POLITIE

Nationaal dreigingsbeeld 2017
Georganiseerde criminaliteit

Frank Boerman
Martin Grapendaal
Fred Nieuwenhuis
Ewout Stoffers

« waakzaam en dienstbaar »

Nationaal dreigingsbeeld 2017
Georganiseerde criminaliteit

Frank Boerman
Martin Grapendaal
Fred Nieuwenhuis
Ewout Stoffers

Uitgave
Dienst Landelijke Informatieorganisatie
Postbus 100
3970 AC Driebergen
De Dienst Landelijke Informatieorganisatie is onderdeel van de Landelijke Eenheid

Zoetermeer, mei 2017

Colofon
Tekst Frank Boerman, Martin Grapendaal, Fred Nieuwenhuis, Ewout Stoffers
Eindredactie Irene Spijker en Iet Voorhoeve
Foto omslag Shutterstock
Opmaak Politiedienstencentrum, Rotterdam
Druk Moduli Print, Horn

Copyright
©2017 Politie, all rights reserved.
Niets uit deze uitgave mag worden verveelvoudigd, op geautomatiseerde wijze opgeslagen of openbaar gemaakt in enige vorm of op enigerlei wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de Politie.

Aan de totstandkoming van deze uitgave is de uiterste zorg besteed. Voor informatie die nochtans onvolledig of onjuist is opgenomen, aanvaarden de auteur(s), redactie en de Landelijke Eenheid geen aansprakelijkheid. Voor eventuele verbeteringen van de opgenomen gegevens houden zij zich gaarne aanbevolen.

Inhoudsopgave

Voorwoord 11

Dankwoord. 13

Deel 1

Introductie. 15

1. Verantwoording. 17
1.1 Opdracht 17
1.2 Theoretisch model 18
1.3 Doelstelling 19
1.4 Afbakening. 19
1.5 Onderzoeksvragen 21
1.6 Deelprojecten 22
1.7 Kwalificatie 23
1.8 Aanvullende toelichting op de begripsafbakening van 'dreiging' 26
1.9 Nieuw ten opzichte van het NDB2012 28
1.10 Ten slotte 29

2. De kwalificaties in een oogopslag 31

Deel 2

Beschrijving en kwalificatie van de criminele verschijnselen 33

1. Illegale markten 35
1.1 Inleiding 35
1.2 Handel in en smokkel van cocaïne. 35
1.2.1 Inleiding 35
1.2.2 Ontwikkelingen in aard en omvang sinds het NDB2012 35
1.2.3 Huidige gevolgen 41
1.2.4 Verwachtingen 42
1.2.5 Kwalificatie van dreiging 44
1.3 Handel in en smokkel van heroïne 45
1.3.1 Inleiding 45
1.3.2 Ontwikkelingen in aard en omvang sinds het NDB2012 45
1.3.3 Huidige gevolgen 48
1.3.4 Verwachtingen 49
1.3.5 Kwalificatie van dreiging 50
1.4 Productie van, handel in en smokkel van synthetische drugs . . 51

1.4.1 Inleiding 51
1.4.2 Ontwikkelingen in aard en omvang sinds het NDB2012 51
1.4.3 Huidige gevolgen 55
1.4.4 Verwachtingen 56
1.4.5 Kwalificatie van dreiging 58
1.5 Productie van, handel in en smokkel van cannabis 59
1.5.1 Inleiding 59
1.5.2 Ontwikkelingen in aard en omvang sinds het NDB2012 59
1.5.3 Huidige gevolgen 62
1.5.4 Verwachtingen 65
1.5.5 Kwalificatie van dreiging 68
1.6 Seksuele uitbuiting 69
1.6.1 Inleiding 69
1.6.2 Ontwikkelingen in aard en omvang sinds het NDB2012 69
1.6.3 Huidige gevolgen 74
1.6.4 Verwachtingen 75
1.6.5 Kwalificatie van dreiging 77
1.7 Arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening 77
1.7.1 Inleiding 77
1.7.2 Ontwikkelingen in aard en omvang sinds het NDB2012 78
1.7.3 Huidige gevolgen 81
1.7.4 Verwachtingen 83
1.7.5 Kwalificatie van dreiging 84
1.8 Mensensmokkel 85
1.8.1 Inleiding 85
1.8.2 Ontwikkelingen in aard en omvang sinds het NDB2012 86
1.8.3 Huidige gevolgen 87
1.8.4 Verwachtingen 89
1.8.5 Kwalificatie van dreiging 91
1.9 Orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering 92
1.9.1 Inleiding 92
1.9.2 Ontwikkelingen in aard en omvang sinds 2005 93
1.9.3 Huidige gevolgen 94
1.9.4 Verwachtingen 94
1.9.5 Kwalificatie van dreiging 95
1.10 Illegale handel in vuurwapens en explosieven 96
1.10.1 Inleiding 96
1.10.2 Ontwikkelingen in aard en omvang sinds het NDB2012 96
1.10.3 Huidige gevolgen 102
1.10.4 Verwachtingen 103

