te voorkomen worden in één paragraaf twee dreigingen besproken die betrekking hebben op het zelfde terrein. Dit betreft financiering met middelen verkregen via horizontale/verticale fraude en financiering met middelen verkregen via andere criminaliteitsvorm dan fraude (in paragraaf 4.11).

een MCA (zie paragraaf 2.3) de potentiële impact bepaald. Met het resultaat van deze analyse wordt het hoofdstuk afgesloten.

4.1 Girale en contante transacties bij vergunde banken

In tegenstelling tot de vorige NRA op het terrein van terrorismefinanciering is de financiering van terrorisme via vergunde banken in Nederland in deze NRA aangemerkt als één van de grootste dreigingen in Nederland. Financiers van terrorisme kunnen gebruikmaken van het bancaire stelsel in Nederland. Volgens deze tf-methode verstrekt persoon A via een girale of contante transactie een geldbedrag aan persoon/organisatie B die het geld gebruikt ten behoeve van terrorisme.

Onduidelijkheid over de bestemming van (overgemaakt) geld en het feit dat het bij de financiering van terrorisme tot op heden vaak om kleine geldbedragen gaat (zie ook hoofdstuk 3), maken het voor banken lastig om transacties op voorhand aan terrorismefinanciering te relateren. Dit wordt extra bemoeilijkt wanneer de ontvangende partij het geld contant opneemt en vervolgens besteedt aan de financiering van terrorisme. Wanneer geldbedragen worden overgemaakt naar personen/organisaties die op een (inter)nationale sanctielijst terrorisme staan en/of gevestigd zijn in een land dat op de lijst van Wwft-hoogrisicolanden staat⁹², is het voor een bank eenvoudiger om een OT vast te stellen en te melden aan de FIU-Nederland. Om op voorhand een transactie als ongebruikelijk aan te merken en te relateren aan terrorismefinanciering, moeten banken – naast (inter)nationale sanctielijsten en een lijst van hoog risicolanden – kunnen beschikken over aanvullende informatie, bijvoorbeeld van inlichtingen- en opsporingsdiensten of mediabronnen. Achteraf – nadat een terroristische aanslag heeft plaatsgevonden – is het voor banken overigens wel mogelijk de transacties van een verdachte analyseren, waarmee bijvoorbeeld inzichtelijk wordt dat deze bepaalde goederen heeft aangeschaft die gebruikt zijn voor het plegen van de terroristische daad.

De FIOD heeft in de periode 2020-2022 zeven tf-onderzoeken afgerond, waarvan er drie (ook) op de tf-dreiging 'financiering via girale of contante transacties bij vergunde banken' betrekking hadden.

4.2 Laagdrempelige mogelijkheden om buitenlandse rekeningen te openen

Een andere nieuwe tf-dreiging die niet in de vorige NRA Terrorismefinanciering naar voren kwam als één van de grootste dreigingen, is de financiering van terrorisme via laagdrempelige mogelijkheden om buitenlandse rekeningen te openen. Het gaat in deze NRA om bankrekeningen bij banken die – omdat ze gevestigd zijn in het buitenland – een buitenlandse IBAN⁹³ en bankvergunning hebben en daarmee niet onder de reikwijdte van de Wwft en DNB-toezicht vallen – en vanuit het buitenland bancaire diensten aan Nederlandse burgers en/of bedrijven verlenen.⁹⁴ Naast de reguliere mogelijkheden voor een inwoner van Nederland om een bankrekening bij een bank in het buitenland te openen, ontstonden de afgelopen jaren

⁹² [Europese-Commissie-actualiseert-Wwft-hoogrisico-landen-per-16-maart-2023.pdf \(bureaufu.nl\)](#).

⁹³ International Bank Account Number.

⁹⁴ Het gaat dus niet om buitenlandse banken met een vestiging in Nederland die vanuit ons land hun diensten aanbieden op basis van een vergunning van DNB.

steeds meer laagdrempelige mogelijkheden om een buitenlandse bankrekening te openen. Bij een aantal van die buitenlandse banken (zonder vestiging in Nederland) kan eenvoudig *online* een bankrekening worden geopend. De mogelijkheid bestaat dat de poortwachtersrol door een buitenlandse bank, die niet onder de reikwijdte valt van de Wwft en DNB-toezicht maar onder de buitenlandse witwas- en terrorismefinancieringwetgeving, minder diepgaand wordt uitgevoerd dan de eisen die DNB stelt aan in Nederland vergunde banken. Naar verwachting geldt dit vooral voor buitenlandse banken die niet in de EU zijn gevestigd. Mogelijk verricht de buitenlandse bank minder grondig cliëntonderzoek, accepteert deze sneller risicovolle klanten en meldt deze VT's of activiteiten⁹⁵ slechts in beperkte mate aan de FIU in het betreffende land. Bovendien bestaat het risico dat deze VT's of activiteiten – zelfs als deze in het betreffende land zijn gemeld – minder snel en/of goed worden doorgegeven aan de FIU-Nederland, waarmee VT's minder snel/goed beschikbaar komen voor Nederlandse opsporingsdiensten.

Personen kunnen in Nederland één of meerdere buitenlandse rekeningen openen, die zij in principe ook voor de financiering van terrorisme kunnen gebruiken. Het internationale element van deze tf-methode maakt het voor Nederlandse banken erg lastig om dit soort transacties te monitoren, wat opsporingsdiensten hindert om personen die terrorisme financieren, op te sporen. Door stapeling van buitenlandse rekeningen – eventueel in combinatie met minder transparante Nederlandse rechtsvormen (zie ook paragraaf 4.3) – kan iemand een tf-constructie steeds ondoorzichtiger maken en de pakkans steeds verder minimaliseren.

De FIU-Nederland maakt in het Jaaroverzicht 2022 melding van 'virtuele IBAN's', volledig digitale alternatieven voor traditionele rekeningen. Genoemd wordt dat zij nieuwe manieren van betalen, waaronder virtuele IBAN's, in 2022 meerdere malen tegenkwam bij kwaadwillenden. Deze werkwijze kwam naar voren in dossiers met betrekking tot zowel jihadistische als extreemrechtse groeperingen. In bepaalde dossiers kwam terug dat Nederlandse ingezetenen één of meerdere virtuele IBAN's openen in een andere Europese lidstaat, die gebruikt werden ter verhulling, om uit het zicht te blijven van de opsporingsdiensten. Ook kwam het voor dat niet-ingezetenen één of meerdere virtuele IBAN's in Nederland openden om dezelfde reden. De FIU-Nederland geeft aan dat virtuele IBAN's gereguleerde producten zijn die in de meeste gevallen een legitiem doel kennen. Het gemak waarmee ze geopend kunnen worden in verschillende landen, zorgt echter voor situaties waarbij de geldstroom onoverzichtelijk wordt. Volgens de FIU-Nederland wordt dit deels ondervangen door de afspraak tussen Europese FIU's om transacties waarbij (recht)personen uit een andere lidstaat zijn betrokken, actief te delen met de FIU van die betreffende lidstaat. Lastiger ligt dit wanneer het gaat om het delen van informatie over transacties via buitenlandse FIU's waarmee geen afspraken gelden. In het geval dat de FIU-Nederland extra informatie wil ontvangen, bijvoorbeeld van een buitenlandse poortwachter, vormt dit echter een tijdrovend proces. Ook kan het een zeer complex proces zijn, bijvoorbeeld wanneer een virtuele IBAN gekoppeld wordt aan andere innovatieve diensten zoals cryptoplatformen (FIU-Nederland, 2023).

⁹⁵ Hier is gekozen voor de aanduiding 'verdachte transacties of activiteiten'. In de meeste Europese landen hebben poortwachters, anders dan in Nederland, de verplichting verdachte transacties of verdachte activiteiten te melden. In Nederland melden OT's. Zie: Tavares et al (2010).

Van de afgeronde FIOD-onderzoeken in de periode 2020-2022 had er geen betrekking op de tf-dreiging 'financiering via laagdrempelige (*online*) mogelijkheden om buitenlandse bankrekening te openen'.

4.3 Internet betaaldiensten (PSP's)

Een dreiging die door tf-experts gezien wordt als één van de grootste dreigingen (en die ook al in de vorige NRA naar voren kwam, maar wel met een enigszins andere formulering⁹⁶), is de financiering van terrorisme via internet betaaldiensten (PSP's). Kort samengevat gaat het bij deze dreiging erom dat webwinkeliers op deze manier klantbetalingen, bijvoorbeeld voor de aankoop van vuurwapens of precursoren voor explosieven, via diverse betaalmethoden accepteren, waarbij die betalingen op bankrekeningen van de aan de PSP gelieerde stichting derdengelden terechtkomen en waarbij PSP's vanaf die rekeningen de betalingen in *batches* uitbetaalt aan de webwinkeliers. De PSP-dienstverlening is voor personen die terrorisme financieren, interessant omdat banken alleen de grote *batch*-betalingen zien en geen inzicht hebben in de onderliggende individuele transacties. Daardoor is onduidelijk welke klanten met welk doel de transacties verrichten. Voor opsporingsinstanties bevatten de grote *batch*-betalingen niet de detailinformatie die vaak nodig is voor opsporingsonderzoek.⁹⁷

De FIOD heeft in de periode 2020-2022 drie tf-onderzoeken afgerond die (ook) betrekking hadden op de tf-dreiging 'financiering via internet betaaldiensten (PSP's)'.

4.4 Girale en/of contante transacties bij vergunde geldtransactiekantoren

In tegenstelling tot de vorige NRA op het terrein van terrorismefinanciering is de financiering van terrorisme via vergunde geldtransactiekantoren in deze NRA aangemerkt als één van de grootste tf-dreigingen. Geldtransactiekantoren houden zich bezig met de bedrijfsmatige uitvoering van geldtransacties of het verrichten van werkzaamheden gericht op de totstandkoming van zulke transacties (zie ook hoofdstuk 3). Personen die terrorisme financieren, kunnen de dienstverlening van geldtransactiekantoren op verschillende manieren gebruiken. Net als bij transacties via vergunde banken verstrekt persoon A volgens deze tf-methode via een girale transactie dan wel een contante transactie een geldbedrag aan persoon/organisatie B die het geld gebruikt ten behoeve van terrorisme. Voor geldtransactiekantoren is het – net als voor banken (zie eerder) – vanwege onduidelijkheid over de bestemming van (overgemaakt) geld en het feit dat het bij de financiering van terrorisme tot op heden vaak om kleine geldbedragen gaat, lastig om transacties op voorhand te relateren aan terrorismefinanciering. Een extra risicofactor bij geldtransactiekantoren is dat in ons land veel betaaldienstagenten⁹⁸ van vergunde geldtransactiekantoren actief zijn,

⁹⁶ In de tweede NRA Terrorismefinanciering ging het om de volgende formulering van de dreiging: 'Verwerving en/of financiering via *online* platforms/*payment service providers*'.

⁹⁷ [Kwetsbaarheden voor witwassen bij PSP's - AMLC](#). Dit artikel gaat alleen in op witwassen, maar een deel van de informatie geldt in feite ook voor terrorismefinanciering.

⁹⁸ Betaaldienstagenten van geldtransactiekantoren moeten genotificeerd zijn bij DNB door het geldtransactiekantoor waarvan zij agent zijn (en dat geldtransactiekantoor moet weer een DNB- of EU-vergunning hebben). Deze betaaldienstagenten staan onder toezicht van DNB, die daar ter plekke onderzoek kan doen.

bijvoorbeeld in belwinkels en tabakszaken. Omdat deze winkels geen financiële instellingen zijn, kan het personeel minder affiniteit en bekendheid hebben met tf-risico's dan het personeel van reguliere geldtransactiekantoren.

Van de afgeronde FIOD-onderzoeken in de periode 2020-2022 had er geen betrekking op de tf-dreiging 'financiering via girale of contante transacties bij vergunde geldtransactiekantoren'.

Deze tf-dreiging betreft vergunde geldtransactiekantoren, maar er zijn in Nederland ook (groepen) personen actief die op onvergunde wijze de diensten van geldtransactiekantoren aanbieden. Deze worden in deze NRA geschaard onder de noemer 'ondergronds bankieren' (zie verderop in deze paragraaf).

4.5 Aanbieders van cryptodiensten

Een dreiging die ook al in de vorige NRA Terrorismefinanciering naar voren kwam als één van de grootste tf-dreigingen (maar wel met een enigszins andere formulering⁹⁹), heeft betrekking op crypto's. In hoofdstuk 3 kwam al aan bod dat er momenteel 36 bij DNB geregistreerde aanbieders van crypto-bewaarpportemonnees en 31 geregistreerde aanbieders van crypto-wisseldiensten zijn die in Nederland hun diensten aanbieden. De tf-risico's met betrekking tot deze crypto's liggen in het feit dat zij het reguliere betaalmiddel op het *darkweb* (het anonieme en afgeschermd deel van het internet) zijn en dat deze door personen die terrorisme financieren, als betaalmiddel kunnen worden gebruikt. Door middel van een zogeheten '*crypto mixing service*' (of *bitcoin-mixer*) – een *online* dienst waarbij crypto's tegen betaling van een commissie worden opgesplitst en in andere samenstelling weer worden samengevoegd – kan de herkomst of bestemming van crypto's worden verhuuld.

Cryptodiensten die in Nederland actief zijn, dienen te beschikken over een registratie bij DNB. Naast de geregistreerde aanbieders van cryptodiensten is er in ons land een onbekend aantal aanbieders actief dat niet bij DNB is geregistreerd. Gezien het feit dat deze aanbieders niet onder de reikwijdte van de Wwft vallen, valt te verwachten dat de tf-dreiging bij deze aanbieders hoger ligt dan bij de geregistreerde aanbieders.

Van de afgeronde FIOD-onderzoeken in de periode 2020-2022 had er geen betrekking op de tf-dreiging 'financiering via aanbieders van cryptodiensten'.

4.6 Onvergunde betaaldienstverleners en hawala-bankieren

Net al in de vorige NRA Terrorismefinanciering is terrorismefinanciering via onvergunde betaaldienstverleners en hawala-bankieren één van de grootste tf-dreigingen (maar wel met een enigszins andere formulering¹⁰⁰). Ondergronds bankieren is een informeel betalingssysteem, buiten de reguliere financiële dienstverlening om en waarop geen toezicht plaatsvindt. Bij ondergronds bankieren wordt gebruikgemaakt van een systeem dat gebaseerd is op vertrouwen en

⁹⁹ In de tweede NRA Terrorismefinanciering ging het om de volgende formulering van de dreiging: 'Verwerving van, verplaatsing van en/of financiering met virtuele valuta's'.

¹⁰⁰ In de tweede NRA Terrorismefinanciering ging het om de volgende formulering van de dreiging: 'Verplaatsing via ondergronds bankieren incl. onvergunde betaaldienstverleners'.

verrekening. Net als bij reguliere banken is het systeem gebaseerd op het verrekenen van schulden en tegoeden, waardoor het mogelijk is om alle verplaatsingen van contant geld binnen de landsgrenzen te houden. In theorie kan ondergronds bankieren met legaal geld plaatsvinden, maar ook dit is op grond van de Wet op het financieel toezicht (Wft) strafbaar omdat een vergunning nodig is om te bankieren. Onder de noemer 'ondergronds bankieren' valt in deze NRA niet alleen hawala-bankieren (zie hieronder) maar ook de diensten van onvergunde betaaldienstverleners:

- Hawala-bankieren. Dit betreft een eeuwenoude traditie en kent zijn oorsprong in het Midden-Oosten en Verre Oosten. Volgens dit systeem zorgt een netwerk van bankiers ervoor dat ingelegd geld aan de ene kant van de wereld aan de andere kant van de wereld uitbetaald kan worden. Het geld wordt onderling door de bankiers verrekend, met als gevolg dat fysiek transport met contant geld slechts in beperkte mate nodig is (OM, 2019). In Nederland wordt hawala-bankieren met name door migranten gebruikt. In sommige landen is het bij gebrek aan reguliere financiële dienstverleners de enige manier om te bankieren.¹⁰¹ Normale bancaire transacties naar strijdgebieden zijn onder meer vanwege het zogenoemde de-risken door banken – waarbij voor bepaalde (typen) cliënten of regio's geen dienstverlening wordt aangeboden of de zakelijke relatie wordt verbroken – vaak niet mogelijk.¹⁰²
- Onvergunde betaaldienstverlening. Bij deze dreiging gaat het om personen of groepen die zonder vergunning van DNB de diensten van geldtransactiekantoren aanbieden.

Voor personen die terrorisme financieren, biedt ondergronds bankieren een aantal voordelen. Internationale betalingen kunnen worden gedaan zonder – in beginsel althans – dat het geld fysiek over de hele route wordt verplaatst en zonder dat van officiële kanalen (Wwft-poortwachters) gebruik wordt gemaakt. Daarmee kunnen de risico's die met fysieke verplaatsing en een girale transactie via een reguliere instelling samengaan, zoals een OT-melding bij de FIU-Nederland, worden ontlopen (Kruisbergen et al., 2012).

Vier van de zeven afgeronde FIOD-onderzoeken in de periode 2020-2022 hadden betrekking op de tf-dreiging 'financiering via onvergunde betaaldienstverleners en hawala-bankieren'. Volgens de FIU-Nederland hadden in 2022 81 VT-dossiers (bestaande uit 3.488 VT's) en in 2021 95 VT-dossiers (bestaande uit 8.173 VT's) (onder meer) betrekking op ondergronds bankieren (FIU-Nederland, 2022, 2023).¹⁰³ Hoeveel van die dossiers daadwerkelijk betrekking hebben op terrorismefinanciering (en niet op witwassen), is onduidelijk.

¹⁰¹ [Verstoring van crimineel ondergronds bankieren vraagt om internationale aanpak | Verhalen uit de praktijk | Nederland tegen georganiseerde misdaad.](#)

¹⁰² [FATF clarifies risk-based approach: case-by-case, not wholesale de-risking \(fatf-gafi.org\).](#) '...de-risking refers to the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach.'

¹⁰³ Dit betreft dossiers die gestart zijn op basis van een indicatie van de genoemde delictsvormen. Een dossier/transactie kan betrekking hebben op meerdere criminaliteitsvormen. Over het jaar 2020 is geen informatie hierover beschikbaar in het betreffende Jaaroverzicht.

Box 4.1 Terrorismedinanciering via ondergronds bankieren

In 2022 veroordeelde de rechtbank in Rotterdam een 36-jarige man tot 30 maanden cel voor onder meer het financieren van een terroristische organisatie en valsheid in geschrifte (ECLI^a:NL:RBROT:2022:7335). Twee andere verdachten werden veroordeeld tot celstraffen tot 18 maanden voor hawala-bankieren – waarbij geldbedragen zijn weggesluisd naar Syrië – waarvan de 36-jarige verdachte gebruikt heeft gemaakt (ECLI:NL:RBROT:2022:7336, ECLI:NL:RBROT:2022:7337). De rechtbank achtte bewezen dat de 36-jarige verdachte over een periode van twee jaar geld verstrekke aan een groot aantal vrouwen en kinderen in gevangenkampen in Syrië. Dit geld was in eerste instantie bedoeld voor voedsel en goederen, maar later was het bedoeld voor 'ontsnappings' van vrouwen en hun kinderen uit de kampen. De verdachte had daarbij een sturende en essentiële rol, aangezien hij opdrachten gaf welke vrouwen moesten worden opgehaald, de smokkel organiseerde en verblijflocaties regelde. Het ging om voornamelijk Nederlandse vrouwen die eerder waren uitgereisd naar Syrië, daar langere tijd verbleven en er gehuwd waren (geweest) met ISIS-strijders/-medewerkers. De verdachte had volgens de rechtbank door zijn handelen het risico genomen dat het geld op (indirecte) wijze terecht kwam bij ISIS en gebruikt werd voor terroristische doeleinden.^b In totaal zamelde de verdachte 107.000 dollar in en verstrekke hij het ingezamelde geld aan 25 Nederlandse en Belgische vrouwelijke ISIS-aanhangers in Syrië, waarvan een aantal op de nationale sanctielijst terrorisme stond (NCTV, 2022).

In 2021 veroordeelde het gerechtshof Den Haag een 43-jarige man, geboren in Syrië, tot een gevangenisstraf van 30 maanden vanwege onder meer hawala-bankieren, terrorismedinanciering, gewoontewitwassen en mensensmokkel (ECLI:NL:GHDHA:2021:2272). De verdachte runde gedurende ongeveer tien maanden feitelijk een geldwisselkantoor buiten iedere vorm van toezicht om. De provisie-gelden die de verdachte hiermee verdiende, werden door hem witgewassen. Het gerechtshof achtte bewezen dat hij hiervan een gewoonte had gemaakt. Daarnaast verstrekke de verdachte aanzienlijke geldbedragen aan zijn broer die streed voor ISIS en Jabath al-Nusra, wat door het gerechtshof gezien werd als terrorismedinanciering.^c

In 2020 deed de rechtbank Den Haag een uitspraak in een zaak waarbij sprake was van terrorismedinanciering, hawala-bankieren, witwassen en mensensmokkel (ECLI:NL:RBDHA:2020:1324). Samen met anderen voerde de verdachte gedurende zo'n tien maanden illegale geldtransacties voor anderen uit. Veelvuldig ontving hij contante geldbedragen buiten het formele geldcircuit om, die hij verplaatste en overdroeg. Voor deze activiteiten zat hij enige tijd in voorlopige hechtenis. Eenmaal in vrijheid gesteld, hervatte hij zijn illegale praktijken. De rechtbank verweet hem, dat hij geldtransacties bedrijfsmatig als betaaldienstverlener had verricht, zonder dat hij daarvoor vergunning had. Omdat de verdachte de provisie uit het hawala-bankieren opstreek en van dat geld gebruikmaakte, werd hij ook voor witwassen vervolgd. Via hawala-bankieren verzond de verdachte tweeënehalf jaar lang geldbedragen naar zijn broer in Syrië, terwijl hij wist dat zijn broer strijder was van de gewapende Jihad-strijd en zich had aangesloten bij een terroristische organisatie. Ook was de verdachte betrokken geweest bij mensensmokkel. De

rechtbank achtte de feiten bewezen en veroordeelde de man tot een gevangenisstraf van drie jaar, waarvan een jaar voorwaardelijk.^d

- a European Case Law Identifier.
- b [Tot 30 maanden cel voor illegale geldtransacties en financieren van terrorisme \(rechtspraak.nl\)](#).
- c [Veroordeling voor onder meer hawala-bankieren en financiering terrorisme \(rechtspraak.nl\)](#).
- d [Illegaal bankieren en financieren van terrorisme - FIU-Nederland](#).

4.7 Stichtingen met weinig transparantie over financiën en geen zelfregulering

De oprichting van stichtingen biedt de mogelijkheid om op een verhullende wijze en met een schijn van legitimiteit terrorisme te financieren. Het feit dat stichtingen relatief eenvoudig zijn op te richten (zie hieronder), maakt deze tf-methode aantrekkelijk voor financiers van terrorisme. Het risico van deze tf-methode ligt bij stichtingen die weinig inzicht bieden in de herkomst en bestemming van financiële middelen en geen aandacht hebben voor een vorm van zelfregulering (hierop wordt later ingegaan). In de vorige NRA op het terrein van terrorismefinanciering hadden twee van de grootste tf-dreigingen betrekking op stichtingen, namelijk 'Verwerving en/of financiering via stichtingen of andere rechtsvormen (charitatief, religieus, educatief) in Nederland' en 'Verwerving en/of financiering via stichtingen of andere rechtsvormen (charitatief, religieus, educatief) in buitenland'.

Een stichting is een rechtsvorm met rechtspersoonlijkheid die geen winstdoel maar een maatschappelijk, sociaal of ideëel doel heeft. Het geld van een stichting komt binnen via donaties, leningen, subsidies en erfenissen. Er is voor de oprichting van een stichting geen minimaal startkapitaal nodig. Wel moet een notaris een notariële akte met daarin de statuten opstellen.¹⁰⁴ De benoeming, herbenoeming en het ontslag van bestuurders van een stichting is vastgelegd in de statuten van de stichting. Wijzigingen binnen het bestuur moeten worden doorgegeven aan de Kamer van Koophandel (KvK), maar de notaris hoeft daarbij niet betrokken te worden. Volgens Justis/TRACK, dat zich baseert op cijfers van de KvK, waren er in 2022 in totaal circa 240.000 stichtingen in Nederland (tabel 4.2). Het aantal jaarlijks opgerichte stichtingen lag in de periode 2020-2022 op ongeveer 9.000-10.000, waarvan de meeste actief zijn binnen de branche 'Levensbeschouwelijke en politieke organisaties, belangen- en ideële organisaties, hobbyclubs' (in 2022 ging het om 2.842 opgerichte stichtingen in deze branche).¹⁰⁵ Bijlage 9 bevat enkele tabellen die voorgaande informatie weergeven.

Tabel 4.2 Ontwikkeling aantal stichtingen in de periode 2020-2022

	2020	2021	2022
Stichting	238.123	240.714	240.064

Bron: data voor deze NRA aangeleverd door Justis/TRACK op 18 augustus 2023.

¹⁰⁴ [De stichting | Ondernemersplein \(kvk.nl\)](#).

¹⁰⁵ Terwijl het aantal (opgerichte) stichtingen in die branche sinds 2020 gedaald is, steeg het aantal (opgerichte) stichtingen in de branche 'Financiële holdings' in die periode van 1.985 in 2020 tot 2.251 in 2022. Andere branches waarin veel (opgerichte) stichtingen actief zijn, zijn 'Financiële bemiddeling, advisering e.d.' en 'Maatschappelijke dienstverlening'.

De stichting als rechtsvorm kan gebruikt worden door personen die terrorisme willen financieren, aangezien dit hen volgens het Centrum voor Criminaliteitspreventie en Veiligheid (CCV, 2021) enkele voordelen biedt:¹⁰⁶

- een stichting kan met weinig kosten en moeite worden opgericht;
- de oprichter van de stichting hoeft maar één keer naar de notaris, waarna bestuurders zonder tussenkomst van de notaris op afstand kunnen worden gewijzigd;
- er is meestal geen verplichte verantwoording over de financiële gang van zaken, waarmee een beperktere financiële transparantie bestaat;
- er is beperkt intern toezicht.

In een onderzoek uit 2019 naar de financiële zelfredzaamheid van uitreizigers komt het gebruik van stichtingen bij terrorismefinanciering een aantal keer naar voren. Zo wordt in de studie genoemd dat een uitreiziger maandelijks € 1.000 ontving van een 'wettelijk erkende islamitische stichting uit Nederland'. Ook komt een casus naar voren waarbij een uitreiziger een dozijn zogenaamde 'goede doelen'-stichtingen heeft opgericht en hiertoe op islamitische fora geld heeft gevraagd in het kader van bijvoorbeeld een hulpactie voor Syrië, Afghanistan, weeskinderen, speelgoed, waterputten of zusters. Honderden bezoekers van deze fora gaven aan zijn oproepen gehoor en doneerden kleine bedragen van €1 tot €2, maar soms ook grotere bedragen van een paar honderd euro. In totaal haalde hij ruim €15.000 op (Soudijn, 2019).

Justis/TRACK heeft op verzoek van het WODC data aangeleverd over enkele aspecten van stichtingen in Nederland in de jaren 2020, 2021 en 2022 (zie bijlage 8). Het gaat (onder meer) om de volgende aspecten:

- het aantal oprichtingen van stichtingen per unieke bestuurder naar land van herkomst;
- het aantal stichtingen waarbij unieke bestuurders (naar land van herkomst) betrokken zijn;
- het aantal keer dat bij stichtingen een bestuurswisseling plaatsvond binnen een periode tot en met 30 dagen na de oprichting.