1.10.5 Kwalificatie van dreiging 104
1.11 Kinderpornografie 105
1.11.1 Inleiding 105
1.11.2 Ontwikkelingen in aard en omvang sinds het NDB2012 106
1.11.3 Huidige gevolgen 108
1.11.4 Verwachtingen 108
1.11.5 Kwalificatie van dreiging 110
1.12 Productie en verspreiding van vals geld 110
1.12.1 Inleiding 110
1.12.2 Ontwikkelingen in aard en omvang sinds het NDB2012 111
1.12.3 Huidige gevolgen 113
1.12.4 Verwachtingen 113
1.12.5 Kwalificatie van dreiging 115
1.13 Matchfixing 116
1.13.1 Inleiding 116
1.13.2 Ontwikkelingen in aard en omvang sinds het NDB2012 116
1.13.3 Huidige gevolgen 119
1.13.4 Verwachtingen 119
1.13.5 Kwalificatie van dreiging 121
1.14 Illegale kansspelen 122
1.14.1 Inleiding 122
1.14.2 Ontwikkelingen in aard en omvang sinds het NDB2012 122
1.14.3 Huidige gevolgen 125
1.14.4 Verwachtingen 126
1.14.5 Kwalificatie van dreiging 127

2. Fraude en witwassen 129
2.1 Inleiding 129
2.2 Acquisitiefraude 131
2.2.1 Inleiding 131
2.2.2 Ontwikkelingen in aard en omvang sinds het NDB2012 132
2.2.3 Huidige gevolgen 134
2.2.4 Verwachtingen 134
2.2.5 Kwalificatie van dreiging 135
2.3 Hypotheekfraude 136
2.3.1 Inleiding 136
2.3.2 Ontwikkelingen in aard en omvang sinds het NDB2012 136
2.3.3 Huidige gevolgen 137
2.3.4 Verwachtingen 137
2.3.5 Kwalificatie van dreiging 138
2.4 Beleggingsfraude 138
2.4.1 Inleiding 138

2.4.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 138
2.4.3 Huidige gevolgen . . . 140
2.4.4 Verwachtingen . . . 141
2.4.5 Kwalificatie van dreiging . . . 141
2.5 Faillissementsfraude . . . 141
2.5.1 Inleiding . . . 141
2.5.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 142
2.5.3 Huidige gevolgen . . . 143
2.5.4 Verwachtingen . . . 144
2.5.5 Kwalificatie van dreiging . . . 144
2.6 Fraude met betaalmiddelen . . . 145
2.6.1 Inleiding . . . 145
2.6.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 145
2.6.3 Huidige gevolgen . . . 147
2.6.4 Verwachtingen . . . 147
2.6.5 Kwalificatie van dreiging . . . 149
2.7 Fraude met online handel . . . 149
2.7.1 Inleiding . . . 149
2.7.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 149
2.7.3 Huidige gevolgen . . . 152
2.7.4 Verwachtingen . . . 153
2.7.5 Kwalificatie van dreiging . . . 153
2.8 Telecomfraude . . . 153
2.8.1 Inleiding . . . 153
2.8.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 154
2.8.3 Huidige gevolgen . . . 155
2.8.4 Verwachtingen . . . 155
2.8.5 Kwalificatie van dreiging . . . 155
2.9 Verzekeringsfraude . . . 155
2.9.1 Inleiding . . . 155
2.9.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 156
2.9.3 Huidige gevolgen . . . 158
2.9.4 Verwachtingen . . . 158
2.9.5 Kwalificatie van dreiging . . . 159
2.10 Voorschotfraude . . . 159
2.10.1 Inleiding . . . 159
2.10.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 160
2.10.3 Huidige gevolgen . . . 161
2.10.4 Verwachtingen . . . 161
2.10.5 Kwalificatie van dreiging . . . 162
2.11 Accijnsfraude . . . 162
2.11.1 Inleiding . . . 162