Uit een analyse van deze data door het WODC blijkt een aantal opvallende zaken die niet zozeer op terrorismefinanciering of andersoortige criminele activiteiten hoeven te duiden maar die wel wijzen op ongebruikelijke activiteiten:

- In de periode 2020-2022 hebben twee in Nederland gevestigde bestuurders (rechtspersonen) in totaal 51-100 stichtingen opgericht.
- Zeven in Nederland gevestigde bestuurders (natuurlijke personen) waren in de periode 2020-2022 betrokken bij in totaal 51-100 stichtingen en twee in het VK gevestigde bestuurders (natuurlijke personen) waren betrokken bij meer dan 100 stichtingen. De twee bestuurders uit het VK waren in 2020 betrokken bij in totaal 392 stichtingen (gemiddeld 196 stichtingen per bestuurder).
- 23 in Nederland gevestigde bestuurders (rechtspersonen) waren in de periode 2020-2022 betrokken bij in totaal 51-100 stichtingen en 17 in Nederland gevestigde bestuurders (rechtspersonen) waren betrokken bij meer dan 100 stichtingen.
- In de periode 2020-2022 waren er 357 bestuurswisselingen (natuurlijke personen) binnen een periode tot en met 30 dagen na de oprichting van de stichting. In verreweg de meeste gevallen (329) hadden deze betrekking op bestuurders die in

¹⁰⁶ Dit artikel gaat alleen in op witwassen, maar een deel van de informatie geldt in feite ook voor terrorismefinanciering.

Nederland waren gevestigd. Verder waren er in deze periode 44 bestuurswisselingen (rechtspersonen) binnen een periode tot en met 30 dagen na de oprichting van de stichting, die allen betrekking hadden op in Nederland gevestigde bestuurders.

Geen van de afgeronde FIOD-onderzoeken in de periode 2020-2022 had betrekking op de tf-dreiging 'financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering'.

Niet alle stichtingen in Nederland zijn weinig transparant over de herkomst en bestemming van financiële middelen en/of besteden geen aandacht aan zelfregulering. Allereerst zijn er stichtingen met de status van Algemeen Nut Beogende Instelling (ANBI). Een stichting kan een ANBI-status krijgen als minimaal 90% van haar activiteiten het algemeen belang dient, indien er geen sprake is van een winstoogmerk en wanneer deze beschikt over een beperkt eigen vermogen. Een stichting met ANBI-status is verplicht om specifieke gegevens, waaronder een financiële verantwoording, openlijk op de eigen website te publiceren. De meeste maar niet alle ANBI's kennen een stichtingsvorm (CCV, 2021). Eind januari 2022 waren er in Nederland 45.047 organisaties als ANBI geregistreerd (Bekkers et al., 2022).¹⁰⁷ Hoewel een stichting met ANBI-status in principe meer inzicht biedt in de financiën, neemt dat het risico op terrorismefinanciering niet volledig weg.

Ten tweede zijn er stichtingen met een Erkenning van het CBF. Een CBF-erkenning geldt als keurmerk voor goede doelen in Nederland die moeten voldoen aan enkele kwaliteitseisen en zich vrijwillig laten toetsen.¹⁰⁸ In 2023 waren er in totaal 641 goede doelen met een CBF-erkenning (Schulpen & Van der Plas, 2023). Box 4.2 geeft per werkgebied het aantal ANBI's dat eind 2020 actief was en het aantal daarvan dat destijds over een CBF-erkenning beschikte. Uit een enquête van Goede Doelen Nederland en het CBF (2021) onder goede doelen met een CBF-erkenning blijkt dat 20% van de responderende organisaties actief is in een hoog risicoland; bij kleine goede doelen ligt dat percentage op 9% en bij grote goede doelen gaat het om 32%. Van de responderende organisaties geeft 16% aan een verhoogd risico te lopen op terrorismefinanciering.

¹⁰⁷ Veel ANBI's zijn filantropische organisaties, maar ook alle gemeenten, provincies, waterschappen en de Staat der Nederlanden zijn van rechtswege een ANBI. Daarnaast zijn non-profit-instellingen waarvan de inkomsten geheel of vrijwel geheel uit overheidssubsidie of vergoedingen voor dienstverlening afkomstig zijn, zoals ziekenhuizen, bibliotheken, schoolbesturen, universiteiten en hogescholen, een ANBI. De ANBI-registratie bevat ook een groot aantal woningcorporaties en zorginstellingen.

¹⁰⁸ [CBF | Toezichthouder goede doelen](#).

Box 4.2 ANBI's en CBF-erkenningen

Het CBF heeft alle ANBI's naar werkgebied gecategoriseerd en geeft daarbij aan welk deel een CBF-erkenning hebben (zie tabel 4.3). Van het totaal aantal ANBI's eind 2020 hadden 625 een CBF-erkenning, waarvan de meeste actief waren binnen de werkgebieden 'internationale hulp en mensenrechten' en 'welzijn'.

Tabel 4.3 Aantal ANBI's en CBF-erkenningen naar werkgebied (in december 2020)^a

Werkgebied	Aantal ANBI	Aantal CBF erkend
Levensbeschouwing	16.583	41
Welzijn	8.228	145
Internationale hulp en mensenrechten	5.927	224
Kunst en cultuur	5.187	20
Gezondheid	4.194	93
Dieren en planten	1.098	37
Natuur en milieu	818	58
Onderwijs en wetenschap	673	6
Hergebruik	493	1
Begraafplaatsen	53	0
Totaal	43.254	625

^a Bekkers et al. (2022) verwijzen naar Microsoft Power BI, via de volgende link: [Microsoft Power BI](#).

Ten derde bestaan er enkele gedragscodes en kwaliteitsstandaarden voor een deel van de stichtingen, die ook zorgen voor een zekere mate van transparantie. In de interviews en expertmeetings zijn de volgende gedragscodes en kwaliteitsstandaarden genoemd. De mogelijkheid bestaat dat er nog meer relevante gedragscodes en kwaliteitsstandaarden bestaan.

- Voor goede doelen in ontwikkelingssamenwerking bestaan de gedragscode en ISO-9001 kwaliteitsstandaarden van Partos, de branchevereniging voor ontwikkelingssamenwerking;
- voor vermogensfondsen bestaan de Code Goed Bestuur en kwaliteitsstandaarden van Fondsen in Nederland (FIN), de branchevereniging van fondsen en foundations;
- voor kerken bestaan de gedragscode en kwaliteitsstandaarden van het Interkerkelijk Contact In Overheidszaken (CIO), een samenwerkingsverband en belangenbehartiger van 28 Christelijke kerken en twee Joodse gemeenschappen.

Naar verwachting zijn de risico's op de financiering van terrorismefinanciering het kleinst bij ANBI-stichtingen met een CBF-erkenning die voldoen aan een van de hierboven genoemde gedragscodes en kwaliteitsstandaarden. De mogelijkheid bestaat dat ook andere criteria van invloed zijn op het risico op terrorismefinanciering via stichtingen, zoals het al dan niet te maken hebben met transacties van/naar het buitenland. In de interviews en expertmeetings zijn dergelijke aanvullende criteria echter niet genoemd. Indien een stichting geen ANBI-status of CBF-erkenning heeft en niet aan een vorm van zelfregulering doet, zouden Wwft-poortwachters bij zo'n stichting nader cliëntonderzoek kunnen verrichten om een goed beeld te verkrijgen van het daadwerkelijke risiconiveau ten aanzien van terrorismefinanciering.

4.8 Fysieke verplaatsing contant geld en/of grootwaardeproducten

Om terrorisme te financieren kan contant geld fysiek worden verplaatst naar de bestemming: binnen Nederland, vanuit het buitenland naar Nederland en vanuit Nederland naar het buitenland. Deze tf-dreiging kwam ook in de vorige NRA naar voren als één van de grootste tf-dreigingen (maar wel met een enigszins andere formulering¹⁰⁹). Het verplaatsen van contant geld kan op verschillende manieren plaatsvinden, bijvoorbeeld via (al dan niet professionele) geldkoeriers of verzending per post. Behalve contant geld kunnen ook grootwaardeproducten ten behoeve van de financiering van terrorisme worden verplaatst. De betreffende grootwaardeproducten vertegenwoordigen zelf natuurlijk een waarde maar kunnen na ontvangst ook worden verkocht zodat met de opbrengsten daarvan terrorisme gefinancierd kan worden.

Verplaatsing van contant geld of grootwaardeproducten naar het buitenland kan via de Rotterdamse haven en Schiphol maar ook via kleinere zee- en luchthavens plaatsvinden. Via lucht- en zeehavens kunnen passagiers contant geld onder de meldgrens van € 10.000 meenemen of zij kunnen luxe, minder opvallende grootwaardeproducten, bijvoorbeeld een aantal zeer kostbare horloges, bij zich hebben. Binnen en buiten de EU is verplaatsing via voertuigen uiteraard ook een optie, maar, afhankelijk van de omvang van de verplaatste hoeveelheden contant geld of grootwaardeproducten en de mate waarin dit opvalt voor douaniers, brengt dit mogelijk te grote risico's met zich mee voor personen die terrorisme willen financieren.

De tf-dreiging 'financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland' kwam in twee van de zeven afgeronde FIOD-onderzoeken in de periode 2020-2022 naar voren. In het Jaaroverzicht van de FIU-Nederland staat informatie over het aantal OT's dat gemeld wordt door de Douane en het aantal VT's dat op basis daarvan is vastgesteld. In hoeverre al deze Douane-meldingen betrekking hebben op het vervoeren van contant geld en/of grootwaardeproducten, is onbekend. Ook is het niet duidelijk of deze VT's betrekking (kunnen) hebben op terrorismefinanciering of vooral op witwassen. Het aantal door de Douane gemelde OT's is de afgelopen jaren gestegen, namelijk van 3.781 in 2021 tot 4.070 in 2022. Het aantal VT's is in die periode juist sterk gedaald, namelijk van 725 in 2020 tot 218 in 2022 (FIU-Nederland, 2021, 2022, 2023).

Tabel 4.4 OT's en VT's m.b.t. Douane Nederland in 2020-2022^a

	2020	2021	2022
OT's	3.781	3.920	4.070
VT's	725	549	218

- a VT's zijn opgevraagd op doormelddatum, dat wil zeggen de datum dat een OT verdacht wordt verklaard. VT's in een bepaald jaar kunnen zodoende niet worden vergeleken met de OT's (opgevraagd op registratiedatum) in een bepaald jaar. De meldingen door de Douane werden tot en met 2020 opgesplitst in meldplicht en meldrecht. In deze tabel zijn voor 2020 de VT's bij elkaar opgeteld.

¹⁰⁹ In de tweede NRA Terrorismefinanciering ging het om de volgende formulering van de dreiging: 'Verplaatsing (fysiek) van contant geld'.

4.9 Legaal verkregen eigen middelen

Terrorisme kan met legaal verkregen eigen middelen gefinancierd worden. Deze tf-dreiging kwam in de vorige NRA op het terrein naar voren als één van de grootste dreigingen (maar wel met een enigszins andere formulering¹¹⁰). De vormen van legale inkomstenbronnen zijn legio. Het kan gaan om financiële middelen die op een legale wijze zijn verkregen door middel van salaris, een uitkering, studiefinanciering, een eigen onderneming, maar het betreft ook legaal verkregen niet-financiële middelen die bijvoorbeeld gebruikt worden bij de (voorbereiding) van een terroristische activiteit. In het laatste geval kan gedacht worden aan de aanschaf van een mes die gebruikt wordt bij aan aanslag.

Uit het eerder genoemde onderzoek van Soudijn (2019) naar de financiële zelfredzaamheid van Nederlandse uitreizigers bleek dat ruim de helft (52%) op enig moment inkomsten had uit eigen werkzaamheden in de vier maanden voorafgaand aan de uitreis. De grote meerderheid van de uitreizigers (95%) ontving een vorm van overheidssteun: inkomsten uit gemeentelijke, regionale of nationale basisvoorzieningen in de vorm van diverse soorten bijstandsuitkeringen, schuldhulpverlening, huur-, zorg- en kindertoeslagen. Bijna de helft (46%) had een beroep gedaan op studiefinanciering via de Dienst Uitvoering Onderwijs (DUO) gedurende één of meer meetmomenten. Uit een studie van Oftedal (2015) naar de financiering van veertig jihadistische cellen in West-Europa bleek dat terrorismefinanciering via legaal verkregen eigen middelen tussen 1994 en 2013 in toenemende mate een belangrijke financieringsmethode voor terroristen werd. Wat *lone actors* betreft blijkt uit een onderzoek dat zij vaak met – veelal beperkte – eigen legale middelen hun terroristische daad financieren (Keatinge & Keen 2017).

De FIOD heeft in de periode 2020-2022 twee tf-onderzoeken afgerond die (ook) op de tf-dreiging 'financiering met legaal verkregen eigen middelen' betrekking hadden.

4.10 Giften (via betaalverzoeken en/of crowdfunding via sociale media)

Giften van familieleden, vrienden, kennissen en/of donateurs buiten het eigen netwerk vormen een andere financiële bron waarmee terrorisme gefinancierd kan worden. Net als de vorige dreiging was ook deze tf-dreiging in de vorige NRA aangemerkt als één van de grootste dreigingen (maar wel met een enigszins andere formulering¹¹¹). Dergelijke giften kunnen op verschillende manieren worden verstrekt, bijvoorbeeld via de overhandiging van een contant geldbedrag of (grootwaarde)product dat op een later moment verkocht kan worden, via een girale of contante transactie bij een bank of geldtransactiekantoor (zie ook paragraaf 4.1), via een betaalverzoek die wordt verstuurd via Whatsapp of een soortgelijk kanaal of via een vorm van *crowdfunding* die gepromoot wordt op sociale media.

In DTN 57 van november 2022 staat dat het bij rechtszaken in Nederland waarin personen zijn veroordeeld voor terrorismefinanciering, doorgaans om relatief kleine bedragen ging die veelal door familieleden of kennissen werden overgemaakt naar

¹¹⁰ In de tweede NRA Terrorismefinanciering ging het om de volgende formulering van de dreiging: 'Verwerving van en/of financiering met legaal verkregen eigen middelen'.

¹¹¹ In de tweede NRA Terrorismefinanciering ging het om de volgende formulering van de dreiging: 'Verwerving van en/of financiering met giften of leningen van particulieren waaronder familie/vrienden'.

Nederlandse uitreizigers in Syrië en Irak (NCTV, 2022). Volgens het OM gaat het om bedragen variërend van € 200 die een vader overmaakt naar zijn uitgereisde zoon, tot enkele duizenden euro's naar andere uitgereisde familieleden of vrienden.¹¹² In de vorige NRA kwam naar voren dat tot april 2020 circa 50 personen werden verdacht van het overmaken van geld naar uitgereisde familieleden en vrienden. Ten tijde van de vorige NRA waren daarvoor 12 strafrechtelijke veroordelingen.

De FIOD heeft in de periode 2020-2022 twee tf-onderzoeken afgerond die (ook) op de tf-dreiging 'financiering via giften via betaalverzoeken en/of crowdfunding via sociale media' betrekking hadden.

Box 4.3 Terrorismedfinanciering via giften

Op 22 juni 2023 zijn een 55-jarige man en zijn 25-jarige dochter aangehouden door de FIOD. Ze worden ervan verdacht ongeveer 5,5 miljoen euro te hebben verzonden naar organisaties die te relateren zijn aan Hamas. Omdat Hamas sinds 2003 op de sanctielijst staat, is dit strafbaar gesteld in de Sanctiewet 1977 in combinatie met Verordening (EG) 2580/2001 en de Sanctieregeling Terrorisme 2002. Ook worden zij ervan verdacht deel te nemen aan een criminele organisatie, die tot doel heeft Hamas financieel te ondersteunen. Tijdens doorzoeken van een woning en een bedrijfspand zijn grote hoeveelheden contant geld in beslag genomen en is beslag gelegd op een banktegoed van circa €750.000.^a De verdachten zijn vermoedelijk betrokken bij een stichting waarvan wordt vermoed dat het een voortzetting is van de stichting Al-Aqsa Nederland^b die volgens de NCTV donaties als financiële inkomstenbron had.^c Al-Aqsa is op de sanctielijst geplaatst vanwege de financiering van organisaties die te linken zijn aan Hamas. Het OM verdenkt de huidige stichting ervan de strafbare activiteiten van de al eerder gesanctioneerde stichting te hebben overgenomen en voortgezet. Het onderzoek is opgestart naar aanleiding van de melding van OT's die door de FIU-Nederland als VT's zijn aangemerkt, en van mediaberichten over fondsenwerving voor Hamas.^{d e}

Volgens informatie die het WODC van de FIOD heeft verkregen, is in een langdurig onderzoek naar drie verdachten binnen het jihadistische netwerk het inzamelen en verstrekken van geld en goederen onderzocht. De verdachten zouden het geld en de goederen hebben ingezameld ten behoeve van vrouwen die onderdeel uitmaken van ISIS en/of Al Qa'ida. Een aantal van de vrouwen verbleef in de gevangenkampen in Syrië en Irak, terwijl anderen op vrije voeten waren in Syrië en Turkije. Sinds medio 2020 werd via Tikkie-betalverzoeken en social media platforms geld ingezameld. Er werden oproepen gedaan om geld te geven voor gevangengenomen zusters en kinderen. Het ingezamelde geld werd op verschillende manieren verstrekt aan tussenpersonen, via bankoverschrijvingen, hawala-bankieren en de fysieke overdracht van contant geld. De tussenpersonen zorgden ervoor dat het geld op de eindbestemming aankwam. Behalve geld werden er ook goederen via een postpakket verstuurd en verstrekt.

^a [Onderzoek naar grootschalige financiering van Hamas | Nieuwsbericht | Openbaar Ministerie \(om.nl\)](#).

^b [Al Aqsa gaat door onder andere naam | Trouw](#).

^c [Al Aqsa Nederland \(nctv.nl\)](#).

^d [Ophef over aanwezigheid vermeende fondsenwerver Hamas bij Nederlandse workshop | De Dikke Blauwe](#).

^e [Fondsenwerver Hamas: 'Ik was bij workshop met ambtenaren Sigrid Kaag' - EWmagazine.nl](#).

¹¹² [Om hoeveel geld gaat het? | Openbaar Ministerie](#).

4.11 Crimineel verkregen middelen: fraude en andere criminaliteitsvormen

In hoofdstuk 3 werd de grote verscheidenheid geschetst van de in Nederland gepleegde misdrijven. De criminele opbrengsten daarvan kunnen gebruikt worden voor de financiering van terrorisme. Twee van de 12 grootste tf-dreigingen hebben betrekking op een criminele financieringsbron, namelijk 'Financiering met middelen verkregen via horizontale/verticale fraude' en 'Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude'. In de vorige NRA Terrorismefinanciering maakte alleen de eerstgenoemde dreiging deel uit van de lijst van grootste tf-dreigingen (maar wel met een enigszins andere formulering¹¹³).

Uit het eerder genoemde onderzoek naar de financiële zelfredzaamheid van Nederlandse uitreizigers kwam naar voren dat sommige uitreizigers via fraude middelen hebben verworven. Zo verdiende een uitreiziger een half jaar voor vertrek naar het strijdgebied € 2.000 met 'advieswerkzaamheden', maar uit politieonderzoek bleek het om inkomsten uit fraude te gaan. Deze persoon had schijnconstructies opgezet met persoonsgebonden budgetten. Een andere uitreiziger liet vermoedelijk een of meer personen onder zijn identiteit werken en ontving maanden na zijn uitreis nog wekelijks via een (Belgisch) uitzendwerkbureau loon op zijn rekening (Soudijn, 2019).

Geen van de afgeronde FIOD-onderzoeken in de periode 2020-2022 had betrekking op de tf-dreigingen 'financiering met middelen verkregen via horizontale/verticale fraude' en 'financiering met middelen verkregen via een andere criminaliteitsvorm dan fraude'.

4.12 Potentiële impact van grootste tf-dreigingen

In de tweede expertmeeting hebben de deelnemers aan de hand van een MCA een kwantitatieve inschatting gemaakt van de potentiële impact van de hiervoor beschreven 12 grootste tf-dreigingen (zie paragraaf 2.3 voor meer informatie over de wijze waarop de potentiële impact is bepaald). De inschattingen werden gemaakt op een schaal van 0 tot 100 waarbij geldt: hoe hoger de score, hoe hoger de potentiële impact van de dreiging ten opzichte van de andere dreigingen. De scores hebben dus vooral een relatieve waarde (tussen de dreigingen onderling) dan een absolute waarde. Immers, de NRA beoogt een ordening in de grootste dreigingen aan te brengen. Tabel 4.5 geeft de MCA-resultaten weer. De meer precieze scores (met de criteriagewichten en de criteriascores) zijn geplaatst in bijlage 6.

De ingeschatte potentiële impact verschilt niet in sterke mate tussen de 12 grootste tf-dreigingen. De laagste score is 48 en de hoogste score is 61. Om deze reden worden de resultaten voor de potentiële impactschatting gecategoriseerd weergegeven. De dreiging 'Financiering via onvergunde betaaldienstverleners en hawala-bankieren' kreeg van de 12 dreigingen de hoogste score (61). De dreiging met de laagst toegekende score, 'Financiering via aanbieders van cryptodiensten', scoort 48. In een nadere analyse van de MCA-resultaten is gekeken naar de potentiële impact die de 12 grootste tf-dreigingen hebben op twee specifieke criteria uit de MCA, namelijk de prevalentie van terrorisme in Nederland en de prevalentie van terrorisme in het buitenland. Daaruit blijkt dat twee tf-dreigingen eruit springen qua score wat betreft de potentiële impact op zowel de prevalentie van terrorisme in Nederland als de

¹¹³ In de tweede NRA Terrorismefinanciering ging het om de volgende formulering van de dreiging: 'Verwerving van en/of financiering met middelen verkregen via fraude (horizontaal en verticaal)'.

prevalentie van terrorisme in het buitenland: de financiering met legaal verkregen eigen middelen en de financiering via onvergunde betaaldienstverleners en hawala-bankieren.

Tabel 4.5 Potentiële impact grootste tf-dreigingen (n=8)

Dreiging	Potentiële impact (op een schaal van 0-100)
Score-categorie '60 of meer'	
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	61
Score-categorie '55 tot en met 59'	
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	58
Financiering met middelen verkregen via horizontale/verticale fraude	57
Financiering via girale of contante transacties bij vergunde banken	57
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering	56
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	55
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	55
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude	55
Score-categorie '50 tot en met 54'	
Financiering met legaal verkregen eigen middelen	50
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	50
Financiering via internet betaaldiensten (PSP's)	50
Score-categorie 'minder dan 50'	
Financiering via aanbieders van cryptodiensten	48

4.13 Tot slot

De NRA legt de focus op 12 tf-dreigingen die – volgens tf-experts – de grootste potentiële impact hebben. Omdat de dreigingen qua potentiële impact niet veel uiteenlopen, worden deze dreigingen in tabel 4.5 gecategoriseerd weergegeven. De tf-dreigingen betreffen financieringsmethoden en -bronnen die – in verschillende combinaties van twee of meerdere dreigingen – een tf-constructie kunnen vormen. Zo'n constructie kan vrij eenvoudig van aard zijn, maar kan ook een complex karakter hebben.

De omvang van de potentiële impact van de dreigingen is bepaald door de uitvoering van een MCA. Experts maakten aan de hand van de criteria 'prevalentie terroristische activiteiten in Nederland', 'prevalentie terroristische activiteiten in het buitenland', 'aantasting financiële sector', 'vermindering subjectieve veiligheid', 'ondermijning gezag' en 'aantasting imago Nederland in het buitenland' kwantitatieve inschattingen.

De dreiging 'financiering via onvergunde betaaldienstverleners en hawala-bankieren' kreeg van de 12 dreigingen de hoogste score. De drie dreigingen met de laagst toegekende score zijn financiering via giften via betaalverzoeken en/of *crowdfunding* via sociale media, via internet betaaldiensten (PSP's) en via aanbieders van cryptodiensten. De potentiële impact van de 12 dreigingen verschilt niet in sterke mate van elkaar.

5 Weerbaarheid van het beleidsinstrumentarium

Dit hoofdstuk beschrijft allereerst de wijze waarop de preventie en bestrijding van terrorismefinanciering in Nederland is georganiseerd, waarna wordt ingegaan op het beschikbare beleidsinstrumentarium om de financiering van terrorisme te voorkomen en tegen te gaan. In deze NRA ligt de focus op het beleidsinstrumentarium dat tot en met juni 2023 bestond. De daaropvolgende paragraaf geeft een toelichting op de door experts ingeschatte weerbaarheid van het beschikbare beleidsinstrumentarium ter preventie en bestrijding van terrorismefinanciering. Het hoofdstuk besluit met een paragraaf over toekomstig beleid gericht op de preventie en bestrijding van terrorismefinanciering.

5.1 Organisatie van terrorismefinanciering-preventie en -bestrijding

Het ministerie van Financiën en het ministerie van JenV dragen de verantwoordelijkheid voor de preventie en repressie van terrorismefinanciering en de aansturing daarvan. Bij het voorkomen en bestrijden van terrorismefinanciering spelen vele publieke en private partijen een rol. In onderstaande subparagrafen wordt nader ingegaan op de wijze waarop de preventie en bestrijding van terrorismefinanciering in Nederland is georganiseerd en welke publieke en private partijen daarbij betrokken zijn.

Terrorismefinanciering-preventie

Op grond van de Wwft (zie paragraaf 5.4 voor meer info) heeft een groot aantal financiële en niet-financiële instellingen en beroepsgroepen een meldplicht: zij moeten OT's melden aan de FIU-Nederland en zijn verplicht onderzoek te doen naar hun cliënten. Zoals in hoofdstuk 3 al werd vermeld, zijn er momenteel 29 verschillende soorten meldingsplichtige instellingen die de rol van Wwft-poortwachter innemen. De FIU-Nederland analyseert de OT's, kan deze verdacht verklaren en stelt deze daarna beschikbaar aan de diverse (bijzondere) opsporings-, inlichtingen- en veiligheidsdiensten (zie hoofdstuk 3 voor meer informatie).

Bij de terrorismefinanciering-preventie spelen de branche-/koepelorganisaties van Wwft-poortwachters ook een rol. Gedacht kan worden aan de NVB, de Koninklijke Notariële Beroepsorganisatie (KNB), de Nederlandse Beroepsorganisatie van Accountants (NBA) en de Nederlandse Vereniging Geld Transactie Kantoren (NVGTK). Deze organisaties informeren hun leden over bijvoorbeeld de wijze van naleving van de Wwft en/of casuïstiek van tf-methoden waarmee hun leden te maken kunnen krijgen, en kweken awareness voor specifieke risico's.

In het kader van de Wwft zijn er zes toezichthouders die het meldgedrag van de Wwft-poortwachters beoordelen en controleren of het cliëntonderzoek in lijn met de wet is:¹¹⁴

- de Autoriteit Financiële Markten (AFM) houdt toezicht op instellingen voor collectieve belegging en effecten, bemiddelaars in levensverzekeringen, beleggingsinstellingen en beleggingsondernemingen;

¹¹⁴ [Toezichthouders - FIU-Nederland](#).

- het Bureau Financieel Toezicht (BFT) houdt toezicht op juridische dienstverleners, notarissen, accountants en belastingadviseurs;
- het Bureau Toezicht Wwft (BTWwft) houdt toezicht op kopers of verkopers van kunstvoorwerpen, bemiddelaars bij koop/verkoop in zaken van grote waarde, domicilieverleners, pandhuizen, taxateurs en makelaars;
- de lokale deken van de Nederlandse Orde van Advocaten (NOvA) in de verschillende arrondissementen houdt toezicht op advocaten die diensten verlenen die onder de Wwft vallen, waaronder advisering over het aan- en verkopen van ondernemingen, het oprichten en beheren van vennootschappen en rechtspersonen en het beheren van geld;
- DNB houdt toezicht op banken, financiële instellingen die toch bancaire activiteiten verrichten, betaaldienstverleners, beroeps- of bedrijfsmatige aanbieders van diensten voor het wisselen tussen crypto's en regulier geld, beroeps- of bedrijfsmatige aanbieders van bewaarportemonnees, verhuurders van safes, wisselinstellingen, elektronischgeldinstellingen, betaaldienstagenten, levensverzekeraars en trustkantoren;
- de Kansspelautoriteit (Ksa) houdt toezicht op speelcasino's en aanbieders van kansspelen op afstand.

Terrorismedinanciering-bestrijding

De AIVD onderzoekt in het belang van de nationale veiligheid personen en organisaties die een terroristische dreiging vormen tegen Nederland.¹¹⁵ De financiering van terrorisme kan een aspect zijn van onderzoek van de inlichtingendienst. Bij de strafrechtelijke opsporing van terrorismedinanciering spelen met name het OM, de financieel-economische recherche van de regionale politie-eenheden, de FIOD en de Dienst Landelijke Recherche een centrale rol. Personen die worden verdacht van terrorismedinanciering, kunnen door het OM worden vervolgd om daarna eventueel te worden berecht. Het OM en het Centraal Justitieel Incassobureau (CJIB) spelen een rol bij het ontnemen van crimineel vermogen. Ook de Koninklijke Marechaussee (KMar) en de Douane Nederland hebben een belangrijke taak bij de bestrijding van terrorismedinanciering. Zo werkt de KMar op Schiphol nauw samen met de FIOD; bij verdenkingen van terrorismedinanciering draagt de KMar de zaak over aan de FIOD. De Douane Nederland levert informatie aan de FIU-Nederland over grensvervoer van grote aantallen liquide middelen en waardevolle goederen met een waarde van € 10.000 of meer, zoals contant geld, horloges, antiek en sieraden, of ongebruikelijke zendingen van liquide middelen zoals goud en cheques.

5.2 Beschikbaar beleidsinstrumentarium

Het beschikbare beleidsinstrumentarium ter voorkoming en bestrijding van terrorismedinanciering omvat alle relevante instrumenten die voortvloeien uit internationale en nationale wet- en regelgeving, wet- en regelgeving op gemeentelijk niveau, sectorale en branchegerichte regelgeving, en regelgeving op organisatieniveau. Zoals ook al in de vorige NRA Terrorismedinanciering naar voren kwam, kan het begrip 'beleidsinstrument' breder worden opgevat dan alleen wet- en regelgeving. Ook samenwerkingsverbanden tussen publieke en/of private organisaties, richtlijnen, handreikingen en beleidsplannen van organisaties die een rol spelen bij de preventie en/of bestrijding van terrorismedinanciering, worden in deze NRA gezien als beleidsinstrumenten.

¹¹⁵ [Terrorisme | AIVD](#).

Aan het begin van de derde expertmeeting is een voorlopige lijst van beschikbare beleidsinstrumenten in gezamenlijkheid besproken. Deze bespreking heeft het volgende overzicht van het beschikbare beleidsinstrumentarium ter preventie en bestrijding van terrorismefinanciering opgeleverd (zie tabel 5.1). Een korte toelichting op ieder beleidsinstrument volgt in de daaropvolgende paragrafen. Aangezien de derde expertmeeting in juni 2023 plaatsvond, heeft onderstaande tabel alleen betrekking op de instrumenten die tot die periode geïmplementeerd waren.

Tabel 5.1 Beleidsinstrumentarium ter preventie en bestrijding van terrorismefinanciering

Internationale wet- en regelgeving	Nationale wet- en regelgeving	Overige beleidsinstrumenten
<ul style="list-style-type: none"> • FATF-aanbevelingen • EU anti-witwasrichtlijnen • Verenigde Naties Veiligheidsraad Resoluties en EU Verordeningen • Overige internationale sanctielijsten • Europese verordening Aangifte liquide middelen • <i>Wire Transfer Regulation 2</i> 	<ul style="list-style-type: none"> • Wet ter voorkoming van witwassen en financieren van terrorisme • Sanctiewet 1977 en sanctieregelingen • Wetboek van Strafrecht • Wetboek van Strafvordering • Wet op de inlichtingen- en veiligheidsdiensten 2017 • Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding • Wet precursoren voor explosieven • Wet op het financieel toezicht • Algemene Douanewet • Wet controle op rechtspersonen • Handelsregisterwet 2007 (inclusief UBO-registers) • Fiscale wetgeving • Sociale wetgeving • Wet op de economische delicten • Wet Bibob 	<ul style="list-style-type: none"> • Nationale samenwerkingsverbanden • Internationale samenwerkingsverbanden • Sectorale regelgeving en voorwaarden • Richtlijnen, handreikingen en beleidsplannen

5.3 Internationale wet- en regelgeving

FATF-aanbevelingen

Het Nederlandse beleid ter preventie en bestrijding van terrorismefinanciering is gebaseerd op de aanbevelingen van de FATF. Leden van de FATF, waaronder Nederland, zijn gebonden aan aanbevelingen gericht op het nemen van preventieve en repressieve maatregelen en maatregelen ter verbetering van nationale rechtsstelsels en internationale samenwerking. De FATF ziet toe op de juiste werking en de effectiviteit van de uitvoering van die regels en voert in dit kader periodiek een landenevaluatie uit om na te gaan in hoeverre een land tegemoetkomt aan de

aanbevelingen. De FATF (2022) heeft een landenevaluatie van het Nederlandse anti-witwas- en terrorismefinancieringsbeleid uitgevoerd.¹¹⁶

EU anti-witwasrichtlijnen

Het grootste deel van de FATF-aanbevelingen is voor de EU-lidstaten omgezet naar diverse opeenvolgende Europese anti-witwasrichtlijnen waarmee op Europees niveau regels zijn vastgesteld ter voorkoming van het gebruik van het financiële stelsel voor witwassen en het financieren van terrorisme. Momenteel is de vijfde EU-anti-witwasrichtlijn van toepassing en is de zesde anti-witwasrichtlijn in ontwikkeling. In Nederland zijn deze regels ter voorkoming van het gebruik van het financieel stelsel voor witwassen en financieren van terrorisme opgenomen in de Wwft (zie paragraaf 5.4).

Verenigde Naties Veiligheidsraad Resoluties en EU Verordeningen

Sanctiemaatregelen zijn politieke instrumenten in het buitenlands en veiligheidsbeleid van de Verenigde Naties (VN) en de EU. Het zijn dwingende, niet-militaire, instrumenten die, in een poging een kentering teweeg te brengen, worden ingezet als reactie op schendingen van het internationale recht of van mensenrechten door regimes die rechtsstatelijke en democratische beginselen niet eerbiedigen. Daarnaast vervullen sancties een rol in de bestrijding van terrorisme. Daartegen gerichte sancties zijn vooral gericht tegen individuen en niet-statelijke entiteiten. Sanctiemaatregelen berusten meestal op een resolutie van de VN Veiligheidsraad (VR) die vervolgens in secundair Europeesrecht worden omgezet. Een aantal sanctiemaatregelen hebben een autonome Europese grondslag. De meest voorkomende sancties zijn wapenembargo's en handelsrestricties, financiële sancties (bevriezing van tegoeden) en reis- en visumrestricties.¹¹⁷

De VN kennen in het kader van de preventie en bestrijding van terrorisme een aantal VR Resoluties. De VN VR resolutie 1.373 (2001) schept voor VN-lidstaten een internationaal bindende verplichting om het financieren van terrorisme te bestrijden en de tegoeden, andere financiële activa of andere economische middelen van personen en organisaties die zich bezighouden met terroristische activiteiten, te bevriezen. VN VR resoluties 1.267 (1999), 2.253 (2015) en 2.368 (2017) leggen staten daarnaast de verplichting op de tegoeden en andere financiële activa van personen en organisaties te bevriezen die door het bij resolutie 1.267, resolutie 2.253, en 2.368 ingestelde comité van de Veiligheidsraad worden aangewezen als zijnde verbonden met Al Qa'ida en ISIS. Ook zijn op deze personen of organisaties een (door)reisverbod en wapenembargo van toepassing. Aan VN VR resolutie 1.373 wordt in EU-verband uitvoering gegeven door het Gemeenschappelijk Standpunt (GS) nr. 2001/930/GBVB, het GS nr. 2001/931/GBVB, de Verordening (EG) nr. 2580/2001 en het GS nr. 2016/1693. Aan VN VR resoluties 1.267 en 2.253 wordt uitvoering gegeven middels de Verordening (EU) nr. 2016/1686.¹¹⁸

Overige internationale sanctielijsten

Naast de VN- en EU-sanctielijsten die zijn samengesteld als gevolg van de hierboven beschreven resoluties en verordeningen, bestaan er ook sanctielijsten van andere (niet-Europese) landen die van belang zijn in het kader van de Nederlandse preventie

¹¹⁶ [The Netherlands' measures to combat money laundering and terrorist financing \(fatf-gafi.org\)](https://www.fatf-gafi.org/).

¹¹⁷ Zie link naar bijlage via [Sanctieregelingen stand van zaken 17 juli 2023 | Rapport | Rijksoverheid.nl](#).

¹¹⁸ Zie link naar bijlage via [Procedures totstandkoming en beëindiging van bevroeringsmaatregelen terrorisme | Publicatie | Rijksoverheid.nl](#).

en bestrijding van terrorismefinanciering. Een voorbeeld hiervan is de lijst van *Specially Designated Nationals* (SDN's) van het *Office of Foreign Assets Control* (OFAC) van het Amerikaanse ministerie van Financiën. Het OFAC beheert en handhaaft economische en handelssancties op basis van het Amerikaanse buitenlands beleid en nationale veiligheidsdoelstellingen tegen gerichte buitenlandse landen en regimes, terroristen, internationale drugshandelaars, degenen die betrokken zijn bij activiteiten die verband houden met de verspreiding van massavernietigingswapens en andere bedreigingen voor de nationale veiligheid, het buitenlands beleid of de economie van de Verenigde Staten. De bezittingen van SDN's zijn geblokkeerd.¹¹⁹ Een ander voorbeeld van een sanctielijst is de Britse *UK Sanctions List* waarop personen, entiteiten en schepen zijn geplaatst op grond van de daar geldende *Sanctions and Anti-Money Laundering Act 2018*.¹²⁰

Europese verordening liquidemiddelencontrole

Sinds juni 2007 gelden regels over het verkeer van liquide middelen in en uit het grondgebied van de EU, die integraal deel uitmaken van het EU-kader ter preventie en bestrijding van witwassen en terrorismefinanciering. De wetgeving verplicht alle burgers die de EU binnenkomen of verlaten en liquide middelen ter waarde van € 10.000 of meer bij zich dragen, die liquide middelen aan te geven bij de douaneautoriteiten. Eind 2018 is een herziene nieuwe verordening met geactualiseerde regels vastgesteld die in juni 2021 in werking is getreden.¹²¹ Sindsdien vallen niet alleen bankbiljetten maar ook liquide activa zoals cheques, reischeques, prepaidkaarten en goud onder de definitie 'liquide middelen'. Ook is de verordening sindsdien van toepassing op liquide middelen die worden vervoerd in post-, vracht- of koerierzendingen.

Wire Transfer Regulation 2

De *Wire Transfer Regulation 2* (WTR2) verplicht sinds juni 2017 betaaldienstverleners en intermediaire betaaldienstverleners naast informatie over de betaler ook informatie over de begunstigde vast te leggen. Zo moeten betaaldienstverleners de naam en het betaalrekeningnummer van de begunstigde bij geldovermakingen voegen. Ook zijn – ten opzichte van de eerdere WTR1 – de verplichtingen aangescherpt voor betaalproducten die anoniem te gebruiken of niet persoonsgebonden zijn.

5.4 Nationale wet- en regelgeving

Wet ter voorkoming van witwassen en financieren van terrorisme

De Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) beoogt het gebruik van het financieel stelsel voor witwassen en financieren van terrorisme te voorkomen door een aantal verplichtingen op te leggen aan een groot aantal financiële en niet-financiële instellingen en beroepsgroepen (zie ook paragraaf 5.1). Deze partijen zijn verplicht cliëntonderzoek te verrichten, waaronder onder meer het identificeren van de cliënt en het verifiëren van diens identiteit, het identificeren van de *Ultimate Beneficial Owner* (UBO) en het nemen van maatregelen om diens identiteit te verifiëren. Ook zijn deze partijen verplicht OT's te melden bij de FIU-Nederland aan de hand van objectieve en subjectieve indicatoren. Een voorbeeld van een objectieve

¹¹⁹ [Home | Office of Foreign Assets Control \(treasury.gov\)](https://www.treasury.gov).

¹²⁰ [The UK Sanctions List - GOV.UK \(www.gov.uk\)](https://www.gov.uk).

¹²¹ [Controle op liquide middelen die EU binnenkomen of verlaten: Raad neemt verordening aan - Consilium \(europa.eu\)](https://europa.eu).

indicator is 'contante wisseltransacties met een waarde van € 10.000 of meer' en een voorbeeld van een subjectieve indicator is 'transacties waarbij een aanleiding bestaat bij een instelling om te veronderstellen dat deze verband kunnen houden met witwassen of het financieren van terrorisme'. De Wwft schrijft een risicogebaseerde aanpak voor: instellingen moeten zelf het risico inschatten dat een cliënt geld witwast of terrorisme financiert en moeten de striktheid van de eigen maatregelen daarop afstemmen. Die maatregelen kunnen variëren van een vereenvoudigd cliëntonderzoek tot het niet aangaan of verbreken van een zakelijke relatie.

Een relevante wijziging ten aanzien van de Wwft sinds de vorige NRA Terrorismefinanciering is dat sinds mei 2020 ook bedrijven die diensten aanbieden voor het wisselen tussen crypto's en regulier geld evenals bedrijven die cryptobewaarpportemonnees aanbieden, op grond van de Wwft onder het toezicht van DNB vallen. Volgens DNB is het toezicht op de cryptomarkt op dit moment nog minder goed geregeld als het toezicht op andere financiële markten. Zij houdt op dit moment alleen toezicht op basis van de Wwft en de Sanctiewet 1977 (zie hieronder), waarbij alleen de genoemde cryptodienstverleners zich bij DNB moeten registreren.¹²²

Sanctiewet 1977 en sanctieregelingen

De Sanctiewet 1977 biedt een grondslag voor de totstandkoming van nationale regels ter uitvoering van internationale sanctiemaatregelen.¹²³ De AFM en DNB zijn belast met het toezicht op de naleving van de Sanctiewet 1977 met betrekking tot het financieel verkeer. Op grond van de Regeling toezicht Sanctiewet 1977 moeten financiële ondernemingen maatregelen treffen op het gebied van de administratieve organisatie en interne controle om zo de bepalingen van de sanctieregelgeving na te leven. Ook zijn financiële ondernemingen zelf verantwoordelijk voor een correcte naleving van de sanctieregelingen door te controleren of relaties van een instelling voorkomen op één of meerdere sanctielijsten. De nationale sanctielijst terrorisme is opgesteld op grond van de Sanctieregeling Terrorisme 2007-II, die ertoe strekt om de tegoeden van personen en organisaties die zich bezighouden met terroristische activiteiten, te kunnen bevriezen.

Wetboek van Strafrecht en Wetboek van Strafvordering

Het Wetboek van Strafrecht (WvSr) bepaalt wat de strafbare feiten zijn en welke straffen ervoor kunnen worden uitgesproken en het Wetboek van Strafvordering (WvSv) bepaalt hoe strafbare feiten vervolgd worden. In hoofdstuk 1 is al een beschrijving gegeven van terrorismefinanciering in het WvSr.

Wet op de inlichtingen- en veiligheidsdiensten 2017

In mei 2018 is de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) in werking getreden. De wet vormt het wettelijk kader voor de AIVD en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en regelt de voorafgaande toetsing door de Toetsingscommissie Inzet Bevoegdheden en de controle gedurende het hele proces en het toezicht achteraf door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten. De vorige Wiv stamde uit 2002 en was sterk verouderd. Sinds die tijd zijn er meerdere technologische ontwikkelingen geweest die het (tele)communicatielandschap hebben veranderd. De Wiv 2017 schrijft voor hoe de AIVD en MIVD om dienen te gaan met het onderscheppen van communicatie via kabels, het hacken van computers, DNA-profielen en het delen van gegevens met

¹²² [Wat u moet weten over crypto's \(dnb.nl\)](#).

¹²³ [Sanctieregelingen stand van zaken 17 juli 2023 | Rapport | Rijksoverheid.nl](#).

buitenlandse collega-diensten. De wet kan op deze manier ook een rol spelen bij de preventie en bestrijding van terrorismefinanciering.

Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding

Op 1 maart 2017 is de Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding in werking getreden.¹²⁴ De wet maakt het mogelijk om preventieve maatregelen te nemen om terroristische aanslagen te voorkomen. Daarmee kan deze wet ook een rol spelen bij de preventie en bestrijding van terrorismefinanciering. Het gaat primair om het reduceren van de dreiging die uitgaat van de jihadistische beweging. Op basis van de wet kunnen onder meer vrijheidsbeperkende maatregelen (art. 2) worden genomen. Het betreft een meldplicht bij de politie, een verbod om zich te bevinden in de omgeving van bepaalde objecten of in bepaalde delen van Nederland (gebiedsverbod) of zich te bevinden in de nabijheid van bepaalde personen (contactverbod). Voor toepassing van de vrijheidsbeperkende maatregelen moet aan twee wettelijke voorwaarden zijn voldaan: (1) de betreffende persoon moet 'door zijn persoonlijke gedragingen in verband kunnen worden gebracht met terroristische activiteiten of de ondersteuning daarvan', en (2) de maatregel moet noodzakelijk zijn met het oog op de bescherming van de nationale veiligheid. Ook kan op basis van de tijdelijke wet een uitreisverbod worden opgelegd (art. 3) ofwel een verbod om zich buiten het Schengengebied te begeven. Voor toepassing van het uitreisverbod geldt als voorwaarde dat er 'gegronde vermoedens' bestaan dat een persoon zal uitreizen buiten het Schengengebied om zich bij de terroristische organisatie ISIS, Al Qa'ida en/of Hay'at Tahrir al-Sham aan te sluiten. Ook deze maatregel moet noodzakelijk zijn met het oog op de bescherming van de nationale veiligheid. Een derde type maatregel dat op basis van de wet genomen kan worden, is het afwijzen of intrekken van subsidies, vergunningen, ontheffingen en/of erkenningen door een bestuursorgaan (art. 6).

Wet precursoren voor explosieven

In september 2014 trad de EU Verordening 'over het op de markt brengen en het gebruik van precursoren voor explosieven' (98/2013) in werking. Deze verordening is op 1 juni 2016 in Nederland geïmplementeerd in de Wet precursoren voor explosieven (Wpe). Deze wet ziet er op toe dat verdachte transacties¹²⁵ met precursoren worden gemeld en dat een aantal precursoren alleen door particulieren kunnen worden gekocht als ze over een vergunning beschikken (Kruize en Gruter, 2021). Explosieven die met precursoren worden gemaakt, kunnen gebruikt worden voor het plegen van een terroristische activiteit. De aanschaf van de precursoren kan in dat geval gezien worden als een vorm van terrorismefinanciering. In februari 2021 trad de aangepaste EU Verordening voor precursoren voor explosieven in werking waarmee ook de Nederlandse wetgeving is aangepast. Sinds 1 februari 2021 geldt een aantal verplichtingen voor bedrijven met betrekking tot het verkopen, bezitten en op de markt brengen van precursoren, oftewel grondstoffen waar explosieven mee gemaakt kunnen worden. Precursoren waarvoor een beperking geldt, mogen niet worden gebruikt door particulieren, tenzij ze een vergunning hebben. Professionele gebruikers kunnen vergunningvrij gebruik maken van precursoren voor explosieven, maar alleen als men kan aantonen dat deze middelen noodzakelijk zijn voor het uitvoeren van hun handels-, bedrijfs- of beroepsactiviteiten. Alle stoffen die zijn verhandeld in een verdachte transactie of die zijn vermist of gestolen, moeten binnen 24 uur gemeld worden bij het Meldpunt Verdachte Transacties Chemicaliën (NCTV, 2021).

¹²⁴ De informatie uit deze subparagraaf komt uit: Van Gestel et al. (2019).

¹²⁵ Het betreft hier andersoortige 'verdachte transacties' dan de VT's volgens de FIU-Nederland.

Wet op het financieel toezicht

Sinds 1 januari 2007 regelt de Wet op het financieel toezicht (Wft) het toezicht op de financiële sector in Nederland. Financieel toezicht beoogt de stabiliteit van het financiële systeem te waarborgen, ervoor te zorgen dat de financiële markten efficiënt werken en consumenten te beschermen tegen een faillissement of ontoelaatbaar gedrag van financiële instellingen. De Wft bepaalt onder andere dat instellingen moeten zorgen voor een integere en beheerste bedrijfsvoering en zorgt voor een toets op geschiktheid en betrouwbaarheid van de beleidsbepalers van financiële ondernemingen. DNB en de AFM zijn de toezichthouders in het kader van de Wft:

- DNB heeft tot taak het 'prudentieel toezicht' op financiële ondernemingen uit te oefenen en beslissingen te nemen over de toelating van financiële ondernemingen tot de financiële markten. Prudentieel toezicht is gericht op de soliditeit van financiële ondernemingen en het bijdragen aan de stabiliteit van de financiële sector.
- De AFM heeft tot taak het 'gedragstoezicht' op financiële markten uit te oefenen en beslissingen te nemen over de toelating van financiële ondernemingen tot die markten. Gedragstoezicht richt zich op ordelijke en transparante financiële marktprocessen, zuivere verhoudingen tussen marktpartijen en zorgvuldige behandeling van cliënten.

Algemene Douanewet

In de Algemene Douanewet staan regels ten behoeve van een goede werking van door Nederland gesloten internationale overeenkomsten inzake de Douane. De wet bevat onder meer regelgeving die betrekking heeft op controlebepalingen en strafrechtelijke bepalingen. In 2021 is de Algemene Douanewet gewijzigd om de wettelijke basis voor het toezicht door de Douane te verbreden tot toezicht op het intra-EU-verkeer en het verkeer in het binnenland. Met deze wetwijziging werd het voor de Douane mogelijk om in het derde landenverkeer niet alleen op liquide middelen maar ook op andere waardevolle goederen, zoals sieraden, dure horloges, edelstenen en antiek, en op documenten die duiden op vermogensbestanddelen, te controleren.

Wet controle op rechtspersonen

De Wet controle op rechtspersonen heeft als doel misbruik door rechtspersonen te voorkomen en bestrijden. Met de wet heeft Nederland een systeem van doorlopende controle van rechtspersonen: een zogenoemde integriteitstoets van de rechtspersoon, de bestuurders en andere bij de rechtspersoon betrokken personen en bedrijven die kan uitmonden in een risicomelding. De wet draagt bij aan een structurele aanpak van financieel-economische criminaliteit. Door rechtspersonen doorlopend te controleren op mogelijk misbruik worden toezichthoudende instanties, opsporingsinstanties en/of andere handhavende instanties in de gelegenheid gesteld adequater op te treden (Justis, 2017). Ook kunnen die partijen een 'netwerktekening' die de onderlinge relevante relaties tussen de bevraagde rechtspersoon en andere (natuurlijke en rechts)personen en/of bedrijven alsmede de relevante faillissementen en ontbindingen in kaart brengt, aanvragen. Het toezicht wordt uitgevoerd door Justis/TRACK.

Handelsregisterwet 2007

Op 1 januari 2008 trad de Handelsregisterwet 2007 in werking die bepalingen bevat omtrent de verplichte inschrijving in het Handelsregister bij de KvK. Deze verplichting geldt niet alleen voor ondernemingen maar ook voor alle Nederlandse privaatrechtelijke en publiekrechtelijke rechtspersonen alsmede hun vestigingen. De KvK beheert ook twee UBO-registers waarin staat wie de eigenaar is van een organisatie of wie zeggenschap of een belang daarin heeft: het UBO-register voor

vennootschappen en andere juridische entiteiten dat is gericht op ondernemingen, stichtingen en verenigingen en het UBO-register voor trusts en soortgelijke juridische constructies. Ten tijde van het schrijven van deze NRA waren UBO-gegevens in de beide registers (sinds 22 november 2022) niet meer openbaar toegankelijk als gevolg van een uitspraak van het Europese Hof in Luxemburg over de UBO-registers.¹²⁶ Inmiddels ligt er een wetsvoorstel voor om de toegang tot de UBO-registers te beperken tot instanties met een wettelijke taak bij het voorkomen en tegengaan van fraude, witwassen en terrorismefinanciering en daarnaast personen en instanties met een legitiem belang, zoals pers en ngo's.¹²⁷ Dit neemt niet weg dat organisaties verplicht blijven om UBO's in te schrijven. Opsporingsdiensten behouden dus toegang tot de beide registers.

Fiscale en sociale wetgeving

Op basis van fiscale wetgeving controleert de Belastingdienst stichtingen met een ANBI-status, waarmee wordt beoogd het risico dat dergelijke stichtingen gebruikt worden voor terrorismefinanciering, te verkleinen. Ook kan op basis van fiscale wetgeving worden gehandhaafd in het geval van onrechtmatig ontvangen toeslagen.

Ook sociale wetgeving kan een relevant beleidsinstrument vormen, gezien het feit dat terrorisme gefinancierd kan worden met verschillende typen middelen van de staat, zoals een uitkering of studiefinanciering. Onder sociale wetgeving vallen onder meer de Wet structuur uitvoeringsorganisatie werk en inkomen, de Wijziging van de socialezekerheidswetgeving de Wet studiefinanciering 2000, de Wet tegemoetkoming onderwijsbijdrage en schoolkosten en de Algemene wet inkomensafhankelijke regelingen. In deze wetten is een grondslag opgenomen voor beëindiging van uitkeringen, studiefinanciering en tegemoetkoming bij deelname aan een terroristische organisatie.

Wet op de economische delicten

De Wet op de economische delicten is een kaderwet waarin alle economische delicten staan beschreven. Bepaalde overtredingen van de Wwft, Wft en de Handelsregisterwet 2007 zijn aangemerkt als een economisch delict.

Wet bevordering integriteitsbeoordelingen door het openbaar bestuur

De Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Wet Bibob) is een bestuursrechtelijk instrument dat van toepassing is op bepaalde vergunningen, subsidies, aanbestedingen en vastgoedtransacties. Bestuursorganen kunnen op grond van de Wet Bibob een vergunning weigeren of intrekken als er een ernstig gevaar bestaat dat de vergunning mede zal worden gebruikt om strafbare feiten te plegen of om crimineel geld te benutten. De Wet Bibob beoogt te voorkomen dat de overheid criminele activiteiten faciliteert en beschermt de concurrentiepositie van bonafide ondernemers.

¹²⁶ [Registratie in UBO-registers | Financiële sector | Rijksoverheid.nl](#).

¹²⁷ [Wetsvoorstel om toegang tot UBO-registers te beperken | Nieuwsbericht | Rijksoverheid.nl](#)

5.5 Overige beleidsinstrumenten

Nationale samenwerkingsverbanden

Er bestaan in Nederland diverse samenwerkingsverbanden op het terrein van de preventie en bestrijding van terrorismefinanciering, zowel tussen publieke dan wel private partijen onderling maar ook tussen publieke en private partijen.

Financieel Expertise Centrum

Het FEC is een samenwerkingsverband waarbinnen de AFM, DNB, het OM, de Nationale Politie, de FIU-Nederland, de FIOD en de Belastingdienst met elkaar samenwerken. Doel van het FEC is het versterken van de integriteit van de financiële sector door het uitwisselen van informatie en het delen van inzichten, kennis en vaardigheden. In het FEC bestaat ook een publiek-private samenwerking (FEC PPS) met de NVB en de vier grootbanken als vaste samenwerkingspartners, waarbij informatie-uitwisseling plaatsvindt in taskforces: de *Serious Crime Taskforce* en de *Terrorismefinanciering Taskforce* (zie hieronder).