2.11.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 162
2.11.3 Huidige gevolgen 166
2.11.4 Verwachtingen 168
2.11.5 Kwalificatie van dreiging 170
2.12 Fiscale fraude 171
2.12.1 Inleiding 171
2.12.2 Omvang en schade van fiscale fraude 171
2.12.3 Inleiding btw-carrouselfraude 173
2.12.4 Recente ontwikkelingen in aard en omvang van btw-carrouselfraude 175
2.12.5 Huidige gevolgen van fiscale fraude 177
2.12.6 Verwachtingen 179
2.12.7 Kwalificatie van dreiging 181
2.13 Witwassen 181
2.13.1 Inleiding 181
2.13.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 181
2.13.3 Huidige gevolgen 186
2.13.4 Verwachtingen 188
2.13.5 Kwalificatie van dreiging 191

3. Georganiseerde vermogenscriminaliteit 193
3.1 Inleiding 193
3.2 Woninginbraak 193
3.2.1 Inleiding 193
3.2.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 194
3.2.3 Huidige gevolgen 198
3.2.4 Verwachtingen 198
3.2.5 Kwalificatie van dreiging 199
3.3 Bedrijfsinbraak 200
3.3.1 Inleiding 200
3.3.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 200
3.3.3 Huidige gevolgen 202
3.3.4 Verwachtingen 202
3.3.5 Kwalificatie van dreiging 203
3.4 Winkeldiefstal 204
3.4.1 Inleiding 204
3.4.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 204
3.4.3 Huidige gevolgen 206
3.4.4 Verwachtingen 207
3.4.5 Kwalificatie van dreiging 207
3.5 Kraken op geldautomaten 208
3.5.1 Inleiding 208

3.5.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 209
3.5.3 Huidige gevolgen . . . 210
3.5.4 Verwachtingen . . . 211
3.5.5 Kwalificatie van dreiging . . . 211
3.6 Overvallen . . . 212
3.6.1 Inleiding . . . 212
3.6.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 212
3.6.3 Huidige gevolgen . . . 213
3.6.4 Verwachtingen . . . 214
3.6.5 Kwalificatie van dreiging . . . 215
3.7 Ladingdiefstal . . . 215
3.7.1 Inleiding . . . 215
3.7.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 216
3.7.3 Huidige gevolgen . . . 218
3.7.4 Verwachtingen . . . 218
3.7.5 Kwalificatie van dreiging . . . 219
3.8 Afpersing . . . 220
3.8.1 Inleiding . . . 220
3.8.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 221
3.8.3 Huidige gevolgen . . . 223
3.8.4 Verwachtingen . . . 224
3.8.5 Kwalificatie van dreiging . . . 224
3.9 Georganiseerde autocriminaliteit . . . 225
3.9.1 Inleiding . . . 225
3.9.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 225
3.9.3 Huidige gevolgen . . . 227
3.9.4 Verwachtingen . . . 227
3.9.5 Kwalificatie van dreiging . . . 228
3.10 Heling . . . 228
3.10.1 Inleiding . . . 228
3.10.2 Ontwikkelingen in aard en omvang sinds het NDB2012 . . . 229
3.10.3 Huidige gevolgen . . . 232
3.10.4 Verwachtingen . . . 233
3.10.5 Kwalificatie van dreiging . . . 234