Programma Terrorismefinanciering

Sinds 2015 draait binnen het FEC een vast programma dat zich richt op het bestrijden van terrorismefinanciering (FEC-TF). Het programma FEC-TF heeft de volgende doelstellingen (FEC, 2023):

- het in kaart brengen van de financiële netwerken van bij de FEC-partners en -participanten bekende personen, die in verband kunnen worden gebracht met terrorisme en andere daarbij relevante personen en entiteiten.
- in de gevallen waarbij het verkregen inzicht daartoe aanleiding geeft: een interventiestrategie opstellen die bijvoorbeeld ziet op fiscaalrechtelijke, bestuursrechtelijke en/of strafrechtelijke vervolgonderzoeken.
- het, met de verworven kennis, opstellen van getoetste typologieën en/of het verankeren van 'lessons learned' bij betrokken partners.

Het Jaarverslag 2022 van het FEC vermeldt dat maandelijks zogeheten TF-datarooms worden georganiseerd waarin ongeveer 25 deelnemers vanuit 13 organisaties (partners en participanten) de analyses en mogelijke interventies bespreken.

Terrorismefinanciering Taskforce

De Terrorismefinanciering Taskforce (TFTF) is in 2017 opgezet met als doel een nauwere samenwerking tussen de publieke en de private partijen te bewerkstelligen om terrorismefinanciering efficiënter en effectiever te bestrijden en zodoende de integriteit van de financiële sector te beschermen (FEC, 2023). De aanvankelijk als pilot gestarte TFTF is in 2019 omgezet in een structurele activiteit in FEC-PPS verband. Het OM treedt op als voorzitter van de TFTF. In de TFTF wordt binnen de bestaande wettelijke kaders subjectinformatie gedeeld tussen publieke en private partijen. In 2020 is Triodos Bank als vijfde bank toegetreden tot de TFTF.¹²⁸

Contraterrorisme Infobox

De Contraterrorisme (CT) Infobox is een samenwerkingsverband tussen tien organisaties binnen het veiligheids-, opsporings- en inlichtingendomein, waaronder de AIVD, de MIVD, de Landelijke Eenheid van de politie, de KMar, het OM, FIU-Nederland

¹²⁸ [Taskforces - FEC-partners](#).

en de NCTV. De CT Infobox brengt informatie over de aangemelde netwerken en personen die betrokken zijn bij terrorisme, bijeen.¹²⁹

Commissie Meldplicht van ongebruikelijke transacties

De Commissie Meldplicht van ongebruikelijke transacties komt tweemaal per jaar bijeen. Branche-/koepelorganisaties van meldingsplichtige instellingen, Wwft-toezichthouders, het OM en de FIU-Nederland voeren met vertegenwoordigers van het ministerie van Financiën en het ministerie van JenV overleg onder meer over ontwikkelingen in het nationaal beleid ter preventie en repressie van witwassen en terrorismefinanciering, de inrichting en uitvoering van de meldplicht en de vaststelling van de indicatoren aan de hand waarvan wordt beoordeeld of een transactie dient te worden aangemerkt als een OT.

Transactie Monitoring Nederland

In juli 2020 is Transactie Monitoring Nederland (TMNL) opgericht door de vijf banken ABN AMRO, ING, Rabobank, Triodos Bank en de Volksbank. De gezamenlijke monitoring ten aanzien van transacties tussen zakelijke entiteiten ging in 2021 van start.¹³⁰ TMNL heeft drie doelstellingen, namelijk 1. het sneller, beter en vollediger identificeren van witwassen en terrorismefinanciering en het bijdragen aan het voorkomen daarvan, 2. de bruikbaarheid van aangeleverde meldingen van OT's aan opsporingsdiensten vergroten, en 3. het bijdragen aan de optimalisering van de inzet van private en publieke middelen in de bestrijding van witwassen en terrorismefinanciering.¹³¹ Het wetsvoorstel plan van aanpak witwassen (zie paragraaf 5.7) beoogt het mogelijk te maken ook transacties van natuurlijke personen te monitoren.

Fintell Alliance NL

De FIU-Nederland werkt in het publiek-private samenwerkingsverband Fintell Alliance NL samen met de banken ABN AMRO, ING, Rabobank, de Volksbank, Triodos en Knab.¹³² Binnen de juridische mogelijkheden worden inzichten gedeeld met als doel meer zicht te krijgen op criminele netwerken en de wijze waarop deze te werk gaan.

Internationale samenwerkingsverbanden

Er bestaan verschillende internationale samenwerkingsverbanden op het terrein van de preventie en repressie van terrorismefinanciering, waarin de FIU-Nederland, opsporingsdiensten en het OM veelvuldig contact hebben met hun buitenlandse partners. Zo vindt er informatiedeling met buitenlandse partners plaats via bijvoorbeeld de kanalen van de *Egmont Group* en FIU.net, Interpol, Europol en Eurojust. Gezamenlijke initiatieven met buitenlandse partners worden opgepakt onder meer binnen het *European Multidisciplinary Platform Against Criminal Threats* (EMPACT) – waaronder een project gericht op de aanpak van ondergronds bankieren in 2021 – en het platform *Joint Chiefs of Global Tax Enforcement* (J5) en het daarin onder gebrachte internationale systeem voor het matchen van data, *Financial Criminal Investigations Net* (FCI-Net). Ook wordt samengewerkt wat betreft Europese en andere internationale rechtshulp, worden multilaterale en bilaterale contacten met verschillende landen onderhouden en zijn in diverse landen liaisonofficiers van de politie en de KMar alsmede liaison-magistraten van het OM geplaatst die onder meer

¹²⁹ [CT Infobox | Nationaal Coördinator Terrorisbestrijding en Veiligheid \(nctv.nl\)](#).

¹³⁰ [Transactie Monitoring Nederland aan de slag \(nvb.nl\)](#).

¹³¹ [Samen financiële criminaliteit bestrijden - TMNL](#).

¹³² [Nationale samenwerking - FIU-Nederland](#).

tot taak hebben samenwerking te bevorderen bij Nederlandse strafrechtelijke onderzoeken, bijvoorbeeld door de uitvoering van Nederlandse rechtshulpverzoeken te begeleiden. Tot slot zijn de toezichthouders, waaronder DNB en de AFM, actief in internationale samenwerkingsverbanden, zoals de *Standing Committee on anti-money laundering and countering terrorist financing* (AMLSC) van de *European Banking Authority* (EBA) en het *Basel Committee on Banking Supervision* (BCBS).

Overige beleidsinstrumenten

Naast de nationale en internationale samenwerkingsverbanden is nog een aantal andersoortige beleidsinstrumenten te onderscheiden:

- *Sectorale regelgeving en voorwaarden*. Binnen sectoren kan ook sprake zijn van regelgeving en voorwaarden die een rol spelen bij het voorkomen en bestrijden van terrorismefinanciering via hun sector. Zo hebben Nederlandse banken algemene bankvoorwaarden waarin de omgangsregels tussen banken en hun klanten staan beschreven. Alle banken die zijn aangesloten bij de NVB, gebruiken dezelfde algemene bankvoorwaarden. Banken kunnen op basis hiervan, indien nodig, klanten uitsluiten.
- *Fraudepreventiesysteem*. De Externe Verwijzingsapplicatie (EVA) is het gezamenlijke fraudepreventiesysteem van de NVB en de Vereniging van financieringsondernemingen in Nederland (VFN). Het EVA-register verbindt de frauderegisters van de aangesloten organisaties met elkaar en mag door banken die lid zijn van de NVB, onderling gedeeld worden.
- *Toezichtarrangementen*. Tussen Wwft-poortwachters en Wwft-toezichthouders kan een toezichtarrangement bestaan: een samenhangend geheel van processen, procedures en afspraken, gericht op het vaststellen van de naleving van de wet- en regelgeving waarop het toezicht betrekking heeft. Daartoe behoren onder meer afspraken over procedures en protocollen en de inrichting van administraties en dossiers. Zo heeft BFT toezichtarrangementen afgesloten met het Register Belastingadviseurs en de Samenwerkende Registeraccountants en Accountants-Administratieconsulenten (SRA).¹³³
- *Richtlijnen, handreikingen, beleidsplannen en overige publicaties*. Onder meer de FATF, *The Wolfsberg Group*¹³⁴, de Wwft-toezichthouders en branche- of beroepsorganisaties publiceren richtlijnen, handreikingen, typologieën en indicatoren, onder meer op het terrein van terrorismefinanciering. Ook publicaties van de FIU-Nederland en het FEC zijn gericht op het bevorderen van het bewustzijn. Daarnaast richten diverse beleidsplannen zich op de preventie en bestrijding van witwassen en terrorismefinanciering, zoals het *Plan van Aanpak Witwassen* van het ministerie van Financiën en het ministerie van JenV (2019). Tot slot rekenen tf-experts, zo bleek in de derde expertmeeting, de Europese SNRA en de Nederlandse NRA tot beleidsinstrument.

5.6 Inschatting weerbaarheid beleidsinstrumentarium

In de derde expertmeeting hebben de zes deelnemende experts voor alle 12 grootste tf-dreigingen *per dreiging* een kwantitatieve inschatting gemaakt van de mate waarin het totale pakket aan beschikbare beleidsinstrumenten de betreffende dreiging

¹³³ [Wwft - Bureau Financieel Toezicht \(bureaufinancieeltoezicht.nl\)](https://www.bureaufinancieeltoezicht.nl).

¹³⁴ De *Wolfsberg Group* is een samenwerkingsverband van 12 mondiale banken dat tot doel heeft raamwerken en richtlijnen te ontwikkelen voor het beheer van risico's op het gebied van financiële criminaliteit. Zie: [Home - Wolfsberg Group \(wolfsberg-group.org\)](https://www.wolfsberg-group.org).

voorkomt dan wel tegengaat. Per tf-dreiging konden zij een score van 0 tot 100 toekennen, waarbij geldt: hoe hoger de score, hoe hoger de weerbaarheid ofwel hoe beter de tf-dreiging wordt voorkomen of tegengegaan. Een score van 100 zou betekenen dat 100% van de potentiële impact van een dreiging wordt weggenomen door beleidsinstrumentarium. Een score van 0 daarentegen zou betekenen dat de potentiële impact volledig blijft bestaan en dat het beleidsinstrumentarium 0% wegneemt van de dreiging. Beide situaties (een score van 0 of 100) zijn echter weinig realistisch. Deze expert-oordelen zijn, net als alle andere expert-oordelen in deze NRA, tot stand gekomen in twee rondes met een tussentijdse plenaire discussie.

Experts zijn bij hun inschatting van de weerbaarheid van het beleidsinstrumentarium uitgegaan van de beleidsinstrumenten die op dat moment (juni 2023) bestonden. Dat betekent dus dat zij bij hun inschatting geen rekening hebben gehouden met wet- en regelgeving en andere beleidsinstrumenten die vanaf juli 2023 zijn of worden ingevoerd. Na een eerste inschattingsronde vond een uitvoerige plenaire bespreking van de resultaten plaats. Hierna kregen de experts de mogelijkheid om – in het geval dat de plenaire bespreking tot nieuwe inzichten had geleid – de eerdere inschatting aan te passen in de tweede inschattingsronde. De resultaten van de tweede (definitieve) inschatting van de weerbaarheid worden weergegeven in tabel 5.2. Hierbij wordt opgemerkt dat het gaat om expertinschattingen en dat de resultaten, hoewel afgerond op gehele getallen, schijnprecisie kunnen suggereren. Vanwege deze reden zijn de resultaten in categorieën gegroepeerd.

Bij drie tf-dreigingen scoort de weerbaarheid tussen de 50 en 60, namelijk bij financiering via girale of contante transacties bij vergunde banken (score 58), met middelen verkregen via horizontale/verticale fraude (score 57) en via girale of contante transacties bij vergunde geldtransactiekantoren (score 54). Dit betekent dat de mitigerende werking van het totale beschikbare beleidsinstrumentarium – volgens experts – bij deze tf-dreigingen relatief groot is. Deze score houdt in dat volgens de experts iets meer dan de helft (respectievelijk 58%, 57% en 54%) van de ingeschatte potentiële impact van deze tf-dreigingen wordt tegengegaan.

De vier tf-dreigingen met de laagste weerbaarheidsscore hebben allen een score lager dan 30. Dit zijn financiering via onvergunde betaaldienstverleners en hawala-bankieren (score 28), met legaal verkregen eigen middelen (score 27), via aanbieders van cryptodiensten (score 25) en via laagdrempelige (*online*) mogelijkheden om buitenlandse bankrekening te openen (score 23). De lage scores houden dus in dat het totale beschikbare beleidsinstrumentarium dat tot en met juni 2023 beschikbaar was en de uitvoering daarvan – volgens experts – tf-dreigingen slechts beperkt tegengaan.

Bij veel van de grootste tf-dreigingen is het zogeheten AIO-principe van toepassing. Dit AIO-principe werd al in de vorige NRA's op het terrein van terrorismefinanciering geïdentificeerd. Het betreft tf-methoden die een of meer van de volgende drie componenten bevatten:

- Anonimiteit: de tf-methode verhuult de identiteit van de financier van terrorisme;
- Internationaal: de tf-methode heeft een internationaal karakter en wordt via of vanuit het buitenland ingezet;
- Ongereguleerd: de tf-methode heeft betrekking op c.q. wordt ingezet in een ongereguleerde sector.

Bij tf-dreigingen waarvoor het AIO-principe in grote mate geldt, is sprake van een relatief lage weerbaarheid van het beleidsinstrumentarium.

Tabel 5.2 Weerbaarheid beleidsinstrumentarium per grootste tf-dreiging (n=6)

Dreiging	Weerbaarheid <i>(op een schaal van 0-100)</i>
Score-categorie '50 of meer'	
Financiering via girale of contante transacties bij vergunde banken	58
Financiering met middelen verkregen via horizontale/verticale fraude	57
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	54
Score-categorie '40 tot en met 49'	
Financiering via internet betaaldiensten (PSP's)	41
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering	41
Score-categorie '30 tot en met 39'	
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	39
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude	36
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	34
Score-categorie '20 tot en met 29'	
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	28
Financiering met legaal verkregen eigen middelen	27
Financiering via aanbieders van cryptodiensten	25
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	23

5.7 Toekomstig beleidsinstrumentarium

De toezichthoudersrol van de AFM en DNB wordt in 2024 naar verwachting uitgebreid als gevolg van de *Markets in Crypto-Assets Regulation (MiCAR)*, het eerste Europese wetgevingspakket voor het reguleren van crypto's en aan crypto's gerelateerde diensten. Deze wet- en regelgeving richt zich op zowel uitgevers van crypto-activa als aanbieders van cryptodiensten en zorgt voor uniforme regels binnen de EU. De MiCAR-verordening is in juni 2023 gepubliceerd. Op het moment van schrijven van deze NRA werkte het ministerie van Financiën aan de implementatie ervan, waarvoor een consultatie voor cryptodienstverleners en uitgevers van cryptoactiva was uitgezet. Het MiCAR-toezicht wordt verdeeld tussen de AFM en DNB:

- de AFM wordt leidend in het toezicht op de *Crypto Asset Service Providers (CASP)* en overige crypto-assets, en in het toezicht op het voorkomen van marktmisbruik;
- DNB wordt leidend in het toezicht op de uitgifte van zogeheten *Stablecoins*, zoals *Asset-Referenced Tokens (ART's)* en *E-Money Tokens (EMT's)*.¹³⁵

¹³⁵ [Markets in Crypto-Assets Regulation \(MiCAR\) \(afm.nl\)](#).

Verder zijn er ten tijde van het schrijven van deze NRA concrete plannen om de advocatuur onder toezicht te stellen van één onafhankelijke landelijke toezichthouder, de nieuw op te richten Onafhankelijke Toezichthouder Advocatuur (OTA). De OTA zal onafhankelijk van zowel de overheid als de beroepsgroep toezicht uitoefenen en handhaven op alle in Nederland ingeschreven advocaten. De OTA wordt een orgaan van de NOvA maar voert als toezichthouder zijn werk onafhankelijk van de advocatuur uit. De nieuwe toezichthouder krijgt één centraal meldpunt waar alle informatie, signalen en klachten over advocaten binnenkomen, en verwijst klachten door naar de lokale dekens voor verdere afhandeling.¹³⁶

Tot slot ligt er momenteel het wetsvoorstel plan van aanpak witwassen voor¹³⁷ dat is ingediend in de Tweede Kamer op 21 oktober 2022. In het wetsvoorstel is een uitbreiding van de mogelijkheden voor informatie-uitwisseling ten behoeve van de poortwachtersfunctie opgenomen en een verbod op contante betalingen voor goederen vanaf €3.000.

5.8 Tot slot

Het beschikbare beleidsinstrumentarium ter voorkoming en bestrijding van terrorismefinanciering omvat alle relevante instrumenten die voortvloeien uit internationale en nationale wet- en regelgeving, wet- en regelgeving op gemeentelijk niveau, sectorale en branchegerichte regelgeving, en regelgeving op organisatieniveau. Ook samenwerkingsverbanden tussen publieke en/of private organisaties en richtlijnen, handreikingen en beleidsplannen van organisaties die een rol spelen bij de preventie en/of bestrijding van terrorismefinanciering, worden in deze NRA gezien als beleidsinstrument. Tabel 5.1 gaf een overzicht van het beleidsinstrumentarium dat tot en met juni 2023 – de maand waarin de derde expertmeeting plaatsvond – beschikbaar was ter preventie en bestrijding van terrorismefinanciering.

Tf-experts hebben in de derde expertmeeting voor de 12 grootste tf-dreigingen in twee rondes met een tussentijdse plenaire discussie een inschatting gemaakt van de mate waarin het totale pakket aan bestaande beleidsinstrumenten de potentiële impact van de dreigingen tegengaat. Bij drie tf-dreigingen scoort de weerbaarheid tussen de 50 en 60, namelijk bij financiering via girale of contante transacties bij vergunde banken, met middelen verkregen via horizontale/verticale fraude en via girale of contante transacties bij vergunde geldtransactiekantoren. Bij deze dreigingen nemen de beschikbare beleidsinstrumenten en de uitvoering daarvan volgens experts iets meer dan de helft van de potentiële impact weg. De vier tf-dreigingen met de laagste weerbaarheidsscore hebben allen een score lager dan 30: financiering via onvergunde betaaldienstverleners en hawala-bankieren, met legaal verkregen eigen middelen, via aanbieders van cryptodiensten en via laagdrempelige (*online*) mogelijkheden om buitenlandse bankrekening te openen.

¹³⁶ [Advocatuur onder toezicht van onafhankelijke landelijke toezichthouder | Nieuwsbericht | Rijksoverheid.nl](#).

¹³⁷ [Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme in verband met het verbod op contante betalingen voor goederen vanaf €3.000 en het uitbreiden van de mogelijkheden voor informatie-uitwisseling ten behoeve van de poortwachtersfunctie \(Wet plan van aanpak witwassen\) | Tweede Kamer der Staten-Generaal](#).

Ondanks de mitigerende werking van het beschikbare instrumentarium op de 12 grootste tf-dreigingen, kunnen deze dreigingen dus nog steeds in meer of mindere mate impact hebben. De mitigerende werking hangt samen met de mate waarin het AIO-principe van toepassing is op de tf-dreigingen. Bij de meeste tf-methoden zijn één of meer van de drie AIO-componenten van toepassing. Hoe meer de AIO-elementen van toepassing zijn bij de tf-dreigingen, hoe lager de weerbaarheid van het beleidsinstrumentarium ter preventie en repressie van de dreigingen.

6 Conclusies

Dit slothoofdstuk beschrijft allereerst de belangrijkste resultaten van deze derde NRA op het terrein van terrorismefinanciering, waarbij de beantwoording van de onderzoeksvragen centraal staat. In het kader van het groeimodel van de NRA-onderzoeksmethodiek wordt de uitvoering van deze NRA vervolgens geëvalueerd, waarbij zowel de sterke punten als de verbeterpunten van de gehanteerde onderzoeksmethodiek worden belicht. Tot slot komen enkele geleerde lessen aan bod waarvan gebruikgemaakt kan worden bij de vormgeving van een volgende NRA.

6.1 Beantwoording van onderzoeksvragen

Onderzoeksvraag 1: Welke contextfactoren van Nederland zijn (mogelijk) van invloed op de prevalentie van terrorismefinanciering, de potentiële impact daarvan en de keuze van personen voor de door hen in te zetten financieringsmethoden of te gebruiken financieringsbronnen?

Net als voor de eerdere NRA's op het terrein van terrorismefinanciering is een contextanalyse uitgevoerd waarbij is ingegaan op de specifieke kenmerken van Nederland die van invloed kunnen zijn op de prevalentie van terrorismefinanciering in Nederland en de potentiële impact daarvan. Deze factoren kunnen een rol spelen bij de bepaling van de in te zetten financieringsmethoden en de te gebruiken financieringsbronnen. Binnen de contextanalyse is gekeken naar de geografische, demografische, religieuze, sociaal-culturele, politieke, economische en criminologische kenmerken van Nederland.

Volgens de AIVD en de NCTV is de internationale jihadistische beweging één van de belangrijkste terroristische dreigingen tegen Nederland. Jihadisten claimen de islam om hun overtuigingen en manier van leven met geweld op te leggen aan anderen. Naar schatting hangen in Nederland zo'n 500 mannen en vrouwen het jihadistisch gedachtegoed aan. Vanwege deze relatie tussen de islam, terrorisme en de financiering daarvan is ingegaan op enkele religieuze kenmerken van Nederland. Circa één op de twintig Nederlanders is islamitisch en daarvan is één op de vijf dermate religieus dat zij ten minste eenmaal per week de moskee bezoeken. Ten tijde van de vorige NRA Terrorismefinanciering meldde de AIVD dat er verhoudingsgewijs veel Nederlandse jihadisten van onder meer Marokkaanse en Turkse afkomst waren. Ongeveer één op de zeven Nederlanders blijkt een niet-westerse migratieachtergrond te hebben en Turkije en Marokko behoren tot de grootste migratielanden. Na de 9/11 aanslagen en andere aanslagen in Europa is in Nederland de tolerantie en het gedogen ten opzichte van moslims afgenomen. Enerzijds kan deze verminderde tolerante houding leiden tot rechtsextremistische acties – en in zijn uiterste vorm terroristische daden – gericht op moslims. Anderzijds kan de verminderde tolerante houding ten opzichte van moslims aanleiding zijn voor jihadisten om terroristische activiteiten in ons land te plegen.

Nederland kenmerkt zich door een grote en internationaal georiënteerde financiële sector. Personen, groepen personen of organisaties die terrorisme financieren, kunnen op verschillende manieren gebruikmaken van het financiële stelsel in Nederland. Geldtransacties kunnen contant of op girale wijze via vergunde banken of betaaldienstverleners (geldtransactiekantoren of internet betaaldiensten) plaatsvinden.

Ook crypto's bieden mogelijkheden voor terrorismefinanciering. Het zonder grenscontroles reizen van personen in het Schengen gebied en vrij verkeer van personen, goederen, diensten en kapitaal tussen de EER-landen maken verhulling van een criminele oorsprong van vermogen mogelijk, omdat dit het volgen van de *paper trail* van transacties bemoeilijkt dan wel onmogelijk maakt. Ook maakt het fysieke verplaatsing over land van contant geld en grootwaardeproducten zonder grenscontroles binnen de EER mogelijk.

Het feit dat Nederland een open, op handel gerichte economie heeft en één van de grootste exporteurs ter wereld is, kan van invloed zijn op de prevalentie van terrorismefinanciering via fysieke verplaatsing van contant geld of grootwaardeproducten binnen, via, vanuit of naar Nederland. De toegangshavens tot Nederland kunnen worden gebruikt bij de import en export van legale goederen en illegale goederen als drugs. In Nederland is sprake van een breed palet aan misdrijven, waarvan de criminele opbrengsten gebruikt kunnen worden voor de financiering van terrorisme. Het gaat om vermogensmisdrijven waaronder vormen van fraude maar ook diefstal/verduistering en inbraak, drugsmisdrijven, vuurwapenmisdrijven, misdrijven met betrekking tot mensenhandel en mensensmokkel en cybercriminaliteit.

Tot slot is er de afgelopen jaren sprake van een versplintering in de Nederlandse politiek die gepaard gaat met verslechterde omgangsvormen in het parlement, waarin polarisatie, extreme uitingen en verharding in politieke debatten in toenemende mate als problematisch worden gezien. De gevolgen van deze polarisatie werken door in de Nederlandse samenleving. Eind 2022 maakte circa driekwart van de Nederlandse bevolking zich zorgen over toenemende tegenstellingen en meningsverschillen tussen burgers met verschillende politieke opvattingen. Deze toenemende onenigheid kan extremisme aanwakkeren. Volgens de AIVD kan extremisme in zijn uiterste vorm tot terrorisme leiden.

Onderzoeksvraag 2: wat zijn de aard, mechanismen en potentiële impact van de grootste tf-dreigingen?

De NRA legt de focus op 12 tf-dreigingen die – volgens tf-experts – de grootste potentiële impact hebben. Deze dreigingen zijn geselecteerd uit een longlist van 27 dreigingen. Omdat de 12 grootste tf-dreigingen qua potentiële impact niet veel uiteenlopen, worden deze in tabel 6.1 gecategoriseerd weergegeven. De omvang van de potentiële impact van de dreigingen is bepaald door de uitvoering van een MCA. Experts maakten aan de hand van de criteria 'prevalentie terroristische activiteiten in Nederland', 'prevalentie terroristische activiteiten in het buitenland', 'aantasting financiële sector', 'vermindering subjectieve veiligheid', 'ondermijning gezag' en 'aantasting imago Nederland in het buitenland' voorlopige kwantitatieve inschattingen. In een plenaire discussie werden deze inschattingen verantwoord en onderbouwd wat bij de experts aanleiding kon geven tot aanpassing van de voorlopige inschattingen. In een tweede ronde maakten de experts hun definitieve kwantitatieve inschatting die uiteindelijk de hoogte van de potentiële impact van de afzonderlijke tf-dreigingen bepaalden.

De dreiging 'financiering via onvergunde betaaldienstverleners en hawala-bankieren' kreeg van de 12 dreigingen de hoogste score, namelijk een score van 61 op een schaal van 0-100. Het laagst in deze lijst met grootste tf-dreigingen staat 'financiering via aanbieders van cryptodiensten' (score 48). Onderstaande tabel maakt duidelijk dat de

potentiële impact van de 12 dreigingen niet in sterke mate van elkaar verschilt (de scores liggen immers tussen 48 en 61).

De tf-dreigingen in tabel 6.1 betreffen financieringsmethoden en -bronnen die in verschillende combinaties van twee of meerdere dreigingen een tf-constructie kunnen vormen. Zo'n constructie kan vrij eenvoudig van aard zijn, maar kan ook een complex karakter hebben. In hoofdstuk 4 van dit rapport is voor elk van de 12 grootste tf-dreigingen ingegaan op de aard en mechanismen van de dreiging.

Tabel 6.1 Potentiële impact grootste tf-dreigingen (n=8)

Dreiging	Potentiële impact (op een schaal van 0-100)
Score-categorie '60 of meer'	
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	61
Score-categorie '55 tot en met 59'	
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	58
Financiering met middelen verkregen via horizontale/verticale fraude	57
Financiering via girale of contante transacties bij vergunde banken	57
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering	56
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	55
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	55
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude	55
Score-categorie '50 tot en met 54'	
Financiering met legaal verkregen eigen middelen	50
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	50
Financiering via internet betaaldiensten (PSP's)	50
Score-categorie 'minder dan 50'	
Financiering via aanbieders van cryptodiensten	48

Onderzoeksvraag 3: welke tf-dreigingen zijn in Nederland nog niet gesignaleerd maar zouden in de toekomst actueel kunnen worden?

In de expertmeetings en verdiepende interviews met experts lag de focus op tf-dreigingen die op dit moment spelen. In de FANO-enquête is wel expliciet gevraagd naar toekomstige tf-dreigingen. Acht respondenten hebben deze vraag beantwoord. Enkele toekomstige dreigingen hadden niet zozeer betrekking op terrorismefinanciering maar op terrorisme, bijvoorbeeld een terroristische dreiging vanuit rechts-extremistische of anti-overheid-/anti-democratische hoek. Ook werd de financiering van *foreign terrorist fighters* in nieuwe strijd- of oorlogsgebieden als toekomstige dreiging genoemd. Verder werden de dreiging van aanslagen op asielzoekerscentra of vluchtelingenopvangcentra, de dreiging van aanslagen op de

vitale infrastructuur, de dreiging richting bewindslieden vanuit een maatschappelijk ongenoegen en de dreiging van (inter)nationale ontduiking van sanctieregelingen met betrekking tot gesanctioneerde personen en organisaties genoemd. Er zijn echter ook specifieke methoden en bronnen van terrorismefinanciering genoemd die zich in de toekomst voor kunnen doen. Genoemde tf-dreigingen zijn de financiering via culturele artefacten (meer specifiek: archeologische vondsten in bijvoorbeeld Arabische en Afrikaanse landen), handel in bijzondere ertsen en grondstoffen en wapenhandel. In de validerende interviews, die zijn uitgevoerd ten tijde van de oorlog tussen Israël en Hamas, is enkele malen benoemd dat in de nabije toekomst terrorismefinanciering via crypto's een meer prominente tf-dreiging zou kunnen worden. Van Hamas is bekend dat financiering via crypto-transacties een belangrijke inkomstenbron is.

Onderzoeksvraag 4: welk beleidsinstrumentarium is in Nederland beschikbaar ter preventie en bestrijding van de grootste tf-dreigingen?

Het beschikbare beleidsinstrumentarium ter voorkoming en bestrijding van terrorismefinanciering omvat alle relevante instrumenten die voortvloeien uit internationale en nationale wet- en regelgeving, wet- en regelgeving op gemeentelijk niveau, sectorale en branchegerichte regelgeving, en regelgeving op organisatieniveau. In deze NRA worden ook samenwerkingsverbanden tussen publieke en/of private organisaties en richtlijnen, handreikingen en beleidsplannen van organisaties die een rol spelen bij de preventie en/of bestrijding van terrorismefinanciering, gezien als beleidsinstrument.

Tabel 6.2 geeft een overzicht van het beleidsinstrumentarium dat tot en met juni 2023 – de maand waarin de derde expertmeeting plaatsvond – beschikbaar was ter preventie en bestrijding van terrorismefinanciering. In hoofdstuk 5 zijn deze beleidsinstrumenten nader toegelicht.

Tabel 6.2 Beleidsinstrumentarium ter preventie en bestrijding van terrorismefinanciering

Internationale wet- en regelgeving	Nationale wet- en regelgeving	Overige beleidsinstrumenten
<ul style="list-style-type: none"> • FATF-aanbevelingen • EU anti-witwasrichtlijnen • Verenigde Naties Veiligheidsraad Resoluties en EU Verordeningen • Overige internationale sanctielijsten • Europese verordening Aangifte liquide middelen • <i>Wire Transfer Regulation 2</i> 	<ul style="list-style-type: none"> • Wet ter voorkoming van witwassen en financieren van terrorisme • Sanctiewet 1977 en sanctieregelingen • Wetboek van Strafrecht • Wetboek van Strafvordering • Wet op de inlichtingen- en veiligheidsdiensten 2017 • Tijdelijke wet bestuurlijke maatregelen terrorismebestrijding • Wet precursoren voor explosieven • Wet op het financieel toezicht • Algemene Douanewet • Wet controle op rechtspersonen • Handelsregisterwet 2007 (inclusief UBO-registers) • Fiscale wetgeving • Sociale wetgeving • Wet op de economische delicten • Wet Bibob 	<ul style="list-style-type: none"> • Nationale samenwerkingsverbanden • Internationale samenwerkingsverbanden • Sectorale regelgeving en voorwaarden • Richtlijnen, handreikingen en beleidsplannen

Onderzoeksvraag 5: wat is de weerbaarheid van het beschikbare beleidsinstrumentarium ter preventie en bestrijding van de grootste tf-dreigingen?

Tf-experts hebben voor de 12 grootste tf-dreigingen in twee rondes met een tussentijdse plenaire discussie een inschatting gemaakt van de mate waarin het totale pakket aan bestaande beleidsinstrumenten de potentiële impact van de dreigingen tegengaat. De resultaten van de expertmeeting worden gecategoriseerd weergegeven in tabel 6.3. Experts zijn bij hun inschatting van de weerbaarheid van het beleidsinstrumentarium uitgegaan van de beleidsinstrumenten die op dat moment (juni 2023) waren geïmplementeerd.

Tabel 6.3 Weerbaarheid beleidsinstrumentarium per grootste tf-dreiging (n=6)

Dreiging	Weerbaarheid <i>(op een schaal van 0-100)</i>
Score-categorie '50 of meer'	
Financiering via girale of contante transacties bij vergunde banken	58
Financiering met middelen verkregen via horizontale/verticale fraude	57
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	54
Score-categorie '40 tot en met 49'	
Financiering via internet betaaldiensten (PSP's)	41
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering	41
Score-categorie '30 tot en met 39'	
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	39
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude	36
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	34
Score-categorie '20 tot en met 29'	
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	28
Financiering met legaal verkregen eigen middelen	27
Financiering via aanbieders van cryptodiensten	25
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	23

Bij drie tf-dreigingen oordelen de experts dat de weerbaarheid van het beleidsinstrumentarium de potentiële impact met meer dan de helft tegengaat (scores groter dan 50), namelijk bij financiering via girale of contante transacties bij vergunde banken (score 58), met middelen verkregen via horizontale/verticale fraude (score 57) en via girale of contante transacties bij vergunde geldtransactiekantoren (score 54). De vier tf-dreigingen met de laagste weerbaarheidsscore hebben allen een score lager dan 30: financiering via onvergunde betaaldienstverleners en hawala-bankieren (score 28), met legaal verkregen eigen middelen (score 27), via aanbieders van cryptodiensten (score 25) en via laagdrempelige (*online*) mogelijkheden om buitenlandse bankrekening te openen (score 23). De lage scores houden dus in dat het totale beleidsinstrumentarium deze tf-dreigingen – volgens experts – slechts in relatief beperkte mate tegengaat. Tabel 6.3 laat zien dat de weerbaarheid van het beleidsinstrumentarium sterk kan verschillen tussen de 12 grootste tf-dreigingen (de scores liggen namelijk tussen 23 en 58).

Ondanks de mitigerende werking van het beschikbare instrumentarium op de 12 grootste tf-dreigingen, kunnen deze dreigingen dus nog steeds in meer of mindere mate impact hebben. De mitigerende werking hangt samen met de mate waarin het

AIO-principe¹³⁸ (zie hoofdstuk 5) van toepassing is op de tf-dreigingen. Bij de meeste tf-methoden zijn één of meer van de drie AIO-componenten van toepassing. Hoe meer de AIO-elementen van toepassing zijn bij de tf-dreigingen, hoe lager de weerbaarheid van het beleidsinstrumentarium ter preventie en repressie van de dreigingen.

Onderzoeksvraag 6: wat zijn de grootste tf-risico's in Nederland wanneer rekening wordt gehouden met potentiële impact en weerbaarheid?

In figuur 6.1 worden in een *heatmap* de expertinschattingen van de potentiële impact en de weerbaarheid van het beleidsinstrumentarium voor de 12 grootste dreigingen tegen elkaar afgezet. De hoogste risico's zijn de dreigingen met een hoge potentiële impact en waarbij sprake is van een lage weerbaarheid van het beschikbare beleidsinstrumentarium. Deze *heatmap* kan worden gezien als samenvatting van de derde NRA Terrorismefinanciering. Wel dient hierbij in ogenschouw te worden gehouden dat de *heatmap* alleen de grootste tf-dreigingen weergeeft en dat de andere dreigingen uit de longlist door de experts als lager risico worden gezien.

De figuur maakt duidelijk dat het risiconiveau van de 12 grootste tf-dreigingen niet sterk van elkaar afwijkt. Dit geldt met name voor de potentiële impactscores die uiteenlopen van 48 tot 61. De weerbaarheid tegen de dreigingen laat een grotere spreiding zien. Alle dreigingen bevinden zich in de figuur in het oranje gebied.¹³⁹ Van al deze risicovolle tf-dreigingen¹⁴⁰ hebben de volgende twee dreigingen het hoogste risiconiveau (het meest linksboven in de figuur weergegeven):

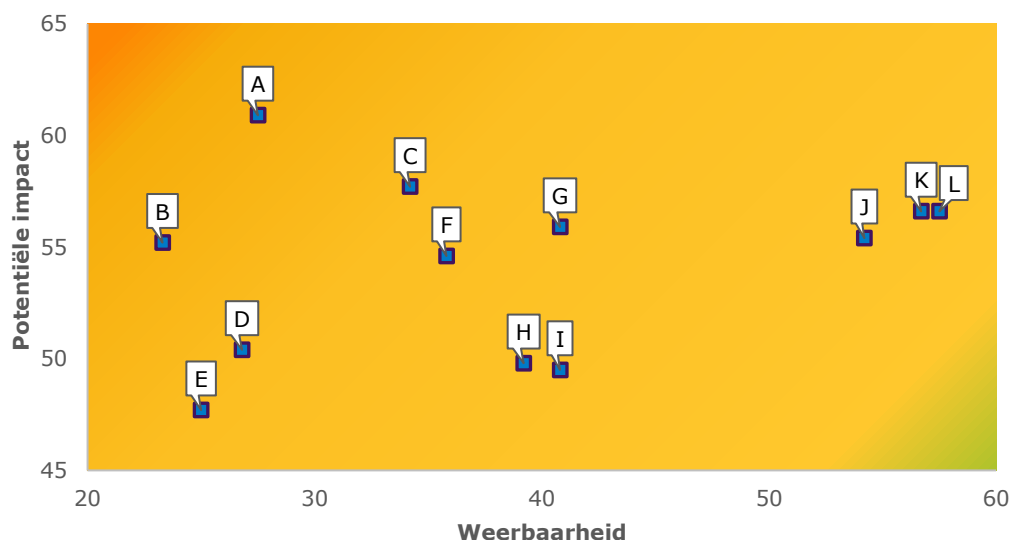
- *Financiering via onvergonde betaaldienstverleners en hawala-bankieren (A in figuur 6.1)*. Met name door een laag ingeschatte weerbaarheid heeft deze tf-dreiging zo'n hoog risiconiveau. De dreiging biedt – volgens het AIO-principe – mogelijkheden om op anonieme wijze geld over te maken, heeft een internationaal karakter en wordt veelal via en/of naar het buitenland ingezet, en heeft betrekking op een ongereguleerde 'sector'. Verder is deze tf-methode relatief eenvoudig toegankelijk voor individuen, groepen en/of organisaties die terrorisme willen financieren.
- *Financiering via laagdrempelige (online) mogelijkheden om een buitenlandse bankrekening te openen (B)*. Bij deze tf-dreiging wordt het hoge risiconiveau met name door een zeer laag ingeschatte weerbaarheid veroorzaakt. Dit is te relateren aan het feit dat sommige online buitenlandse bankrekeningen relatief eenvoudig – met, afhankelijk van het land, mogelijk minder strenge tf-regelgeving en -toezicht ten aanzien van financiële dienstverleners – geopend kunnen worden en dat er momenteel geen beleidsinstrumentarium bestaat om dit aan te pakken. Zodra iemand eenmaal beschikt over een buitenlandse bankrekening, kan hij of zij transacties naar, via of vanuit deze rekening laten lopen, die minder inzichtelijk zijn voor Nederlandse banken en opsporingsdiensten die daardoor over een minder goede informatiepositie beschikken.

¹³⁸ AIO staat voor Anonimiteit (de methode verhult de identiteit van de financier van terrorisme), Internationaal (de methode heeft een internationaal karakter en wordt via of vanuit het buitenland ingezet) en Ongereguleerd (de methode heeft betrekking op c.q. wordt ingezet in een ongereguleerde sector).

¹³⁹ Om zo duidelijk mogelijk de verschillen in beeld te brengen is de weergegeven figuur een uitsnede uit een figuur met assen die lopen van 0 tot en met 100, waarbij de kleuren verlopen van linksboven: rood (hoogste potentiële impact en laagste weerbaarheid) naar rechtsonder: groen (laagste potentiële impact en hoogste weerbaarheid). De volledige *heatmap* met assen van 0 tot en met 100 is te vinden in bijlage 8.

¹⁴⁰ Dit betreft een *overall* risicoanalyse. Niet voor iedere partij binnen een risicovolle sector geldt een hoog risiconiveau. Wwft-poortwachters dienen nader cliëntonderzoek te verrichten om een goed beeld te verkrijgen van het daadwerkelijke risiconiveau ten aanzien van terrorismefinanciering.

Figuur 6.1 Heatmap derde NRA: potentiële impact afgezet tegen weerbaarheid voor de grootste tf-dreigingen



A	Onvergonde betaaldienstverleners en hawala-bankieren	G	Stichtingen met weinig transparantie over financiën en geen zelfregulering
B	Laagdrempelige (<i>online</i>) mogelijkheden openen buitenlandse bankrekening	H	Giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media
C	Fysieke verplaatsing (grote hoeveelheden) contant geld/grootwaardeproducten	I	Internet betaaldiensten (PSP's)
D	Legaal verkregen eigen middelen	J	Girale/contante transacties vergunde geldtransactiekantoren
E	Aanbieders cryptodiensten	K	Middelen verkregen via horizontale/verticale fraude
F	Middelen verkregen via andere criminaliteitsvorm dan fraude	L	Girale/contante transacties bij vergunde banken

Van de 12 grootste tf-dreigingen ligt het minst hoge risiconiveau bij de drie tf-dreigingen die het meest rechtsonder in de figuur staan: financiering via internet betaaldiensten (PSP's) (I), via girale/contante transacties bij vergunde geldtransactiekantoren (J), via middelen verkregen via horizontale/verticale fraude (K) en via girale/contante transacties bij vergunde banken (L). Hoewel bij deze dreigingen nog steeds sprake is van een aanzienlijk risiconiveau, wordt hun risiconiveau verhoudingsgewijs het laagst ingeschat. Dat relatief lage risiconiveau wordt met name veroorzaakt door de hoog ingeschatte weerbaarheid, wat te relateren is aan de verbetering van het cliëntonderzoek en transactiemonitoring in de afgelopen jaren door zowel vergunde banken als vergunde geldtransactiekantoren.

In tegenstelling tot de vorige NRA wordt deze derde NRA voor terrorismefinanciering niet afgesloten met de RPI-scores (Resterende Potentiële Impact) van de grootste dreigingen. De reden is dat niet uitgesloten kan worden dat bij het bepalen van de potentiële impact van de grootste dreigingen, ook rekening is gehouden met de weerbaarheid (of een gebrek daaraan) van het beleidsinstrumentarium. Dit kan per dreiging verschillend uitpakken. Dit neemt niet weg dat de RPI-scores indicatief zijn

voor de ernst van de dreigingen. De RPI-scores bepalen dan ook de volgorde van de legenda van de dreigingen in de *heatmap*. De RPI-scores van de 12 grootste dreigingen op het gebied van terrorismefinanciering worden gerapporteerd in bijlage 8.

Onderzoeksvraag 7: wat zijn concrete, recente voorbeelden van de grootste tf- risico's?

Het voert te ver om hier opnieuw de concrete, recente voorbeelden van de grootste tf-
risico's weer te geven. Verwezen wordt naar hoofdstuk 4 van dit rapport, waarin
uitgebreid is ingegaan op de aard en mechanismen van de 12 grootste tf-dreigingen.
Daarbij is, ter illustratie en uitleg van de wijze waarop deze dreigingen gestalte
kunnen krijgen, voor een beperkt aantal dreigingen recente casuïstiek opgenomen.

Onderzoeksvraag 8: welke verbeterpunten zijn te benoemen voor volgende NRA's?

Deze onderzoeksvraag wordt in onderstaande paragrafen van dit hoofdstuk uitvoerig
beantwoord. Allereerst worden de sterke punten en aandachtspunten van de in deze
NRA gehanteerde onderzoeksmethodiek belicht. Vervolgens worden enkele geleerde
lessen beschreven, waarmee bij de uitvoering van een volgende NRA rekening
gehouden kan worden.

6.2 Evaluatie van de derde NRA

In hoofdstuk 2 is uitvoerig beschreven op welke wijze deze derde NRA is uitgevoerd.
De gekozen aanpak bouwt voort op de ervaringen uit de eerdere NRA's en past binnen
het gekozen groeimodel voor methodologieontwikkeling van de Nederlandse NRA's.
Om te kunnen leren van de opgedane ervaringen is geprobeerd zo transparant
mogelijk te rapporteren en is de zelfevaluatie uitgevoerd die in deze paragraaf wordt
beschreven.

Evenals in de vorige NRA's is de toegepaste onderzoeks aanpak gestructureerd aan de
hand van het ISO 31000 kader voor risicomanagement. Kort samengevat komt de
gehanteerde onderzoeksmethodiek neer op het volgende:

- Een contextanalyse waarin de specifieke kenmerken van Nederland zijn geschetst die van invloed kunnen zijn op de prevalentie van terrorismefinanciering en de potentiële impact daarvan. Deze factoren kunnen een rol spelen bij het bepalen van de in te zetten financieringsmethoden en de te gebruiken financieringsbronnen. Voor deze contextanalyse is een literatuurstudie verricht en zijn relevante kwantitatieve databronnen geraadpleegd.
- Ten behoeve van een inventarisatie van tf-dreigingen zijn recente (sinds 2020 verschenen) rapporten bestudeerd, waaronder de Europese SNRA, en is de FANO-enquête uitgezet onder publieke en private partijen met een taak bij de preventie en/of bestrijding van terrorismefinanciering.
- In de eerste expertmeeting hebben vertegenwoordigers van expertorganisaties de tf-dreigingen met de volgens hen grootste potentiële impact geïdentificeerd.
- In de periode na de eerste expertmeeting is in verdiepende interviews met vertegenwoordigers van expertorganisaties en andere partijen met een taak bij het tegengaan van terrorismefinanciering nader ingegaan op de aard, mechanismen en casuïstiek van de dreigingen die op de voorlopige shortlist van grootste tf-dreigingen stonden.
- In de tweede expertmeeting is – naar aanleiding van de bevindingen van de interviews – de shortlist van grootste tf-dreigingen in samenspraak met de experts

aangepast en vastgesteld, waarna de experts de potentiële impact van de dreigingen hebben ingeschat aan de hand van een MCA.

- In de derde expertmeeting hebben experts voor elk van de grootste tf-dreigingen de weerbaarheid van het totale beschikbare beleidsinstrumentarium ingeschat.
- Door de ingeschatte potentiële impact van de tf-dreigingen af te zetten tegen de ingeschatte weerbaarheid is inzicht verkregen in het risiconiveau van de grootste tf-dreigingen. Voor alle 12 dreigingen zijn bij een aantal publieke organisaties dataverzoeken ingediend en zijn zoveel mogelijk beschikbare kwantitatieve data evenals recente casuïstiek opgenomen in de rapportage.
- Tot slot zijn in de eindfase van het onderzoek de resultaten van de NRA gevalideerd. Hiertoe is nagegaan in welke mate de resultaten van de qua strekking overlappende grootste dreigingen tussen de derde NRA voor terrorismefinanciering en de parallel uitgevoerde derde NRA voor witwassen corresponderen. Hiertoe is de samenhang tussen de RPI-scores bepaald (zie bijlage 8). Ook zijn validerende interviews met acht experts werkzaam bij zes sleutelorganisaties afgenomen met als belangrijkste doel na te gaan in hoeverre zij het risiconiveau van de 12 grootste tf-dreigingen herkennen.

Sterke punten

Ten aanzien van de uitvoering van deze derde NRA is een aantal sterke punten te benoemen, waarvan een deel ook al in de vorige NRA's Terrorismefinanciering is genoemd:

- *Transparante beschrijving van de toegepaste methodologie.* De toegepaste methodologie, waaronder de wijze van dataverzameling en de toegepaste MCA, is transparant beschreven met het oog op het groeimodel van de NRA (leren van ervaringen) en een verdere aanscherping van de toegepaste methodologie. Beoogd is de reproduceerbaarheid van het onderzoek te maximaliseren.
- *Nauwe betrokkenheid van het veld.* Alle relevante organisaties die op een bepaalde manier een rol spelen bij de preventie en/of repressie van terrorismefinanciering, zijn op één of meerdere momenten betrokken bij het onderzoek. In deze derde NRA zijn publieke en private partijen in nog grotere mate betrokken dan bij de eerdere NRA's. Dit is gerealiseerd op de volgende manieren:
 - een kick-off bijeenkomst aan het begin van het onderzoek;
 - een groter aantal publieke en private partijen dat voor de FANO-enquête is uitgenodigd (39 organisaties in deze NRA ten opzichte van 33 organisaties in de tweede NRA Terrorismefinanciering);
 - een groter aantal publieke en private partijen waarmee een verdiepend interview plaatsvond (27 organisaties in deze NRA ten opzichte van 21 organisaties in de tweede NRA Terrorismefinanciering).
 - een grotere rol van experts in de derde expertmeeting bij het vaststellen van de criteria die onderdeel zijn van de MCA (naar aanleiding van een geleerde les van de vorige NRA Terrorismefinanciering, zie ook hoofdstuk 1).
- *Stringent uitnodigingsbeleid expertmeetings.* Voor de expertmeetings werden vertegenwoordigers van expertorganisaties uitgenodigd die beschikten over de deskundigheid en ervaring om de belangrijkste tf-dreigingen te kunnen overzien. Ten opzichte van de vorige NRA's is er een stringenter uitnodigingsbeleid voor de expertmeetings gehanteerd, met als doel om het expertiseniveau van de deelnemers zo hoog mogelijk te krijgen. De uitnodiging van de acht deelnemers voor de expertmeetings vond plaats op basis van de resultaten van de FANO-enquête, waarbij de eigen ervaring van organisaties met meerdere tf-feiten/-casus leidend was. Dit zorgde ervoor dat aan de expertmeetings alleen

vertegenwoordigers van organisaties deelnamen die ervaring hadden met casuïstiek van één of meerdere tf-dreigingen.

- *Grote meerwaarde van het toegepaste Group Decision Support System (GDSS)*. De GDSS vereenvoudigt het verzamelen van data en zorgt ervoor dat de cijfermatige inschattingen van alle deelnemende experts meegenomen worden waarmee dus ook alle relevante invalshoeken in de uiteindelijke risicoanalyse worden meegenomen. De GDSS is in vergelijking met een 'gewone' bijeenkomst tijdsefficiënt, creëert de mogelijkheid voor verdieping van de resultaten door middel van plenaire discussies en draagt eraan bij dat experts actief blijven deelnemen aan de bijeenkomst (door de afwisseling van groepsdiscussie en het aanleveren van inschattingen/oordelen op een laptop).
- *Structureerende werking van MCA*. De MCA werd uitgevoerd in de GDSS-omgeving en droeg bij aan het structureren van de tweede expertmeeting, de dataverzameling en de transparantie van de resultaten en de wijze waarop de resultaten zijn behaald. In de MCA is gebruikgemaakt van vooraf – in samenspraak met de deelnemers – vastgestelde criteria aan de hand waarvan de experts de potentiële impact van de grootste tf-dreigingen beoordeelden. Door bij het beoordelen van de ernst van de tf-dreigingen gebruik te maken van vooraf gedefinieerde criteria en de experts *per criterium* scores te laten toekennen aan de 12 tf-dreigingen (en niet *per dreiging* alle criteria te laten scoren) ontstond er voor de experts minder ruimte hun eventuele belangenposities te laten meewegen en de uiteindelijke MCA-resultaten in een bepaalde richting te sturen.
- *Delphi-methode belangrijk bij risicoanalyse*. De Delphi-methode werd ingezet bij het identificeren van de grootste tf-dreigingen, het bepalen van de potentiële impact van de dreigingen en het inschatten van de weerbaarheid van het beleidsinstrumentarium. In twee rondes met een tussentijdse groepsdiscussie konden experts hun keuzes dan wel inschattingen motiveren en onderbouwen. Naar aanleiding van de groepsdiscussie stelden experts in de eerste expertmeeting hun aanvankelijke oordelen zodanig bij dat enkele tf-dreigingen die na de eerste identificatieronde buiten de lijst van grootste tf-dreigingen waren gebleven, alsnog een plaats in die lijst bereikten. Bij de tweede en derde expertmeeting konden experts in een tweede ronde hun eerste inschattingen van de potentiële impact en weerbaarheid naar aanleiding van de plenaire discussie aanpassen.
- *Validatie resultaten NRA*. In de eindfase van de NRA zijn de resultaten van de NRA gevalideerd door 1) voor de acht qua strekking overlappende dreigingen van de derde NRA voor terrorismefinanciering en de derde NRA voor witwassen de samenhang van de RPI-scores te bepalen (zie bijlage 8, tabel B8.1), en 2) validerende interviews af te nemen. De RPI-scores voor de dreigingen die zowel in de NRA voor terrorismefinanciering als de NRA witwassen naar voren komen als grootste dreigingen, blijken in hoge mate te corresponderen.¹⁴¹ Hiernaast leidden de validerende interviews bij acht experts werkzaam bij zes sleutelorganisaties tot een bevestiging van de resultaten van de NRA. De experts erkenden in grote mate het risiconiveau van de 12 grootste tf-dreigingen.

Daarnaast kunnen enkele andere sterke punten van deze NRA worden benoemd die volgden uit de geleerde lessen van de tweede NRA en de aanbevelingen uit het *Mutual Evaluation Report* van de FATF:

- *Onderbouwing FANO-enquête*. De FANO-enquête is ten opzichte van de vorige NRA versterkt door in de enquête nog explicieter te vragen naar de eigen praktijkkennis van (vertegenwoordigers van) organisaties met de prevalentie van de tf-dreigingen

¹⁴¹ Pearsons R = 0,92, p = 0,001, N = 8. Zie bijlage 8 voor nadere informatie.

in de longlist. Indien een respondent aangaf bekend te zijn met feiten/casus van een bepaalde tf-dreiging, is gevraagd naar een beknopte toelichting op casuïstiek. Dit zorgde voor meer onderbouwing van de antwoorden van respondenten en maakte nog beter inzichtelijk welke respondenten wel/niet over relevante tf-expertise beschikten. Een andere doorgevoerde aanpassing ten aanzien van de enquête is het praktische punt dat deze *online* is uitgezet. Dit maakte het voor respondenten naar verwachting eenvoudiger om de enquête in te vullen dan de mailenquête die bij de vorige NRA's is toegepast.

- *Nadere specificatie tf-dreigingen.* In deze NRA is op verschillende manieren aandacht besteed aan een nadere specificering van de tf-dreigingen om verfijning in de risicobepaling mogelijk te maken. Dit leidde tot een uitbreiding van de longlist van tf-dreigingen ten behoeve van de FANO-enquête tot 28 dreigingen. In de tweede NRA bestond de FANO-longlist uit 23 dreigingen. Ook was er expliciete aandacht voor de specificering van de tf-dreigingen in de expertmeetings en verdiepende interviews.
- *Meer kwantitatieve data.* In deze NRA zijn bij de beschrijving van contextuele factoren (hoofdstuk 3) en de 12 grootste tf-dreigingen (hoofdstuk 4) in grotere mate dan in de tweede NRA Terrorismefinanciering relevante kwantitatieve databronnen betrokken. Het gaat om:
 - data uit recente Jaaroverzichten van de FIU-Nederland;
 - door het OM – op verzoek van het WODC – verstrekte gegevens over het aantal afgeronde zaken met een onherroepelijke uitspraak en het aantal lopende zaken;
 - door DNB – op verzoek van het WODC – verstrekte data over de actuele aantallen van de diverse typen van financiële instellingen die in Nederland opereren met een geldige Nederlandse of buitenlandse vergunning;
 - door Justis/TRACK – op verzoek van het WODC – verstrekte data over stichtingen in Nederland;
 - door de FIOD – op verzoek van het WODC – verstrekte informatie over het aantal onderzoeken met betrekking tot de 12 grootste tf-dreigingen (evenals informatie over casuïstiek met betrekking tot FIOD-projecten).