Deel 3 **Cybercrime en milieucriminaliteit . . . 235**

1. Inleiding . . . 237

2. Cybercrime en gedigitaliseerde criminaliteit . . . 239
2.1 Inleiding . . . 239
2.2 Ontwikkelingen van cybercrime en gedigitaliseerde criminaliteit . 240

2.2.1 Cybercrime 241
2.2.2 Hightechcrime 244
2.2.3 Gedigitaliseerde criminaliteit 246
2.3 Invloed op aard en omvang van criminaliteit 249
2.4 Verwachtingen en gevolgen 253
2.4.1 Verwachtingen 253
2.4.2 Gevolgen 256
2.5 Conclusie 257

3. Milieucriminaliteit 261
3.1 Inleiding 261
3.2 Afval- en reststromen 263
3.3 Bodemketen en oppervlaktewater 271
3.4 Omgang met gevaarlijke stoffen 275
3.5 Gevolgen van milieucriminaliteit 278
3.6 Conclusie 279

Deel 4 Signaleringen en nabeschouwing 283

1. Signaleringen 285
1.1 Inleiding 285
1.2 De rol van de overheid 286
Horizontaal toezicht 286
Wet- en regelgeving in de milieusector 287
1.3 Digitale technologie 288
Internet of Things 288
Cloudcomputing 290
Crowdfunding 290
Blockchain, bitcoin en payment service provider 291
1.4 De criminele praktijk 292
Do-it-Yourself 293
Crime-as-a-Service 295
Criminele uitbesteding en professionalisering 295
Criminele veelzijdigheid 298
1.5 Georganiseerde criminaliteit in de wijken: onaantastbaarheid en normvervaging 300

2. Nabeschouwing 303
2.1 Inleiding 303
2.2 Nabeschouwing 303
2.3 Slotconclusie 311

Bijlagen 313

1. Begeleidingscommissie 315
2. Samenstelling consensusgroep 317
3. Gevolgeninstrument 319

Voorwoord

Het vierde Nationaal dreigingsbeeld georganiseerde criminaliteit (NDB) is een feit. Voortbordurend op het NDB2012 heeft opnieuw een inventarisatie plaatsgevonden van de stand van zaken rond de georganiseerde criminaliteit in Nederland. Er werden 34 verschillende vormen van georganiseerde criminaliteit onderzocht en van een dreigingsinschatting voorzien. Aparte aandacht werd besteed aan milieucriminaliteit en cybercrime. Zo'n vijftig onderzoekers en analisten hebben aan het NDB gewerkt. Daarbij waren alle eenheden van de politie betrokken, de FIOD, het Ministerie van Sociale Zaken en Werkgelegenheid, de Politieacademie en de Koninklijke Marechaussee. Een team onderzoekers van de Landelijke Eenheid heeft het hele proces van totstandkoming inhoudelijk vormgegeven, gecoördineerd en voor het eindrapport zorg gedragen.

Het NDB vormt elke vier jaar het vertrekpunt voor de beleidsvorming in de aanpak van de georganiseerde criminaliteit. Op grond van het NDB formuleert de opdrachtgever, het College van procureurs-generaal, een advies aan de minister omtrent de prioriteiten in de aanpak, om de schaarse middelen doelmatig en doeltreffend in te zetten. Dit is de hoofddoelstelling van het NDB – bijdragen aan de prioritering. Daarnaast heeft het NDB als doel het signaleren van belangwekkende ontwikkelingen die niet per se in de prioritering tot uitdrukking hoeven te komen.

Met de NDB's zijn in de loop der jaren ook twee andere effecten bereikt. Ten eerste zijn informatie en kennis uit het NDB gebruikt ter legitimatie van beleid. Het beleid dat elke vier jaar wordt vastgesteld, is niet in beton gegoten; allerlei omstandigheden kunnen ertoe nopen beleidsuitgangspunten bij te stellen. Het verleden heeft uitgewezen dat het NDB in de argumentatie daarvoor vaak een centrale rol speelt.
Het tweede effect is dat de vier opeenvolgende NDB's een informele geschiedschrijving bieden van het criminele landschap sinds het begin van deze eeuw. Zo is het buitengewoon interessant om de verschillende NDB's na te lezen op de ontwikkeling die cybercrime heeft doorgemaakt. In het NDB2004 wordt opgemerkt dat de mate waarin criminele groeperingen profiteren van de ontwikkelingen op het gebied van informatie- en communicatietechnologie, vooralsnog beperkt lijkt. In 2008 is de vaststelling dat het internet bij vrijwel alle beschreven criminele verschijnselen een rol speelt. In 2012 is het gebruik van internet 'alomtegenwoordig'. En nu, anno 2017, heeft de digitale technologie het criminele bedrijf blijvend veranderd.