Bij al deze partijen, evenals bij het FEC, heeft het WODC dataverzoeken ingediend, waarbij gevraagd werd (kwantitatieve) data aan te leveren over elk van de 12 grootste tf-dreigingen. Op het niveau van de dreigingen heeft dit echter slechts in zeer beperkte mate kwantitatieve data opgeleverd. Alleen Justis/TRACK en de FIOD leverden kwantitatieve data met betrekking tot de dreigingen. De verzamelde informatie was wel behulpzaam bij het beschrijven van de context waarbinnen de dreigingen plaatsvinden, de aard en mechanismen van de dreigingen en het verkrijgen van inzicht in ervaringen van organisaties met de dreigingen.

Aandachtspunten

Net als bij de eerdere NRA's zijn er ook aandachtspunten waarmee rekening gehouden moet worden bij het op waarde schatten van de resultaten van de NRA. Deze aandachtspunten zijn grotendeels inherent aan de gekozen aanpak en kwamen om die reden ook al bij de vorige NRA's naar voren. In de keuze voor de toegepaste onderzoeksmethodologie is geprobeerd een zorgvuldige afweging te maken van zowel de voor- als nadelen die te verbinden zijn aan onderzoeksinstrumenten.

De NRA is met name gebaseerd op de oordelen en inschattingen van vertegenwoordigers van expertorganisaties. Hoewel geprobeerd is in de gekozen onderzoeks aanpak de voorwaarden voor een betrouwbare dataverzameling te optimaliseren, kan niet worden uitgesloten dat bij het identificeren van de grootste tf-

dreigingen, het inschatten van de potentiële impact daarvan en het beoordelen van de weerbaarheid van het beleidsinstrumentarium ook subjectieve elementen hebben meegespeeld en dat deze mogelijk (deels) op perceptie/ persoonlijke inschatting hebben plaatsgevonden.

6.3 **Lessen voor de volgende NRA**

In deze paragraaf worden lessen beschreven die volgen uit de opgedane ervaringen in de tot nu toe uitgevoerde NRA's, en waarmee bij de uitvoering van de volgende NRA's rekening gehouden kan worden.

Zoals in hoofdstuk 1 al werd aangegeven, noemde de FATF in haar landenevaluatie van het Nederlandse beleid ten aanzien van witwassen en terrorismefinanciering dat er bij aankomende NRA's meer gebruikgemaakt zou moeten worden van kwantitatieve data over de risico's op het gebied van terrorismefinanciering. In deze derde NRA zijn, zoals bij de subparagraaf 'sterke punten' al aan bod kwam, bij de beschrijving van contextuele factoren (hoofdstuk 3) en de 12 grootste tf-dreigingen (hoofdstuk 4) in nog grotere mate dan in de vorige NRA relevante kwantitatieve databronnen betrokken. De verzamelde kwantitatieve informatie bleek vooral van illustratieve waarde te zijn. Het streven was echter om voor elk van de grootste tf-dreigingen kwantitatieve data op te nemen die een indicatie of meer inzicht zouden bieden in het risicogehalte van de betreffende dreigingen.

In de beginfase van deze NRA zijn aan diverse potentiële data-leveranciers vooraankondigingen gedaan ten aanzien van een dataverzoek. Zodra de definitieve lijst van grootste tf-dreigingen bekend was (in de tweede expertmeeting), zijn de dataverzoeken uitgegaan. De data konden verstrekt worden in de periode van mei tot en met oktober 2023.¹⁴² Op het niveau van de dreigingen zijn uiteindelijk in beperkte mate data verstrekt (alleen door de FIOD en Justis/TRACK). De enige tf-dreiging waarvoor kwantitatieve data zijn aangeleverd die daadwerkelijk meer inzicht bieden in de dreiging, is 'financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering'. Op basis van data van Justis/TRACK zijn aanvullende inzichten verkregen in ongebruikelijke situaties met betrekking tot stichtingen.

Redenen voor het niet of in beperkte mate verstrekken van kwantitatieve data over elk van de 12 grootste tf-dreigingen zijn – voor zover het WODC dit kan inschatten – de tijdsinvestering die het dataverzoek van de organisaties vergt, de beperkte capaciteit bij organisaties om hiervoor tijd vrij te maken, knelpunten dan wel onmogelijkheden om bepaalde relevante informatie uit de datasystemen van de organisaties te halen en/of de vertrouwelijkheid van de betreffende data.

¹⁴² Omdat het WODC geen zicht heeft op de precieze aard en omvang van de data en andere informatie die deze partijen beschikbaar hebben, is een algemene vraag uitgegaan voor het leveren van data en kwalitatieve informatie. Wel zijn daarbij aanwijzingen gegeven voor het type kwantitatieve en kwalitatieve informatie dat voor de NRA behulpzaam zou zijn. Zo werd aangegeven dat de betreffende partij wellicht naar bepaalde dreigingen specifiek onderzoek heeft gedaan, waardoor er cijfermatige overzichten of kwalitatieve beschrijvingen van casuïstiek beschikbaar zijn. Ook is gevraagd uit de datasystemen informatie te leveren die zicht biedt op het jaarlijkse aantal zaken/dossiers per dreiging, achtergrondinformatie over de complexiteit van de zaak en/of een indicatie van de omvang van de zaak (bijvoorbeeld in euro).

In hoofdstuk 1 kwam al aan bod dat de risicoanalyse een overkoepelende dataset vereist die voor alle dreigingen de benodigde gegevens van voldoende kwaliteit bevat. Ten behoeve van de risicoanalyse in de NRA's zouden in ieder geval de volgende typen kwantitatieve data beschikbaar moeten zijn:

- data over de prevalentie van de verschillende tf-dreigingen;
- data over de potentiële impact van de diverse dreigingen op de criteria van de MCA;
- data over de weerbaarheid van het beschikbare beleidsinstrumentarium ter preventie en/of bestrijding van iedere dreiging.

Die data zijn nu niet beschikbaar en zelfs als die data wel beschikbaar zouden komen en tijdig beschikbaar zouden worden gesteld ten behoeve van de NRA, dan bemoeilijken verschillende aspecten nog steeds de risicoanalyse. Allereerst blijft bij alle vormen van criminaliteit, en dus ook bij de verschillende tf-dreigingen die zijn te relateren aan een vorm van criminaliteit, een groot deel verborgen; dit *'dark number'* komt niet terug in de data die gebruikt worden voor de risicoanalyse. Ten tweede zijn er geen data beschikbaar over toekomstige of nog niet gesignaleerde tf-dreigingen die bij de risicoanalyse betrokken kunnen worden.

Wel kan in de volgende NRA's in nog grotere mate gebruik gemaakt worden van kwantitatieve data als aanvullende toelichting op (onderdelen van) de grootste tf-dreigingen en de context waarbinnen de dreigingen spelen. Daarvoor is dan wel een optimale en tijdige medewerking van de potentiële dataleveranciers een noodzaak, hetgeen tijdens de uitvoering van de voorliggende derde NRA Terrorismefinanciering in sommige gevallen een knelpunt vormde. Bij toekomstige NRA's zouden de aanvragers van de NRA op verzoek van de onderzoekers al in de beginfase van het onderzoek een actievere rol kunnen innemen om de potentiële dataleveranciers te bewegen tijdig de data (zoals al is uitgevraagd voor deze derde NRA) te verstrekken.

Geconcludeerd kan worden dat een risicoanalyse op basis van kwantitatieve data voor de NRA's niet reëel is. De volgende NRA's zullen dus – net als de nu uitgevoerde NRA – een hoofdzakelijk kwalitatieve insteek hebben waarbij de risicoanalyse gebaseerd zal zijn op de oordelen en inschattingen van vertegenwoordigers van expertorganisaties.

Summary

Background of the study

The Dutch policy for the prevention and combat¹⁴³ of terrorist financing is based on the recommendations of the Financial Action Task Force (FATF) and regulations of the European Union (EU). As a member of the FATF, the Netherlands is bound by the recommendations of this intergovernmental body aimed at taking preventive and repressive measures against money laundering and terrorist financing, measures with regard to national legal systems and international cooperation. For the EU member states, most of the FATF recommendations have been converted into several successive Anti-Money Laundering Directives. Based on these directives, the EU member states must implement a risk-oriented policy against money laundering and terrorist financing and establish a National Risk Assessment (NRA). For the Netherlands, the implementation of the NRA is laid down in the Money Laundering and Terrorist Financing Prevention Act (*Wet ter voorkoming van witwassen en financieren van terrorisme, Wwft*). Article 1f paragraph 1 of the Wwft states that the Ministers of Finance and Justice and Security jointly publish a report, to be updated every two years, of the identified, analysed and assessed national risks in the areas of money laundering and terrorist financing.

The Research and Data Centre (*Wetenschappelijk Onderzoek- en Datacentrum, WODC*) carried out a third NRA on Terrorist Financing for the European Netherlands in the period June 2022 to December 2023.¹⁴⁴ The risk analysis carried out for the NRA covers the period January 2020 to June 2023. The NRA has a fivefold purpose:

- 1 identifying the terrorist financing threats with the greatest potential impact (i.e. the greatest terrorist financing threats);
- 2 determining the level of potential impact of the greatest terrorist financing threats;
- 3 determining the level of resilience of the policy instruments for the prevention and/or repression of the greatest terrorist financing threats;
- 4 providing insight into the nature and mechanisms of the greatest terrorist financing threats; and
- 5 determining the risk level of the greatest terrorist financing threats by comparing the potential impact of the threats and the resilience of the policy instruments.

Research methodology

The structure of the third NRA is – as in the previous NRAs – determined by the ISO 31000 framework for risk management. The research methodology used includes the following components:

¹⁴³ The terms 'repression' and 'combatting' are viewed in this NRA as being synonymous. Both terms are used in this report for the sake of variety.

¹⁴⁴ Since 2017, two previous NRAs in the field of terrorist financing have been carried out by the WODC for the European Netherlands. In addition, two NRAs on money laundering have since been carried out for the European Netherlands. Two NRAs have also been carried out for the Caribbean Netherlands since 2017, relating to both terrorist financing and money laundering. Parallel to the realisation of the third NRA on Terrorist Financing, the WODC conducted the third NRA on money laundering (for the European Netherlands).

- A context analysis outlining the specific characteristics of the Netherlands that may influence the prevalence of terrorist financing and its potential impact. These factors can play a role in determining the financing methods and the sources of financing to be used. For this context analysis, a literature study was conducted and relevant quantitative data sources were consulted.
- For the purpose of an inventory of terrorist financing threats, recent reports (published since 2020) have been studied, including the European Supra National Risk Assessment (SNRA), and the so-called FANO survey¹⁴⁵ has been conducted among public and private parties with a task in the prevention and/or combat of terrorist financing.
- In the first expert meeting, representatives of expert organisations identified the terrorist financing threats which they view as the threats having the greatest potential impact.
- After the first expert meeting, in-depth interviews were conducted with representatives of expert organisations and other parties with a role in combatting terrorist financing to further discuss the nature, mechanisms and cases of the threats on the provisional shortlist of the greatest terrorist financing threats.
- In the second expert meeting – based on the findings from the interviews – the shortlist of the greatest terrorist financing threats was adjusted and finally established, after which the experts assessed the potential impact of the threats using a Multi Criteria Analysis (MCA).
- In the third expert meeting, experts assessed the resilience of the total package of available policy instruments for each of the greatest terrorist financing threats.
- By comparing the assessed potential impact of the terrorist financing threats with the assessed resilience, insight was gained into the risk level of the 12 greatest terrorist financing threats.
- Data requests have been submitted to a number of public organisations for all 12 threats and as much available quantitative data as possible as well as recent cases have been included in the report.
- In the final phase of the study, validating interviews are conducted with eight experts working at six key organisations, with the main aim of determining the extent to which they recognize the risk level of the 12 greatest terrorist financing threats. In addition, the correlation has been determined for the eight threats with the same scope that are included in the list of greatest threats in both the third NRA on Terrorist Financing and the third NRA on Money Laundering.

Greatest terrorist financing threats

From a longlist of 27 terrorist financing threats experts in the field of terrorist financing identified in the first expert meeting the ten threats that, in their opinion, scored highest in terms of potential impact within the Dutch context. This led to a preliminary shortlist of 15 greatest terrorist financing threats, which was shortened to 12 threats in the second expert meeting. The NRA focuses on this final shortlist of 12 greatest terrorist financing threats, which are shown categorised in Table Sum1 because the greatest threats do not vary much in terms of potential impact.

¹⁴⁵ In this online survey, respondents were asked to indicate in a longlist of threats whether they have experience with facts/cases of the threats from their own work and to what extent they consider the prevalence of the threats to be plausible or not based on the information available at their organisation. FANO stands for Facts/cases (*Feiten/casus*), Likely (*Aannemelijk*), Unlikely (*Niet aannemelijk*) and Unknown (*Onbekend*).

The terrorist financing threats in Table Sum1 concern financing methods and financial sources that can – in various combinations of two or more threats – form a terrorist financing construction. Such a construction can be quite simple in nature, but can also be complex in nature. The threat 'financing via unlicensed money transfer organisations and hawala banking' received the highest score of the 12 threats, namely a score of 61 on a scale of 0 to 100. Lowest in this list of the greatest terrorist financing threats is 'financing via crypto service providers' (score 48). The table below makes it clear that the potential impact of the 12 threats does not differ greatly from each other (after all, the scores are between 48 and 61).

Table Sum1 Potential impact of 12 greatest terrorist financing threats (n=8)

	Potential impact (on a scale of 0-100)
Score category '60 or more'	
Financing via unlicensed money transfer organisations and hawala banking	61
Score category '55 to 59'	
Financing via the physical movement of (large amounts of) cash or high-value products in/via the Netherlands or to/from abroad	58
Financing with funds obtained via horizontal/vertical fraud	57
Financing via wire transfers or cash transactions at licensed banks	57
Financing via foundations with little transparency about finances and no self-regulation	56
Financing via wire transfers or cash transactions at licensed money transfer organisations	55
Financing via easily accessible (online) ways to open a foreign bank account	55
Financing with funds obtained via a form of crime other than fraud	55
Score category '50 to 54'	
Financing with legally obtained own resources	50
Financing via donations through payment requests and/or crowdfunding through social media	50
Financing via internet payment services (Payment Service Providers, PSPs)	50
Score category 'Less than 50'	
Financing via crypto service providers	48

Resilience of the policy instruments

The available policy instruments to prevent and combat terrorist financing include all relevant instruments arising from international and national legislation and regulations, legislation and regulations at a municipal level, sectoral and branch-oriented regulations, and regulations at an organisational level. This NRA also views partnerships between public and/or private organisations and guidelines, guidances and policy plans of organisations that play a role in the prevention and/or combat of terrorist financing as a policy instrument. Table Sum2 provides an overview of the policy instruments that were available until June 2023 – the month in which the third expert meeting took place – to prevent and combat terrorist financing.

Table Sum2 Policy instruments to prevent and combat terrorist financing

International laws and regulations	National laws and regulations	Other policy instruments
<ul style="list-style-type: none"> • FATF recommendations • EU Anti-Money Laundering Directives • United Nations Security Council Resolutions and EU Regulations • Other international sanctions lists • European regulation on declaration of liquid assets • Wire Transfer Regulation 2 	<ul style="list-style-type: none"> • Money Laundering and Terrorist Financing Prevention Act¹⁴⁶ • Sanctions Act 1977 and sanction regulations • Penal Code • Code of Criminal Procedure • Intelligence and Security Services Act 2017 • Temporary law on administrative measures to combat terrorism • Explosives Precursors Act • Financial Supervision Act • General Customs Act • Legal Entities Supervision Act • Trade Register Act 2007 (including UBO-registers) • Tax legislation • Social legislation • Economic Offenses Act • Public Administration Probity Screening Act 	<ul style="list-style-type: none"> • National partnerships • International partnerships • Sectoral regulations and conditions • Guidelines, guidances and policy plans

For the 12 greatest threats, in the third expert meeting terrorist financing experts assessed the extent to which the total package of existing policy instruments counters the potential impact of the threats. The results of the expert meeting are shown categorised in Table Sum3. In their assessment of the resilience of the policy instruments, experts based their assessment on the policy instruments that had been implemented at that time (June 2023).

For three terrorist financing threats, the experts judge that the resilience of the policy instruments counters the potential impact by more than half (scores greater than 50), namely 'financing via wire transfers or cash transactions at licensed banks' (score 58), 'financing with funds obtained via horizontal/vertical fraud' (score 57) and 'financing via wire transfers or cash transactions at licensed money transfer organisations' (score 54). The four terrorist financing threats with the lowest resilience score all have a score lower than 30: financing via unlicensed money transfer organisations and hawala banking (score 28), with legally obtained own resources (score 27), via crypto service providers (score 25) and via easily accessible (online) ways to open a foreign bank account (score 23). The low scores therefore mean that the total package of policy instruments – according to experts – only counteract these terrorist financing threats to a relatively limited extent. The table below shows that the resilience of the policy instruments can differ greatly between the 12 greatest terrorist financing threats (the scores are between 23 and 58).

¹⁴⁶ In the Netherlands, the Wwft requires a large number of institutions to report Unusual Transactions (*Ongebruikelijke Transacties, OTs*) to the Financial Intelligence Unit (FIU) – the Netherlands.

Table Sum3 Resilience of policy instruments per greatest terrorist financing threat (n=6)

	Weerbaarheid <i>(op een schaal van 0-100)</i>
Score category '50 or more'	
Financing via wire transfers or cash transactions at licensed banks	58
Financing with funds obtained via horizontal/vertical fraud	57
Financing via wire transfers or cash transactions at licensed money transfer organisations	54
Score category '40 to 49'	
Financing via internet payment services (PSPs)	41
Financing via foundations with little transparency about finances and no self-regulation	41
Score category '30 to 39'	
Financing via donations through payment requests and/or crowdfunding through social media	39
Financing with funds obtained via a form of crime other than fraud	36
Financing via the physical movement of (large amounts of) cash or high-value products in/via the Netherlands or to/from abroad	34
Score category '20 to 29'	
Financing via unlicensed money transfer organisations and hawala banking	28
Financing with legally obtained own resources	27
Financing via crypto service providers	25
Financing via easily accessible (online) ways to open a foreign bank account	23

Despite the mitigating effect of the available instruments on the 12 greatest terrorist financing threats, the threats can still have a greater or lesser degree of impact. The mitigating effect is related to the extent to which the AIU principle¹⁴⁷ applies to the terrorist financing threats. With most terrorist financing methods one or more of the three AIU components apply. The more the AIU elements apply to terrorist financing threats, the lower the resilience of the policy instruments for preventing and repressing the threats.

Risk level of greatest terrorist financing threats

In Figure Sum1, a heat map compares the expert judgements of the potential impact and resilience of the policy instruments for the 12 greatest terrorist financing threats. The highest risks are threats with a high potential impact and low resilience of the available policy instruments. This heatmap can be seen as a summary of the third NRA on Terrorist Financing. However, it must be taken into account that the heatmap only shows the greatest terrorist financing threats and that the other threats from the longlist, that are also part of the NRA, are seen by the experts as moderate risks.

¹⁴⁷ AIU stands for Anonymous (the method conceals the identity of the financier of terrorism), International (the method has an international character and is used via or from abroad) and Unregulated (the method relates to or is used in an unregulated sector).

Figure Sum1 Heatmap third NRA: potential impact compared to resilience to the greatest terrorist financing threats¹⁴⁸



A	Unlicensed money transfer organisations and hawala banking	G	Foundations with little transparency about finances and no self-regulation
B	Easily accessible (online) ways to open a foreign bank account	H	Donations through payment requests and/or crowdfunding through social media
C	Physical movement of (large amounts of) cash or high-value products	I	Internet payment services (PSPs)
D	Legally obtained own resources	J	Wire transfers or cash transactions at licensed money transfer organisations
E	Crypto service providers	K	Funds obtained via horizontal/vertical fraud
F	Funds obtained via a form of crime other than fraud	L	Wire transfers or cash transactions at licensed banks

The figure shows that the risk level of the 12 greatest terrorist financing threats does not differ significantly from each other. This applies in particular to the potential impact scores, which range from 48 to 61. The resilience to the threats shows a greater spread. All threats are in the orange area in the figure. Of all these high-risk terrorist financing threats, the following two threats have the highest risk level (shown at the top left of the figure):

- *Terrorist financing via unlicensed money transfer organisations and hawala banking (A in Figure Sum1)*. This terrorist financing threat has such a high risk level mainly due to a low assessed resilience. According to the AIU principle the threat offers opportunities to transfer money anonymously, has an international character and is often deployed via and/or abroad, and concerns an unregulated 'sector'. Furthermore, this terrorist financing method is relatively easily accessible to individuals, groups and/or organisations who want to finance terrorism.

¹⁴⁸ To visualise the differences as clearly as possible, the figure shown is a cut-out from a figure with axes ranging from 0 to 100, with colours flowing from top left: red (highest potential impact and lowest resilience) to bottom right: green (lowest potential impact and highest resilience). The full heatmap with axes from 0 to 100 can be found in Appendix 8.

- *Terrorist financing via easily accessible (online) ways to open a foreign bank account (B)*. With this terrorist financing threat, the high risk level is mainly caused by a very low assessed resilience. This is related to the fact that some digital foreign bank accounts can be opened relatively easily – with, depending on the country, possibly less strict terrorist financing regulations and supervision with regard to financial service providers – and that there are currently no policy instruments to counter this. Once an individual has a foreign bank account, he or she can conduct transactions to, through or from this account, which are hard to monitor by Dutch banks and are less transparent to investigative authorities, which therefore have a weaker information position.

Of the 12 greatest terrorist financing threats, the least high risk level lies with the four terrorist financing threats located furthest at the (bottom) right of the figure: financing 'via internet payment services (PSPs)' (I), via 'wire transfers or cash transactions at licensed banks' (J), via 'funds obtained via horizontal/vertical fraud' (K) and via 'wire transfers or cash transactions at licensed banks' (L). Although these threats still involve a significant level of risk, their risk level is judged to be relatively the lowest. This is mainly due to the highly assessed resilience, which can be related to the improvement of customer due diligence and transaction monitoring by both licensed banks and licensed money transfer organisations in recent years.

Literatuur

- AIVD (Algemene Inlichtingen- en Veiligheidsdienst) (2023). *Jaarverslag 2022*. AIVD.
- Algemene Rekenkamer (2022). *Bestrijden witwassen deel 3: Stand van zaken 2021*. Algemene Rekenkamer.
- Bekkers, R.H.F.P., G.J. van Leijenhorst & A.E.M. Leijten (2022). *Toezicht op algemeen nut*.
- Béné, C., Wood, R. G., Newsham, A., & Davies, M. (2012). Resilience: New utopia or new tyranny? Reflection about the potentials and limits of the concept of resilience in relation to vulnerability reduction programmes. *IDS Working Papers*, 2012(405), 1-61.
- Besamusca, E., & Verheul, J. (2010). 'Introduction'. In: E. Besamusca & J. Verheul (red.), *Discovering the Dutch: On culture and society of the Netherlands*. Amsterdam University Press.
- Boerman, F., Grapendaal, M., Nieuwenhuis, H. & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017 georganiseerde criminaliteit*. Dienst Landelijke Informatieorganisatie. Landelijke Eenheid Politie.
- Bruinsma, M. & Spapens, T. (2018). Terrorist access to firearms in the Netherlands. In: N. Duquet (Ed.), *Triggering terror: Illicit gun markets and firearms acquisition of terrorist networks in Europe* (pp. 285-325). Flemish Peace Institut.
- CBS (Centraal Bureau voor de Statistiek) (2023). *Nederland Handelsland. Export, import & investeringen 2022*. CBS.
- CCV (Centrum voor Criminaliteitspreventie en Veiligheid) (2021). *Malafide Stichtingen*. CCV.
- De Goede, M. (2007). *Literatuurstudie terrorismefinanciering 2004-2006: Rapport aan de Nationaal Coördinator Terrorismebestrijding*. Universiteit van Amsterdam, Faculteit der Geesteswetenschappen.
- Egmont Group of Financial Intelligence Units (2019). *Counter Terrorist Financing Project: Lone actors and small cells*.
- Europese Commissie (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*. Europese Commissie.
- Eurostat (2023). *Demography of Europe. 2023 interactive edition*. 11 May 2023.
- Ferwerda, H, J. Wolsink & Van Leiden, I. (2020). *De lading van vuurwapens: Een onderzoek naar de impact van illegale vuurwapens in Nederland*. Politie & Wetenschap.
- FATF (Financial Action Task Force) (2012-2023). *International standards on combating money laundering and the financing of terrorism & proliferation: The FATF Recommendations*. Updated 2023. FATF.
- FATF (Financial Action Task Force) (2013). *Guidance national money laundering and terrorist financing risk assessment*. FATF.
- FATF (Financial Action Task Force) (2022). *Anti-money laundering and counter-terrorist financing measures – The Netherlands. Fourth Round Mutual Evaluation Report*. FATF.
- FATF (Financial Action Task Force) (2023). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. FATF.
- FIU Nederland (Financial Intelligence Unit Nederland) (2021). *Jaarverslag 2020*. FIU Nederland.

- FIU Nederland (Financial Intelligence Unit Nederland) (2022). *Jaarverslag 2021*. FIU Nederland.
- FIU Nederland (Financial Intelligence Unit Nederland) (2023). *Jaarverslag 2022*. FIU Nederland.
- Financieel Expertise Centrum (2023). *Jaarverslag 2022*. Financieel Expertise Centrum.
- Gestel, B., Van Berkel, J.J., & Kouwenberg, R.F. (2019). *Bestuurlijke vrijheidsbeperking van jihadisten: Het gebruik van de 'Tijdelijk wet bestuurlijke maatregelen terrorismebestrijding' in de eerste periode na inwerkingtreding van de wet*. WODC. Cahier 2019-4.
- Goede Doelen Nederland en Centraal Bureau Fondsenwerving (2021). *Waar staan we nu? Reflectie op het voorkomen van terrorismefinanciering in de goededoelensector*. GDN/CBF.
- Institute for Economics & Peace (2023). *Global Terrorism Index 2023: Measuring the Impact of Terrorism*. IEP.
- ISO 31000:2009 (2009a). *Risk management: Principles and guidelines*. International Organization for Standardization.
- ISO/IEC 31010:2009 (2009b). *Risk management: Risk assessment techniques*. International Organization for Standardization.
- Jonsson, M. (2015). *Funding the Islamic State: Sources of revenue, financing requirements and long-term vulnerabilities to counter-measures*. Asia Security Briefing, December, 2015. FOI Memo 5525, Projekt Nr: A15103.
- Junger, M., B. Veldkamp & L. Koning (2022). *Fraudevictimisatie in Nederland*. Universiteit Twente.
- Justis (2017). *De Wet controle op rechtspersonen: Een continue controle op rechtspersonen*. Justis.
- Keatinge, T. & Keen, F. (2017). *Lone-actor and small cell terrorist attacks: A new front in counter-terrorist finance?* RUSI. Occasional Paper.
- Kroon, M. (1992). *Effects of accountability on groupthink and intergroup relations: Laboratory and field studies*. Proefschrift Rijksuniversiteit Utrecht. Thesis Publishers.
- Kruisbergen, E.W., Van de Bunt, H.G., Kleemans, E.R., Kouwenberg, R.F., Huisman, K., Meerts, C.A., & De Jong, D. (2012). *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Boom Lemma. Onderzoek en beleid 306.
- Kruize, P. & Gruter, P. (2021). *Evaluatie van de Wet precursoren voor explosieven: Met aandacht voor het vergunningstelsel voor particulieren en de registratie- en meldplicht van bedrijven*. Ateno.
- Lees, F.P. (1980). *Loss Prevention in the Process Industries*. Butterworth-Heinemann.
- Mijnhardt, W. (2010). 'A tradition of tolerance'. In: E. Besamusca & J. Verheul (red.), *Discovering the Dutch: On culture and society of the Netherlands*. Amsterdam University Press.
- Miltenburg, E., B. Geurkink, S. Tunderman, D. Beekers & Den Ridder, J. m.m.v. E. Hartevelde (2022). *Burgerperspectieven 2022. Bericht 2*. SCP.
- Ministers van Financiën en Justitie en Veiligheid (2019). *Plan van aanpak witwassen: Juni 2019*. Ministerie van Financiën/Ministerie van JenV.
- Minister van Justitie en Veiligheid (2022). *Aanpak georganiseerde criminaliteit op hoofdlijnen*. 26 april 2022. Brief aan de Tweede Kamer. Kenmerk: 3977507. Bijlage 3 : Ondergronds bankieren. Ministerie van Justitie en Veiligheid.
- Nanaeva, Z. & A., Faruk A. & Shirazi, N.S. (2021). *Open banking in Europe: The impact of the Revised Payments Services Directive on Solarisbank and Insha*. MPRA Paper 110763, University Library of Munich, Germany.