Het NDB heeft aldus op verschillende manieren zijn waarde bewezen. Dat neemt niet weg dat we alert moeten blijven op de vraag of het NDB in zijn huidige beproefde vorm de 'criminele lading' nog wel dekt. Het onderzoeksdomein van het NDB is de georganiseerde criminaliteit, de criminaliteit die zich in verschillende vormen manifesteert in de

samenwerking tussen personen: de criminele samenwerkingsverbanden. Tegenwoordig profileren zich echter individuen op de criminele markt die over betrekkelijk weinig technologische *knowhow* beschikken, maar grote schade kunnen veroorzaken door middel van *ransomware* en kant-en-klare softwarepakketten die te koop zijn op het darkweb. Hier is in verminderde mate sprake van samenwerking en zien we een toename van criminele eenlingen. Tegelijkertijd is er een toenemende diversificatie in de criminele activiteiten. Waar in het verleden de criminele samenwerkingsverbanden zich beperkten tot één soort criminele bedrijvigheid, zien we nu meer en meer dat ze hun activiteiten spreiden. Er zijn bijvoorbeeld csv's die heroïne- en cocaïnehandel combineren met mensensmokkel en witwassen. Deze parallelle ontwikkelingen hebben de manier waarop we naar de georganiseerde criminaliteit kijken, veranderd. Dit zal ook consequenties hebben voor de wijze van analyseren en gebruiken van data van de georganiseerde criminaliteit.

Ten slotte wil ik mijn dank uitspreken aan iedereen die heeft bijgedragen aan dit NDB. In het bijzonder aan alle medewerkers van de genoemde organisaties die hebben meegewerkt aan de vervaardiging van het NDB. Daarnaast aan de leden van de begeleidingscommissie, die, allen vanuit de eigen deskundigheid, enthousiast het proces van totstandkoming hebben begeleid.

P.J. Aalbersberg
Politiechef Amsterdam
Portefeuillehouder intelligence en voorzitter begeleidingscommissie

Dankwoord

Dit *Nationaal dreigingsbeeld* (NDB) is het product van de inspanningen van velen. We zijn dank verschuldigd aan allen die, vaak onder tijdsdruk, een bijdrage hebben geleverd. Zonder hen zou dit NDB niet zijn wat het geworden is.

Waren eerdere NDB's aan politiezijde vooral het product van het Korps landelijke politiediensten, ditmaal hebben alle politie-eenheden meegewerkt aan de deelonderzoeken die ten behoeve van het NDB zijn uitgevoerd.
De Inspectie van het Ministerie van Sociale Zaken en Werkgelegenheid, de Koninklijke Marechaussee, onderzoeksbureau Bruinsma en de Fiscale Inlichtingen- en Opsporingsdienst hebben de onderzoeken naar respectievelijk arbeidsuitbuiting, mensensmokkel, synthetische drugs en verticale fraude voor hun rekening genomen.
Het onderzoek naar milieucriminaliteit dat de projectleiding van het NDB ter beschikking werd gesteld, werd in opdracht van de Strategische Milieukamer uitgevoerd door een team dat bestond uit medewerkers van de politie, de Politieacademie en de inlichtingen- en opsporingsdiensten van de Inspectie Leefomgeving en Transport en de Nederlandse Voedsel- en Warenautoriteit.
Interne en externe deskundigen zijn geïnterviewd voor de deelrapporten.
De leden van de begeleidingscommissie hebben het hele proces op de voet gevolgd en de auteurs van gedegen commentaar voorzien.
Collega's van de Dienst Landelijke Informatieorganisatie en het Politiedienstencentrum hebben zich ingezet voor de productie van het eindrapport: zij waren betrokken bij het corrigeren en drukklaar maken van de manuscripten.