- Nationaal Coördinator Terrorismebestrijding en Veiligheid) (2021). *Wet precursoren voor explosieven aangescherpt*. NCTV.
- NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid) (2022). *Dreigingsbeeld Terrorisme Nederland 57*. NCTV.
- NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid) (2023a). *Dreigingsbeeld Terrorisme Nederland 58*. NCTV.
- NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid) (2023b). *Dreigingsbeeld Terrorisme Nederland 59*. NCTV.
- Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen (2022a). *Slachtoffers van mensenhandel in beeld bij CoMensha 2017-2021*. Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen.
- Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen (2022b). *Dadermonitor mensenhandel 2017-2021*. Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen.
- OM (Openbaar Ministerie) (2019). 'Ondergronds Bankieren'. In: *Inzicht Magazine*, 2019/03.
- Oftedal, E. (2015). The financing of jihadi terrorist cells in Europe. Z.pl.: Norwegian Defence Research Establishment (FFI). FFI-rapport 2014/02234.
- Schulpen, L. & Van der Plas, D. (2023). *State of the Sector. Introductie van de Goede Doelen Index*. CBF/Radboud Universiteit Nijmegen.
- Schulten, N., Doosje, B., Spaaij, R., & Kamphuis, J.H. (2019). *Psychopathologie en terrorisme: Stand van zaken, lacunes en prioriteiten voor toekomstig onderzoek*. Universiteit van Amsterdam.
- Snel, E., G. Engbersen, J. de Boom, Y. Seidler, N. Sam, G. Enneking, F. l'Istelle, L. van Heck & J. van Linder (2023). *Corona & Cohesie: Dashboard Sociale Impact Corona. Verslag meting 5 (juni 2022) en meting 6 (november 2022)*. Risbo & Erasmus School of Social and Behavioural Sciences.
- Soudijn, M. (2019). Van salafistisch gedachtegoed alleen kun je niet leven: De financiële zelfredzaamheid van 131 uitreizigers nader bekeken. *Tijdschrift voor Criminologie*, 61(1).
- Tavares, C., G. Thomas & Roudaut, M. (2010). *Money laundering in Europe: Report of work carried out by Eurostat and DG Home Affairs*. Eurostat Methodologies and Working papers. Publications Office of the European Union.
- United States Department of State. Bureau of International Narcotics and Law Enforcement Affairs (2022). *International Narcotics Control Strategy Report Volume I. Drug and Chemical Control*. United States Department of State.
- Van der Veen, H.C.J. & Ferwerda, J. (2016). *Verkenning methoden en data National Risk Assessment Witwassen en Terrorismefinanciering*. WODC. Cahier 2016-12.
- Van der Veen, H.C.J. & Heuts, L.F. (2017a). *National Risk Assessment Witwassen*. WODC. Cahier 2017-13.
- Van der Veen, H.C.J. & Heuts, L.F. (2017b). *National Risk Assessment Terrorismefinanciering*. WODC. Cahier 2017-14.
- Van der Veen, H.C.J. & Heuts, L.F. (2018). *National Risk Assessment Witwassen en Terrorismefinanciering Bonaire, Sint Eustatius en Saba*. WODC. Cahier 2018-17.
- Van der Veen, H.C.J. & Heuts, L.F. m.m.v. E.C. Leertouwer (2020a). *National Risk Assessment Witwassen 2019*. WODC. Cahier 2020-11.
- Van der Veen, H.C.J. & Heuts, L.F. m.m.v. E.C. Leertouwer (2020b). *National Risk Assessment Terrorismefinanciering 2019*. WODC. Cahier 2020-12.
- Van der Veen, H.C.J. & Heuts, L.F. (2021). *National Risk Assessment Witwassen en Terrorismefinanciering 2021 Bonaire, Sint Eustatius en Saba*. WODC. Cahier 2021-14.

- Van Dijk, J., M. Cruyff & Van der Heijden, P. (2021). *Multiple Systems Estimation Slachtoffers Mensenhandel Nederland 2016-2019*. WODC.
- Van Wonderen, R., Burggraaff, D., Ganpat S., Van Beek, G. & Cauberghs, O. (2023). *Rechtsextremisme op sociale mediaplatforms? Ontwikkelingspaden en handelingsperspectieven*. Verwey-Jonker Instituut.
- Van Zanden, J.L. (2010). 'The Economy of the Polder'. In: E. Besamusca & J. Verheul (red.), *Discovering the Dutch: On culture and society of the Netherlands*. Amsterdam University Press.
- Verbeek-Oudijk, D., Hardus, S., Van den Broek, A. & Reijnders, M. (2023). *Sociale en Culturele Ontwikkelingen. Stand van Nederland 2023*. SCP.
- Wesseling, M., & De Goede, M. (2018). *Beleid bestrijding terrorismefinanciering: Effectiviteit en effecten (2013-2016)*. University of Amsterdam, AISSR/WODC.
- World Trade Organization (2023). *World trade Statistical Review 2023*. World Trade Organization.

Links naar websites

- [4. Online oplichting en fraude \(cbs.nl\)](#).
- [Aanbod aan migrantenpartijen sterk toegenomen \(nos.nl\)](#).
- [ACI World confirms top 20 busiest airports worldwide](#).
- [Advocatuur onder toezicht van onafhankelijke landelijke toezichthouder | Nieuwsbericht | Rijksoverheid.nl](#).
- [Balanstotaal van Nederlands grootste banken met 2% gekrompen](#).
- [Bestrijden van mensenhandel | Mensenhandel en mensensmokkel | Rijksoverheid.nl](#).
- [Bestrijden van mensensmokkel | Mensenhandel en mensensmokkel | Rijksoverheid.nl](#).
- [Betaaldiensten waarvoor een vergunning nodig is \(dnb.nl\)](#).
- [Burgerperspectieven bericht 2 2022 | Publicatie | Sociaal en Cultureel Planbureau \(scp.nl\)](#)
- [CBF | Toezichthouder goede doelen](#).
- [Controle op liquide middelen die EU binnenkomen of verlaten: Raad neemt verordening aan - Consilium \(europa.eu\)](#).
- [CT Infobox | Nationaal Coördinator Terrorismebestrijding en Veiligheid \(nctv.nl\)](#).
- [Data zoeken - DNB](#).
- [Definities gebruikt in het Dreigingsbeeld Terrorisme Nederland | Dreigingsbeeld Terrorisme Nederland | Nationaal Coördinator Terrorismebestrijding en Veiligheid \(nctv.nl\)](#).
- [Delphi Method | RAND](#).
- [De stichting | Ondernemersplein \(kvk.nl\)](#).
- [Europe Neobanking Market Size & Share Analysis - Industry Research Report - Growth Trends \(mordorintelligence.com\)](#).
- [EUR-Lex - 32023D1514 - EN - EUR-Lex \(europa.eu\)](#).
- [Europese-Commissie-actualiseert-Wwft-hoogrisico-landen-per-16-maart-2023.pdf \(bureauft.nl\)](#).
- [Exclusive: Israel seized Binance crypto accounts to 'thwart' Islamic State, document shows | Reuters](#).
- [Extremisme | AIVD](#).
- [Extremisme | Nationaal Coördinator Terrorismebestrijding en Veiligheid \(nctv.nl\)](#).
- [FATF clarifies risk-based approach: case-by-case, not wholesale de-risking \(fatf-gafi.org\)](#).

- [Fracties | Tweede Kamer der Staten-Generaal.](#)
- [Fraude | Openbaar Ministerie \(om.nl\).](#)
- [Geen registratieplicht bij DNB voor aanbieders van crypto-to-crypto omwisseldiensten.](#)
- [GTI-2020-web-1.pdf \(visionofhumanity.org\).](#)
- [Hamas kreeg 41 miljoen dollar in cryptomunten in aanloop naar aanval | De Standaard.](#)
- [Hezbollah Military Wing \(nctv.nl\).](#)
- [Hoe maken jullie het onderscheid tussen financiering van humanitaire hulp en financiering van terrorisme? | Openbaar Ministerie \(om.nl\).](#)
- [Hoe werken Cryptocurrencies? Wij leggen het je uit! \(techopedia.com\).](#)
- [Home \(fatf-gafi.org\).](#)
- [Home | Office of Foreign Assets Control \(treasury.gov\).](#)
- [Home - Wolfsberg Group \(wolfsberg-group.org\).](#)
- [https://icov.nl/organisatie/.](#)
- [Israel freezes crypto accounts seeking Hamas donations, police say | Reuters.](#)
- [Jihadistische dreiging tegen Nederland | Terrorisme | AIVD.](#)
- [Jihadisme tegengaan | Terrorismebestrijding | Rijksoverheid.nl.](#)
- [Kwetsbaarheden voor witwassen bij PSP's - AMLC.](#)
- [Levenslang voor schietpartij in tram op 24 Oktoberplein Utrecht | Nieuws | Rechtspraak.](#)
- [Markets in Crypto-Assets Regulation \(MiCAR\) \(afm.nl\).](#)
- [Nationale samenwerking - FIU-Nederland.](#)
- [Netherlands - The World Factbook \(cia.gov\).](#)
- [Om hoeveel geld gaat het? | Openbaar Ministerie.](#)
- [Procedures totstandkoming en beëindiging van bevroeringsmaatregelen terrorisme | Publicatie | Rijksoverheid.nl.](#)
- [Publications Office \(europa.eu\).](#)
- [Register van aanbieders van cryptodiensten \(dnb.nl\).](#)
- [Registratie in UBO-registers | Financiële sector | Rijksoverheid.nl.](#)
- [Religieuze betrokkenheid in Nederland \(cbs.nl\).](#)
- [Samen financiële criminaliteit bestrijden - TMNL.](#)
- [Sanctieregelingen stand van zaken 17 juli 2023 | Rapport | Rijksoverheid.nl.](#)
- [StatLine - Bevolkingsontwikkeling; maand en jaar \(cbs.nl\).](#)
- [StatLine - Verdiensten en arbeidsvolume; uitvoerstromen \(cbs.nl\).](#)
- [Taskforces - FEC-partners.](#)
- [Terrorisme | AIVD.](#)
- [THE NETHERLANDS - EBF.](#)
- [The UK Sanctions List - GOV.UK \(www.gov.uk\).](#)
- [Toezichthouders - FIU-Nederland.](#)
- [Top-15 container ports in European Union in 2022 - PortEconomics.](#)
- [Transactie Monitoring Nederland aan de slag \(nvb.nl\).](#)
- [Van bankrekeningfraude tot hulpvraagfraude - Het CCV.](#)
- [Versplintering - Parlement.com.](#)
- [Verstoring van crimineel ondergronds bankieren vraagt om internationale aanpak | Verhalen uit de praktijk | Nederland tegen georganiseerde misdaad.](#)
- [Wat u moet weten over crypto's \(dnb.nl\).](#)
- [Welke landen horen bij de Europese Economische Ruimte \(EER\)? | Rijksoverheid.nl.](#)
- [Welke landen zijn Schengenlanden? | Rijksoverheid.nl.](#)
- [Welke zeehavens zijn er in Nederland? \(cbs.nl\).](#)
- [wetten.nl - Regeling - Wet ter voorkoming van witwassen en financieren van terrorisme - BWBR0024282 \(overheid.nl\).](#)

- [Wetsvoorstel om toegang tot UBO-registers te beperken | Nieuwsbericht | Rijksoverheid.nl](#)
- [Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme in verband met het verbod op contante betalingen voor goederen vanaf €3.000 en het uitbreiden van de mogelijkheden voor informatie-uitwisseling ten behoeve van de poortwachtersfunctie \(Wet plan van aanpak witwassen\) | Tweede Kamer der Staten-Generaal.](#)
- [Wwft - Bureau Financieel Toezicht \(bureauft.nl\).](#)

Casuïstiek

- [Al Aqsa gaat door onder andere naam | Trouw.](#)
- [Al Aqsa Nederland \(nctv.nl\).](#)
- [Fondsenwerver Hamas: 'Ik was bij workshop met ambtenaren Sigrid Kaag' - EWmagazine.nl.](#)
- [Illegaal bankieren en financieren van terrorisme - FIU-Nederland.](#)
- [Onderzoek naar grootschalige financiering van Hamas | Nieuwsbericht | Openbaar Ministerie \(om.nl\).](#)
- [Ophef over aanwezigheid vermeende fondsenwerver Hamas bij Nederlandse workshop | De Dikke Blauwe.](#)
- [Tot 30 maanden cel voor illegale geldtransacties en financieren van terrorisme \(rechtspraak.nl\).](#)
- [Veroordeling voor onder meer hawala-bankieren en financiering terrorisme \(rechtspraak.nl\).](#)

Bijlage 1 Samenstelling begeleidingscommissie

Voorzitter

Prof. dr. W.F.M. Bams Universiteit Maastricht, School of Business and Economics

Leden

Mr. drs. Z. Zuidema Ministerie van Justitie en Veiligheid, Directie
Rechtshandhaving en Criminaliteitsbestrijding (tot en met januari 2023)

Drs. T. van den Berk Ministerie van Justitie en Veiligheid, Directie
Rechtshandhaving en Criminaliteitsbestrijding (vanaf april 2023)

Mr. dr. T.J. van Koningsveld Offshore Kenniscentrum
Dr. M. Wesseling WES Consulting

Bijlage 2 Lijst van geïnterviewden

Tabel B2.1 Verdiepende interviews

Organisatie ^a	Aantal geïnterviewden
ABN AMRO	2 medewerkers
ANBI-team (Ministerie van Financiën)	3 medewerkers
Autoriteit Financiële Markten	2 medewerkers
Bitvavo	2 medewerkers
Bureau Financieel Toezicht	3 medewerkers
Bureau Toezicht Wwft	2 medewerkers
Centraal Bureau Fondsenwerving	2 medewerkers
De Nederlandsche Bank	4 medewerkers
Douane Nederland	1 medewerker
Financial Intelligence Unit Nederland	1 medewerker
Fiscale Inlichtingen- en Opsporingsdienst	3 medewerkers
Fondsen in Nederland ^a	1 medewerker
Goede Doelen Nederland ^a	1 medewerker
Human Security Collective ^a	1 medewerker
ING	2 medewerkers
Justis/TRACK	1 medewerker
Kamer van Koophandel	1 medewerker
Koninklijke Nederlandse Beroepsorganisatie van Accountants	2 medewerkers
Nationale Politie	2 medewerkers
Nederlandse Vereniging van Banken	1 medewerker
Nederlandse Vereniging van Geld Transactiekantoren	3 medewerkers
Openbaar Ministerie	4 medewerkers
Rabobank	2 medewerkers
Samenwerkende Brancheorganisaties Filantropie ^a	1 medewerker
Verenigde Betaal Instellingen Nederland	2 medewerkers
Verenigde Bitcoinbedrijven Nederland	2 medewerkers
Volksbank	1 medewerker
Totaal aantal geïnterviewden	52

^a Voor deze goede doelen organisaties is een groepsinterview uitgevoerd.

Tabel B2.2 Validerende interviews

Organisatie	Aantal geïnterviewden
Algemene Inlichtingen- en Veiligheidsdienst	1 medewerker
Financial Intelligence Unit Nederland	1 medewerker
Fiscale Inlichtingen- en Opsporingsdienst	1 medewerker
Nationale Politie	1 medewerker
Nederlandse Vereniging van Banken	2 medewerkers
Openbaar Ministerie	2 medewerkers
Totaal aantal geïnterviewden	8

Tabel B2.3 Evaluatieve interviews

Organisatie	Aantal geïnterviewden
Ministerie van Justitie en Veiligheid	1 medewerker
Ministerie van Financiën	1 medewerker
Nationaal Coördinator Terrorismebestrijding en Veiligheid	1 medewerker
Totaal aantal geïnterviewden	3

Bijlage 3 Deelnemers expertmeetings

Tabel B3.1 Deelnemers expertmeetings

Organisatie	1 ^e expertmeeting	2 ^e expertmeeting	3 ^e expertmeeting
Bureau Financieel Toezicht	Deelnemer I	Deelnemer II	<i>Uitgenodigd, geen deelname</i>
De Nederlandsche Bank	Deelnemer I	Deelnemer I	Deelnemer II
Douane Nederland	Deelnemer I	Deelnemer II	<i>Uitgenodigd, geen deelname</i>
Financial Intelligence Unit Nederland	Deelnemer I	Deelnemer I	Deelnemer II
Fiscale Inlichtingen- en Opsporingsdienst	Deelnemer I	Deelnemer II	Deelnemer II
Nationale Politie	Deelnemer I	Deelnemer II	Deelnemer II
Nederlandse Vereniging van Banken	Deelnemer I	Deelnemer II ^a	Deelnemer II ^a
Openbaar Ministerie	Deelnemer I	Deelnemer II	Deelnemer II
Totaal aantal deelnemers	8	8	6

a Deze organisatie heeft een vertegenwoordiger van een grootbank afgevaardigd.

Bijlage 4 FANO-enquête tf-dreigingen en responsoverzicht

Onderstaande tekst en tabellen zijn via een *online* enquête voorgelegd aan toezichthouders, opsporingsinstanties, handhavers, poortwachters en brancheorganisaties van poortwachters die zijn betrokken bij de preventie en/of bestrijding van terrorismefinanciering. De enquête is uitgezet via de enquêtetool van Onderzoekdoen.nl.

Doel enquête

Via deze enquête willen wij achterhalen of uw organisatie via de *eigen werkzaamheden* (dus niet via berichten uit de media, via andere organisaties of via andere bronnen) ervaring heeft met feiten/casussen van 'dreigingen' op het terrein van (1) *de financiering van terroristische activiteiten in Nederland vanuit Nederland of het buitenland*, en (2) *de financiering van terroristische activiteiten in het buitenland vanuit Nederland*. Bij 'dreigingen' gaat het om methoden die (kunnen) worden ingezet om terroristische activiteiten te financieren en/of de financiële middelen hiertoe te verwerven. De enquête moet ook inzichtelijk maken in hoeverre uw organisatie de prevalentie van de dreigingen al dan niet aannemelijk acht (op basis van informatie die bij uw organisatie via de eigen werkzaamheden beschikbaar is). Evenals bij de vorige *National Risk Assessment* (NRA) Terrorismefinanciering geschiedt dit volgens de zogeheten FANO-systematiek.

Toelichting enquête

Aan u wordt gevraagd om in de longlist van terrorismefinanciering-dreigingen *bij iedere dreiging* een van de volgende letters te markeren:

- een **F** indien er volgens u sprake is van deze dreiging en er via de eigen werkzaamheden één of meer **Feiten/casussen** bekend zijn bij uw organisatie;
- een **A** indien het volgens u **Aannemelijk** is dat deze dreiging speelt maar er via de eigen werkzaamheden geen feiten/casussen bekend zijn bij uw organisatie;
- een **N** indien het volgens u **Niet aannemelijk** is dat deze dreiging speelt op basis van de informatie waarover uw organisatie via de eigen werkzaamheden beschikt;
- een **O** indien het voor u **Onbekend** is of een dreiging speelt, omdat uw organisatie geen zicht heeft hierop via de eigen werkzaamheden, of omdat u de dreiging niet kent.

U kunt per dreiging slechts één keuze maken. Indien u een F bij een bepaalde dreiging invult, gaan wij ervan uit dat uw organisatie via de eigen werkzaamheden ervaring heeft met ten minste één specifieke casus. Wij stellen om die reden de vervolgvraag om voor die dreiging(en) een heel beknopte beschrijving van een Feit/casus (of een verwijzing hiernaar) te geven.

In een vervolgvraag bestaat de mogelijkheid om dreigingen die volgens u ontbreken, toe te voegen. Indien u hier een dreiging toevoegt, dient u ook een F of A aan te geven. In het geval van een F zien we ook graag een heel beknopte beschrijving van

het Feit of de casus waar uw organisatie via de eigen werkzaamheden bekend mee is (of een verwijzing hiernaar).

Tot slot willen wij weten of er volgens u bepaalde terrorismefinanciering-dreigingen bestaan die nu nog niet in Nederland zijn gesignaleerd maar in de toekomst wel actueel kunnen worden.

Wij behandelen de door u aangeleverde informatie vertrouwelijk en bij de verwerking hiervan worden geen persoonlijke gegevens opgeslagen. Wel is het voor ons van belang te weten welke organisaties gerespondeerd hebben. Om deze reden vragen we u aan te geven namens welke organisatie u de enquête invult.

Enquêtevraag 1: Namens welke organisatie vult u de enquête in? (verplicht invullen)

Enquêtevraag 2a

Aan u wordt gevraagd om in de longlist van terrorismefinanciering-dreigingen *bij iedere dreiging* een van de volgende letters te markeren:

- een **F** indien er volgens u sprake is van deze dreiging en er via de eigen werkzaamheden één of meer **Feiten/casussen** bekend zijn bij uw organisatie;
- een **A** indien het volgens u **A**nnemelijk is dat deze dreiging speelt maar er via de eigen werkzaamheden geen feiten/casussen bekend zijn bij uw organisatie;
- een **N** indien het volgens u **N**iet aannemelijk is dat deze dreiging speelt op basis van de informatie waarover uw organisatie via de eigen werkzaamheden beschikt;
- een **O** indien het voor u **O**nbekend is of een dreiging speelt, omdat uw organisatie geen zicht heeft hierop via de eigen werkzaamheden, of omdat u de dreiging niet kent.

Welke letter is van toepassing op iedere dreiging in onderstaande longlist van terrorismefinanciering-dreigingen? (per dreiging kunt u 1 letter aanvinken, verplicht invullen)

Dreiging	F	A	N	O
1. Financiering via girale transacties bij vergunde banken
2. Financiering via contante transacties/stortingen bij vergunde banken
3. Financiering via onvergunde banken
4. Financiering via girale transacties bij vergunde betaaldienstverleners
5. Financiering via contante transacties/stortingen bij vergunde betaaldienstverleners
6. Financiering via onvergunde betaaldienstverleners
7. Financiering via ondergronds bankieren
8. Financiering via (derdengeldenrekeningen via) notarissen
9. Financiering via (derdengeldenrekeningen via) advocaten

Dreiging	F	A	N	O
10. Financiering via charitatieve stichtingen, verenigingen of een andere rechtsvorm met een CBF-keurmerk
11. Financiering via charitatieve stichtingen, verenigingen of een andere rechtsvorm zonder een CBF-keurmerk
12. Financiering via stichtingen, verenigingen of een andere rechtsvorm met een religieus oogmerk in Nederland
13. Financiering via <i>buitenlandse</i> stichtingen, verenigingen of een andere rechtsvorm met een religieus oogmerk
14. Financiering via andere rechtsvormen
15. Financiering via vergunde aanbieders van cryptodiensten
16. Financiering via onvergunde aanbieders van cryptodiensten
17. Financiering met legaal verkregen eigen middelen (bijvoorbeeld salaris of inkomsten uit eigen onderneming)
18. Financiering met legaal verkregen middelen via leningen van particulieren (waaronder familie/vrienden)
19. Financiering met legaal verkregen middelen via giften van particulieren (al dan niet via (<i>online</i>) <i>crowdfunding</i> , bijvoorbeeld voor zogenaamde 'goede doelen')
20. Financiering met middelen verkregen via verticale fraude
21. Financiering met middelen verkregen via horizontale fraude
22. Financiering met middelen verkregen via een andere criminaliteitsvorm dan fraude
23. Financiering via leningen van particulieren (waaronder familie/vrienden), waarbij de middelen zijn verkregen via een vorm van criminaliteit
24. Financiering via giften van particulieren (al dan niet via (<i>online</i>) <i>crowdfunding</i> , bijvoorbeeld voor zogenaamde 'goede doelen'), waarbij de middelen zijn verkregen via een vorm van criminaliteit
25. Financiering via handel in/overdracht van (grootwaarde)producten (<i>goud, juwelen, auto's, prepaidkaarten, telefoonkaarten e.d.</i>)
26. Financiering via fysieke overdracht van (grote hoeveelheden) contant geld
27. Financiering via fictieve goederenstromen
28. Financiering via inzet van tussenpersonen (<i>katvangers, stromannen, geldkoeriers, money mules</i>)

Enquêtevraag 2b: Volgens u is er van onderstaande dreiging(en) sprake en is er via de eigen werkzaamheden één of meer Feiten/casus bekend bij uw organisatie. Kunt u voor deze dreiging(en) een beknopte beschrijving van een Feit/casus (of een verwijzing hiernaar) geven? (niet verplicht invullen)

1. ...
2. ...
3. ...
Etc.

Enquêtevraag 3a: Welke terrorismefinanciering-dreigingen heeft u gemist in de longlist die in enquêtevraag 2a wordt weergegeven? (niet verplicht invullen)

1. ...
2. ...
3. ...
4. ...
5. ...

Enquêtevraag 3b: Volgens u is er van onderstaande dreiging(en) sprake en is er via de eigen werkzaamheden één of meer Feiten/casus bekend bij uw organisatie. Kunt u voor deze dreiging(en) een beknopte beschrijving van een Feit/casus (of een verwijzing hiernaar) geven? (niet verplicht invullen)

1. ...
2. ...
3. ...
4. ...
5. ...

Enquêtevraag 4: Welke terrorismefinanciering-dreigingen zijn in Nederland nog niet gesignaleerd maar zouden in de toekomst actueel kunnen worden? (niet verplicht invullen)

1. ...
2. ...
3. ...
4. ...
5. ...

Enquêtevraag 5: Ruimte voor opmerkingen (*niet verplicht invullen*)

...

Hartelijk dank voor het invullen van de FANO-enquête.

Responsoverzicht

Tabel B4.1 Lijst van respondenten FANO-enquête (aangeschreven organisaties)

Organisatie	Organisatie
ABN-AMRO	ING
Autoriteit Financiële Markten	International Card Services
Belastingdienst	Kansspelautoriteit
Bureau Economische Handhaving	Nationale Politie
Bureau Financieel Toezicht	Nederlandse Beroepsorganisatie van Accountants
Bureau Toezicht Wwft	Nederlandse Orde van Advocaten
Centraal Bureau Fondsenwerving	Nederlandse Vereniging van Banken
De Nederlandsche Bank	Nederlandse Vereniging Geld Transactie Kantoren
Douane Nederland	Openbaar Ministerie
Financial Intelligence Unit Nederland	Verenigde Bitcoinbedrijven Nederland
Fiscale Inlichtingen- en Opsporingsdienst	Vereniging Nederlandse Organisaties Vrijwilligerswerk
Fondsen in Nederland (Partin heeft enquête ingevuld)	Volksbank
HS Collective	

Bijlage 5 Van longlist naar shortlist grootste tf-dreigingen

Tabel B5.1 Resultaten FANO-enquête (n=25)

Longlist terrorismefinanciering-dreigingen	F	A	N	O
Financiering via charitatieve stichtingen, verenigingen of een andere rechtsvorm zonder een CBF-keurmerk	8	8	4	5
Financiering via girale transacties bij vergunde banken	7	7	7	4
Financiering via stichtingen, verenigingen of een andere rechtsvorm met een religieus oogmerk in Nederland	6	9	4	6
Financiering met legaal verkregen middelen via giften van particulieren, al dan niet via (<i>online</i>) <i>crowdfunding</i> (bijvoorbeeld voor zogenaamde 'goede doelen')	6	8	5	6
Financiering via contante transacties/stortingen bij vergunde banken	6	7	7	5
Financiering met middelen verkregen via verticale fraude	6	6	3	10
Financiering via <i>buitenlandse</i> stichtingen, verenigingen of een andere rechtsvorm met een religieus oogmerk	5	10	3	7
Financiering met legaal verkregen eigen middelen	5	9	4	7
Financiering via ondergronds bankieren	5	8	6	6
Financiering met legaal verkregen middelen via leningen van particulieren (waaronder familie/vrienden)	4	9	5	7
Financiering via inzet van tussenpersonen	4	9	3	9
Financiering via contante transacties/stortingen bij vergunde betaaldienstverleners	4	5	8	8
Financiering via andere rechtsvormen	3	12	3	7
Financiering met middelen verkregen via horizontale fraude	3	10	2	10
Financiering via girale transacties bij vergunde betaaldienstverleners	3	7	9	6
Financiering via fictieve goederenstromen	3	7	3	12
Financiering via fysieke overdracht van (grote hoeveelheden) contant geld	2	9	5	9
Financiering via handel in/overdracht van (grootwaarde)producten	2	8	4	11
Financiering via onvergunde betaaldienstverleners	2	7	6	10
Financiering via vergunde aanbieders van cryptodiensten	1	14	2	8
Financiering met middelen verkregen via een andere criminaliteitsvorm dan fraude	1	11	3	10
Financiering via leningen van particulieren (waaronder familie/vrienden), waarbij de middelen zijn verkregen via een vorm van criminaliteit	1	10	3	11

Tabel B5.2 Resultaten 1^e identificatieronde grootste dreigingen (n=8)

Longlist terrorismefinanciering-dreigingen	Aantal	Aandeel
Financiering via stichtingen of verenigingen zonder een accountants-gecontroleerd keurmerk	8	100%
Financiering via onvergunde banken of ondergronds bankieren	8	100%
Financiering met legaal verkregen middelen via giften	5	63%
Financiering met legaal verkregen eigen middelen (bijv. salaris, inkomsten uit eigen onderneming, middelen ter gebruik bij terrorismefinanciering)	5	63%
Financiering via girale transacties bij vergunde banken	5	63%
Financiering met middelen verkregen via horizontale fraude	4	50%
Financiering met legaal verkregen middelen via <i>crowdfunding</i> platforms	4	50%
Financiering met legaal verkregen middelen via leningen (waaronder familie/vrienden)	4	50%
Financiering via contante transacties/stortingen bij vergunde banken	4	50%
Financiering door middel van verkoop van producten (bijv. extremistische memorabilia)	3	38%
Financiering via fysiek (grensoverschrijdend) vervoer/ overdracht van (grote hoeveelheden) contant geld	3	38%
Financiering met legaal verkregen middelen via betaalverzoeken	3	38%
Financiering via in Nederland onvergunde aanbieders van cryptodiensten	3	38%
Financiering via onvergunde betaaldienstverleners	3	38%
Financiering via fictieve goederenstromen / dienstverlening	2	25%
Financiering via handel in/ (grensoverschrijdend) vervoer/overdracht van (grootwaarde)producten	2	25%
Financiering met middelen verkregen via een andere criminaliteitsvorm dan fraude	2	25%
Financiering met middelen verkregen via verticale fraude	2	25%
Financiering via in Nederland vergunde aanbieders van cryptodiensten	2	25%
Financiering via andere rechtsvormen in Nederland	2	25%
Financiering via buitenlandse banken (buitenlandse IBAN's)	2	25%
Financiering via girale transacties bij vergunde betaaldienstverleners	2	25%
Financiering via contante transacties/stortingen bij vergunde betaaldienstverleners	1	13%
Financiering via inzet van tussenpersonen	0	0%
Financiering via buitenlandse rechtsvormen (bijv. via stichtingen of verenigingen)	0	0%
Financiering via stichtingen of verenigingen met een accountants-gecontroleerd keurmerk (CBF e.d.)	0	0%
Financiering via (derdengeldenrekeningen via) advocaten	0	0%
Financiering via (derdengeldenrekeningen via) notarissen	0	0%

Tabel B5.3 Resultaten 2^e identificatieronde grootste dreigingen (n=8)

Longlist terrorismefinanciering-dreigingen	Aantal	Aandeel
Financiering via in Nederland onvergunde aanbieders van cryptodiensten	8	100%
Financiering met legaal verkregen eigen middelen (bijv. salaris, inkomsten uit eigen onderneming, middelen ter gebruik bij terrorismefinanciering)	6	75%
Financiering via buitenlandse banken (buitenlandse IBAN's)	6	75%
Financiering via stichtingen of verenigingen zonder een accountants-gecontroleerd keurmerk	6	75%
Financiering via onvergunde betaaldienstverleners / onvergunde banken	6	75%
Financiering met middelen verkregen via horizontale fraude	4	50%
Financiering met legaal verkregen middelen via <i>crowdfunding</i> platforms	4	50%
Financiering via girale of contante transacties bij vergunde betaaldienstverleners	4	50%
Financiering via girale transacties bij vergunde banken	4	50%
Financiering via fysiek (grensoverschrijdend) vervoer/ overdracht van (grote hoeveelheden) contant geld	3	38%
Financiering met middelen verkregen via een andere criminaliteitsvorm dan fraude	3	38%
Financiering met middelen verkregen via verticale fraude	3	38%
Financiering met legaal verkregen middelen via giften	3	38%
Financiering via in Nederland vergunde aanbieders van cryptodiensten	3	38%
Financiering via contante transacties/stortingen bij vergunde banken	3	38%
Financiering door middel van verkoop van producten (bijv. extremistische memorabilia)	2	25%
Financiering via handel in/ (grensoverschrijdend) vervoer/overdracht van (grootwaarde)producten	2	25%
Financiering met legaal verkregen middelen via betaalverzoeken	2	25%
Financiering met legaal verkregen middelen via leningen (waaronder familie/vrienden)	2	25%
Financiering via andere rechtsvormen in Nederland	2	25%
Financiering via inzet van tussenpersonen	1	13 %
Financiering via fictieve goederenstromen / dienstverlening	1	13 %
Financiering via buitenlandse rechtsvormen (bijv. via stichtingen of verenigingen)	1	13 %
Financiering via ondergronds bankieren	1	13 %
Financiering via stichtingen of verenigingen met een accountants-gecontroleerd keurmerk (CBF e.d.)	0	0%
Financiering via (derdengeldenrekeningen via) advocaten	0	0%
Financiering via (derdengeldenrekeningen via) notarissen	0	0%

Tabel B5.4 Voorlopige en definitieve shortlist grootste tf-dreigingen

Voorlopige shortlist	Definitieve shortlist
Financiering via girale transacties bij vergunde banken	Financiering via girale of contante transacties bij vergunde banken
Financiering via contante transacties/stortingen bij vergunde banken	
Financiering via buitenlandse banken (buitenlandse IBAN's)	Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen
Financiering via girale of contante transacties bij vergunde betaaldienstverleners	Financiering via girale of contante transacties bij vergunde geldtransactiekantoren
	Financiering via internet betaaldiensten (PSP's)
Financiering via in Nederland vergunde aanbieders van cryptodiensten	Financiering via aanbieders van cryptodiensten
Financiering via in Nederland onvergunde aanbieders van cryptodiensten	
Financiering via onvergunde betaaldienstverleners / onvergunde banken	Financiering via onvergunde betaaldienstverleners en hawala-bankieren
Financiering via fysiek (grensoverschrijdend) vervoer/overdracht van (grote hoeveelheden) contant geld	Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland
Financiering via stichtingen of verenigingen zonder een accountants-gecontroleerd keurmerk	Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering (CBF-erkenning en/of ander keurmerk/gedragscodes)
Financiering met middelen verkregen via horizontale fraude	Financiering met middelen verkregen via horizontale/verticale fraude dan fraude
Financiering met middelen verkregen via verticale fraude	
Financiering met middelen verkregen via een andere criminaliteitsvorm dan fraude	Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude
Financiering met legaal verkregen eigen middelen (bijvoorbeeld salaris, inkomsten uit eigen onderneming, middelen ter gebruik bij terrorismefinanciering)	Financiering met legaal verkregen eigen middelen (bijv. salaris, inkomsten uit eigen onderneming, middelen om terrorisme te plegen)
Financiering met legaal verkregen middelen via giften	Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media
Financiering met legaal verkregen middelen via <i>crowdfunding</i> platforms	

Bijlage 6 Potentiële impact grootste tf-dreigingen

Tabel B6.1 Resultaten 1^e ronde toekennen gewicht MCA-criteria (op een schaal van 0-10, n=8)

criterium	Gewicht
Prevalentie terroristische activiteiten in Nederland	7,5
Prevalentie terroristische activiteiten in het buitenland	6,8
Aantasting financiële sector	6,5
Vermindering subjectieve veiligheid	6,4
Ondermijning gezag	6,1
Aantasting imago Nederland in het buitenland	5,8

Tabel B6.2 Resultaten 2^e ronde toekennen gewicht MCA-criteria (op een schaal van 0-10, n=8)

criterium	Gewicht
Prevalentie terroristische activiteiten in Nederland	8,0
Prevalentie terroristische activiteiten in het buitenland	7,3
Aantasting financiële sector	6,6
Vermindering subjectieve veiligheid	6,3
Ondermijning gezag	6,1
Aantasting imago Nederland in het buitenland	5,8

Tabel B6.3 Resultaten 1^e inschattingsronde potentiële impact van grootste tf-dreigingen (op een schaal van 0-100, n=8)^a

Dreiging	Criterium A	Criterium B	Criterium C	Criterium D	Criterium E	Criterium F	Potentiële impact
Financiering via girale of contante transacties bij vergunde banken	55,8	55,0	40,0	56,3	73,8	65,0	57,5
Financiering met middelen verkregen via horizontale/verticale fraude	66,9	62,5	41,3	63,8	55,0	46,3	56,6
Financiering via onvergunde betaaldienstverleners en/of hawala-bankieren	66,3	71,3	41,3	57,5	51,3	43,8	56,2
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	59,4	59,4	36,3	55,0	60,6	60,0	55,4
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	55,6	63,8	33,8	53,8	66,3	52,5	54,7
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude	50,6	56,3	48,8	61,9	54,4	54,4	54,2
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering (CBF-erkenning en/of ander keurmerk/gedragscodes)	61,3	58,8	40,0	51,9	49,4	56,9	53,4
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	53,8	60,0	38,8	57,5	45,0	60,0	52,6
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	70,0	60,0	34,4	44,4	42,5	40,0	49,8
Financiering met legaal verkregen eigen middelen (bijv. salaris, inkomsten uit eigen onderneming, middelen om terrorisme te plegen)	80,0	68,1	33,1	34,4	35,6	35,0	49,7
Financiering via internet betaaldiensten (PSP's)	50,0	51,3	33,8	46,3	58,8	53,8	49,1
Financiering via aanbieders van cryptodiensten	50,0	58,8	32,5	47,5	49,4	47,5	48,0

a Criterium A = Prevalentie terroristische activiteiten in Nederland; Criterium B = Prevalentie terroristische activiteiten in het buitenland; Criterium C = Vermindering subjectieve veiligheid; Criterium D = Ondernijming gezag; Criterium E = Aantasting financiële sector; Criterium F = Aantasting imago Nederland in het buitenland.

Tabel B6.4 Resultaten 2^e inschattingsronde potentiële impact van grootste terrorismefinanciering-dreigingen (op een schaal van 0-100, n=8)^a

Dreiging	Criterium A	Criterium B	Criterium C	Criterium D	Criterium E	Criterium F	Potentiële impact
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	75,0	73,8	50,0	62,5	52,5	45,0	60,9
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	60,0	66,3	46,3	61,3	50,0	61,3	57,7
Financiering met middelen verkregen via horizontale/verticale fraude	66,9	62,5	41,3	63,8	55,0	46,3	56,6
Financiering via girale of contante transacties bij vergunde banken	53,1	53,8	40,0	55,0	73,8	65,0	56,6
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering (CBF-erkenning en/of ander keurmerk/gedragscodes)	62,5	60,0	48,8	55,6	49,4	56,9	55,9
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	59,4	59,4	36,3	55,0	60,6	60,0	55,4
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	56,3	63,8	33,8	52,5	67,5	55,0	55,2
Financiering met middelen verkregen via andere criminaliteitsvorm dan fraude	50,6	56,3	50,0	63,1	54,4	54,4	54,6
Financiering met legaal verkregen eigen middelen (bijv. salaris, inkomsten uit eigen onderneming, middelen om terrorisme te plegen)	82,5	69,4	33,1	34,4	35,6	35,0	50,4
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	68,8	60,0	34,4	44,4	43,8	40,0	49,8
Financiering via internet betaaldiensten (PSP's)	51,3	51,3	33,8	46,3	58,8	55,0	49,5
Financiering via aanbieders van cryptodiensten	52,5	56,3	31,3	46,3	49,4	47,5	47,7

a Criterium A = Prevalentie terroristische activiteiten in Nederland; Criterium B = Prevalentie terroristische activiteiten in het buitenland; Criterium C = Vermindering subjectieve veiligheid; Criterium D = Ondernijming gezag; Criterium E = Aantasting financiële sector; Criterium F = Aantasting imago Nederland in het buitenland.

Bijlage 7 Weerbaarheid grootste tf-dreigingen

Tabel B7.1 Resultaten 1^e inschattingsronde weerbaarheid beleidsinstrumentarium per grootste tf-dreiging (op een schaal van 0-100, n=6)

Dreiging	Weerbaarheid
Financiering via girale of contante transacties bij vergunde banken	60,0
Financiering met middelen verkregen via horizontale/verticale fraude	60,0
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	56,7
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	45,0
Financiering via internet betaaldiensten (PSP's)	44,2
Financiering met middelen verkregen via andere criminaliteitsvorm	44,2
Financiering met legaal verkregen eigen middelen (bijv. salaris, inkomsten uit eigen onderneming, middelen om terrorisme te plegen)	41,8
Financiering via aanbieders van cryptodiensten	40,8
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering (CBF-erkenning en/of ander keurmerk/gedragscode)	40,8
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	40,0
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	26,7
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	24,2

Tabel B7.2 Resultaten 2^e inschattingsronde weerbaarheid beleidsinstrumentarium per grootste tf-dreiging (op een schaal van 0-100, n=6)

Dreiging	Weerbaarheid
Financiering via girale of contante transacties bij vergunde banken	57,5
Financiering met middelen verkregen via horizontale/verticale fraude	56,7
Financiering via girale of contante transacties bij vergunde geldtransactiekantoren	54,2
Financiering via internet betaaldiensten (PSP's)	40,8
Financiering via stichtingen met weinig transparantie over financiën en geen zelfregulering (CBF-erkenning en/of ander keurmerk/gedragscode)	40,8
Financiering via giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	39,2
Financiering met middelen verkregen via andere criminaliteitsvorm	35,8
Financiering via fysieke verplaatsing van (grote hoeveelheden) contant geld of grootwaardeproducten in/via Nederland of naar/vanuit het buitenland	34,2
Financiering via onvergunde betaaldienstverleners en hawala-bankieren	27,5
Financiering met legaal verkregen eigen middelen (bijv. salaris, inkomsten uit eigen onderneming, middelen om terrorisme te plegen)	26,8
Financiering via aanbieders van cryptodiensten	25,0
Financiering via laagdrempelige (<i>online</i>) mogelijkheden om buitenlandse bankrekening te openen	23,3

Bijlage 8 Aanvullende analyses

De Resterende Potentiële Impact (RPI) van de dreigingen (tabel B8.1) maakt inzichtelijk in welke mate de potentiële impact van de dreigingen wordt tegengegaan door de weerbaarheid.¹⁴⁹

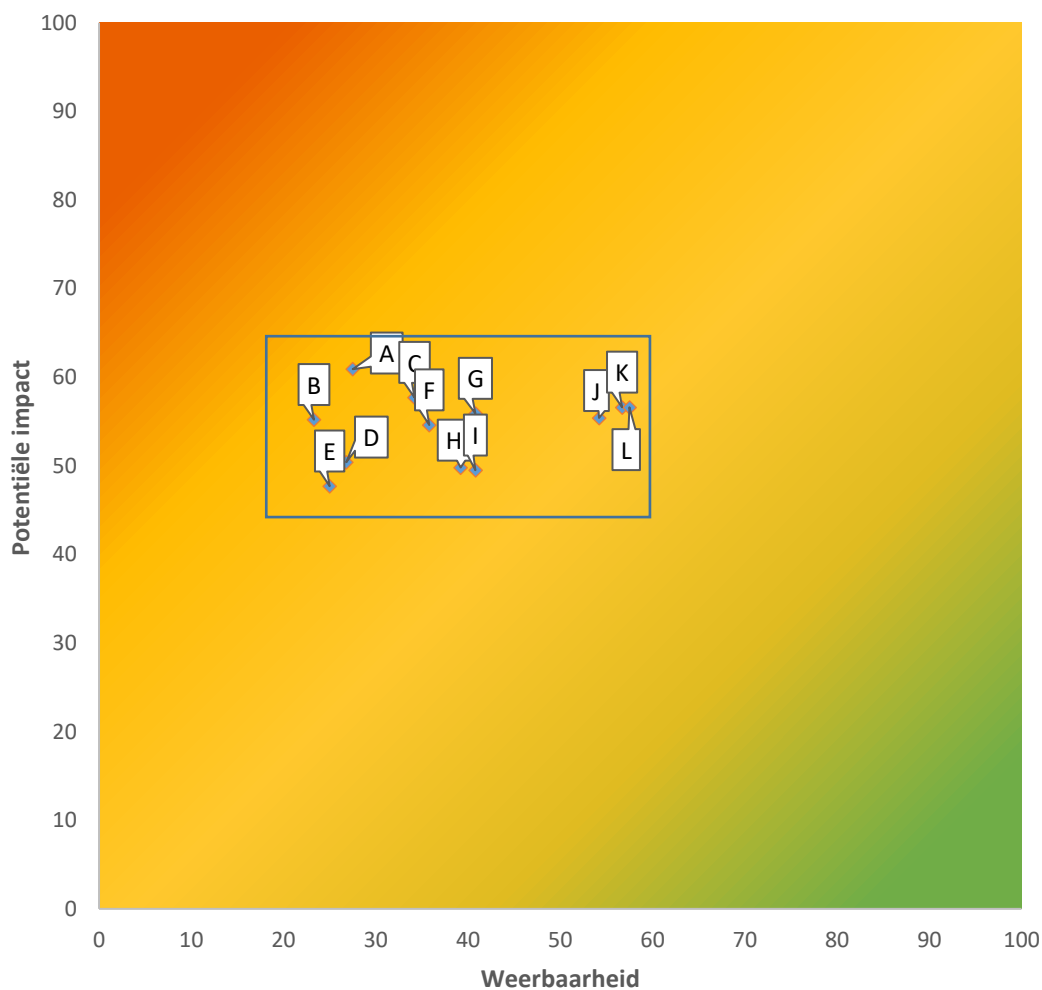
Tabel B8.1 RPI-scores van de 12 grootste tf-dreigingen

Dreiging	Potentiële impact	Weerbaarheid	RPI
Onvergonde betaaldienstverleners en hawala-bankieren	61	28	44
Laagdrempelige (<i>online</i>) mogelijkheden openen buitenlandse bankrekening	55	23	42
Fysieke verplaatsing (grote hoeveelheden) contant geld/grootwaardeproducten	58	34	38
Legaal verkregen eigen middelen	50	27	37
Aanbieders cryptodiensten	48	25	36
Middelen verkregen via andere criminaliteitsvorm dan fraude	55	36	35
Stichtingen met weinig transparantie over financiën en geen zelfregulering	56	41	33
Giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media	50	39	30
Internet betaaldiensten (PSP's)	50	41	29
Girale/contante transacties vergunde geldtransactiekantoren	55	54	25
Middelen verkregen via horizontale/verticale fraude	57	57	25
Girale/contante transacties vergunde banken	57	58	24

Figuur B8.1 geeft de volledige *heatmap* voor de derde NRA Terrorismefinanciering weer, waarbij de assen voor potentiële impact en weerbaarheid lopen van 0 tot en met 100. Blauw gekaderd wordt de uitsnede van de *heatmap* weergegeven die in het conclusiehoofdstuk is opgenomen.

¹⁴⁹ RPI = Potentiële Impact * (100 – Weerbaarheid) / 100).

Figuur B8.1 Volledige heatmap derde NRA Terrorismefinanciering^a



A	Onvergunde betaaldienstverleners en hawala-bankieren	G	Stichtingen met weinig transparantie over financiën en geen zelfregulering
B	Laagdrempelige (<i>online</i>) mogelijkheden openen buitenlandse bankrekening	H	Giften via betaalverzoeken en/of <i>crowdfunding</i> via sociale media
C	Fysieke verplaatsing (grote hoeveelheden) contant geld/grootwaardeproducten	I	Internet betaaldiensten (PSP's)
D	Legaal verkregen eigen middelen	J	Girale/contante transacties vergunde geldtransactiekantoren
E	Aanbieders cryptodiensten	K	Middelen verkregen via horizontale/verticale fraude
F	Middelen verkregen via andere criminaliteitsvorm dan fraude	L	Girale/contante transacties bij vergunde banken

a In de weergegeven figuur lopen de assen van 0 tot en met 100, waarbij de kleuren verlopen van linksboven: rood (hoogste potentiële impact en laagste weerbaarheid) naar rechtsonder: groen (laagste potentiële impact en hoogste weerbaarheid).

Samenhang RPI-scores derde NRA's Terrorismefinanciering en Witwassen

In de validatiefase van het onderzoek is een analyse uitgevoerd op de acht dreigingen die zowel bij de derde NRA voor terrorismefinanciering als bij de derde NRA voor witwassen voorkomen in de lijst van grootste dreigingen. Tabel B8.2 geeft de RPI-scores voor de beide NRA's.

Tabel B8.2 RPI-scores voor de qua strekking overlappende dreigingen van de derde NRA's voor witwassen en terrorismefinanciering

Dreiging	RPI-scores 3 ^e NRA Witwassen	RPI-scores 3 ^e NRA Terrorismefinanciering
Ondergronds bankieren en/of hawala-bankieren	42,2	44,2
Laagdrempelig openen buitenlandse bankrekening	41,4	42,3
Fysieke verplaatsing grote hoeveelheden contant geld/grootwaardeproducten	37,1	38,0
Minder transparante Nederlandse rechtsvormen	37,0	33,1
Aanbieders financiële cryptodiensten	36,1	35,8
Payment Service Providers	35,7	29,3
Vergunde geldtransactiekantoren	26,7	25,4
Vergunde banken ¹⁵⁰	22,4	24,1

De toegepaste methode bij de NRA's voor witwassen en terrorismefinanciering is qua grondvorm identiek. Wel zijn de gegevens voor de verschillende NRA's bij grotendeels verschillende experts verzameld en ook zijn de toegepaste criteria voor de MCA's niet identiek. Er wordt een sterke samenhang tussen de RPI-scores voor de derde NRA's voor terrorismefinanciering en witwassen gevonden (Pearsons R = 0,92, p = 0,001, N = 8).

¹⁵⁰ Voor de dreiging vergunde banken bij de derde NRA Witwassen is uitgegaan van de gemiddelde score voor girale en contante transacties.

Bijlage 9 Kwantitatieve data Justis/TRACK

Tabel B9.1 Stichtingen, oprichtingen en betrokken bestuurders in 2020-2022

Jaar	Totaal	Oprichtingen	Bestuurders	Aantal bestuurders per oprichting
2020	238.123	9.934	22.870	2,3
2021	240.714	9.640	22.122	2,3
2022	240.064	9.088	20.513	2,3

Tabel B9.2 Aantal opgerichte stichtingen naar hoofdbranche in 2020-2022

Hoofdbranche o.b.v. 3 cijferige SBI-codes	2020	2021	2022
Levensbeschouwelijke en politieke organisaties, belangen- en ideële organisaties, hobbyclubs (SBI-code 94.9)	3.111	3.003	2.842
Financiële holdings (SBI-code 64.2)	1.985	1.953	2.251
Financiële bemiddeling, advisering e.d. ^a (SBI-code 66.1)	1.259	1.487	1.254
Maatschappelijke dienstverlening ^b (SBI-code 88.9)	879	797	680
Overig	2.702	2.400	2.061
Totaal	9.936	9.640	9.088

a Niet voor verzekeringen en pensioenfondsen.

b Zonder overnachting niet specifiek gericht op ouderen en gehandicapten.

Tabel B9.3 Aantal bestuurders (natuurlijke personen en rechtspersonen) naar aantal opgerichte stichtingen in 2020-2022

	1-20 oprichtingen	21-50 oprichtingen	51-100 oprichtingen	101 en meer oprichtingen
2020	<i>Natuurlijke persoon</i>			
Bestuurder in Nederland gevestigd	19.751	0	0	0
Bestuurder in buitenland gevestigd	1.135	1	0	0
	<i>Rechtspersoon</i>			
Bestuurder in Nederland gevestigd	742	2	0	0
Bestuurder in buitenland gevestigd	4	0	0	0
2021	<i>Natuurlijke persoon</i>			
Bestuurder in Nederland gevestigd	18.942	2	0	0
Bestuurder in buitenland gevestigd	1.017	0	0	0
	<i>Rechtspersoon</i>			
Bestuurder in Nederland gevestigd	858	3	1	0
Bestuurder in buitenland gevestigd	1	0	0	0
2022	<i>Natuurlijke persoon</i>			
Bestuurder in Nederland gevestigd	17.411	2	0	0
Bestuurder in buitenland gevestigd	922	0	0	0
	<i>Rechtspersoon</i>			
Bestuurder in Nederland gevestigd	876	0	1	0
Bestuurder in buitenland gevestigd	4	0	0	0

Tabel B9.4 Aantal bestuurders dat direct betrokken is bij stichtingen in 2020-2022

	1-20 stichtingen	21-50 stichtingen	51-100 stichtingen	101 en meer stichtingen
2020	<i>Natuurlijk persoon</i>			
Bestuurder in Nederland gevestigd	26.448	16	4	0
Bestuurder in buitenland gevestigd	1.297	0	0	2
	<i>Rechtspersoon</i>			
Bestuurder in Nederland gevestigd	1.125	15	6	7
Bestuurder in buitenland gevestigd	4	0	0	0
2021	<i>Natuurlijk persoon</i>			
Bestuurder in Nederland gevestigd	26.346	18	2	0
Bestuurder in buitenland gevestigd	1.192	0	0	0
	<i>Rechtspersoon</i>			
Bestuurder in Nederland gevestigd	1.278	13	8	5
Bestuurder in buitenland gevestigd	1	0	0	0
2022	<i>Natuurlijk persoon</i>			
Bestuurder in Nederland gevestigd	23.857	16	1	0
Bestuurder in buitenland gevestigd	1.031	0	0	0
	<i>Rechtspersoon</i>			
Bestuurder in Nederland gevestigd	1.229	11	9	5
Bestuurder in buitenland gevestigd	4	0	0	0

Tabel B9.5 Aantal bestuurswisselingen bij stichtingen binnen 0 t/m 30 dagen in 2020-2022

	2020	2021	2022
	<i>Natuurlijke persoon</i>		
Bestuurder in Nederland gevestigd	106	121	102
Bestuurder in buitenland gevestigd	13	8	7
	<i>Rechtspersoon</i>		
Bestuurder in Nederland gevestigd	7	18	19
Bestuurder in buitenland gevestigd	0	0	0

Het Wetenschappelijk Onderzoek- en Datacentrum (WODC) is het kennisinstituut voor het ministerie van Justitie en Veiligheid. Het WODC doet zelf onafhankelijk wetenschappelijk onderzoek of laat dit doen door erkende instituten en universiteiten, ter ondersteuning van beleid en uitvoering.

Meer informatie:

www.wodc.nl