Ten slotte noemen we enkele personen bij naam vanwege hun bijzondere verdienste: Maike Gieling, Jos Lammers, Rudie Neve, Weiko Piebes, Henk Sollie, Irene Spijker, Ewout Stoffers en Iet Voorhoeve.

Mei 2017

Dienst Landelijke Informatieorganisatie
Projectleiding NDB

Frank Boerman
Martin Grapendaal
Fred Nieuwenhuis

Deel 1

Introductie

1 Verantwoording

1.1 Opdracht

In het Besluit beheer politie[1] van 2015 is vastgelegd dat de politie in opdracht van het College van procureurs-generaal vierjaarlijks een nationaal dreigingsbeeld opstelt ten behoeve van de bestrijding van de georganiseerde criminaliteit. Het gaat om een toekomstgerichte analyse van de georganiseerde criminaliteit waarin dreigingen voor de Nederlandse samenleving zijn geëxpliciteerd. De minister van Veiligheid en Justitie stelt, op basis van een beleidsprogramma, elke vier jaar de hoofdlijnen van het beleid ter bestrijding van de georganiseerde criminaliteit vast. Het *Nationaal dreigingsbeeld* (NDB) levert een bijdrage aan dit beleidsprogramma.

Het *Nationaal dreigingsbeeld 2017* (NDB2017) heeft een aantal voorgangers. In 2004 werd in de Regeling nationale en bovenregionale recherche[2] vastgelegd dat elke vier jaar een nationaal dreigingsbeeld zou worden vervaardigd, en in datzelfde jaar verscheen bij de voormalige Dienst Nationale Recherche Informatie het *Nationaal dreigingsbeeld zware of georganiseerde criminaliteit. Een eerste proeve.*[3] In 2006 zag de *Vervolgstudie Nationaal dreigingsbeeld*[4] het licht, in 2008 het *Nationaal dreigingsbeeld 2008. Georganiseerde criminaliteit*[5] en in 2012 het *Nationaal dreigingsbeeld 2012. Georganiseerde criminaliteit*[6].

In 2013 hebben de opdrachtgever (College van procureurs-generaal) en de opdrachtnemer (korpsleiding politie) van het Nationaal dreigingsbeeld een werkgroep opdracht gegeven tot doorontwikkeling van het NDB. Daarbij diende de werkgroep rekening te houden met toekomstbestendigheid en aansluiting op gewijzigde stakeholdersverwachtingen, en verdere kwaliteitsverhoging na te streven. De werkgroep bestond uit deelnemers vanuit de politie (Landelijke Eenheid), het Openbaar Ministerie (Parket-Generaal, Landelijk Parket en Functioneel Parket) en het departement van Veiligheid en Justitie (Directie Rechtshandhaving

1 Besluit van 8 juni 2015, houdende regels over het beheer van de politie (Besluit beheer politie). *Staatsblad* 2015, 223. In het meest recente Besluit beheer politie, dat in werking is getreden op 1 januari 2017, is geen opdracht opgenomen voor het vervaardigen van een dreigingsbeeld. Zie Besluit van 9 december 2016, houdende wijziging van het Besluit beheer politie in verband met de wijziging van de inrichting van de politie. *Staatsblad* 2016, 504.

2 *Staatscourant* 2004, 19.

3 Dienst Nationale Recherche Informatie (2004). *Nationaal dreigingsbeeld zware of georganiseerde criminaliteit. Een eerste proeve.* Zoetermeer: Korps landelijke politiediensten, Dienst Nationale Recherche Informatie (afgekort als: NDB2004).

4 F. Boerman & A. Mooij (2006). *Vervolgstudie Nationaal dreigingsbeeld. Nadere beschouwing van potentiële dreigingen en witte vlekken uit het Nationaal dreigingsbeeld 2004*. Zoetermeer: Korps landelijke politiediensten, Dienst Nationale Recherche Informatie.

5 F. Boerman, M. Grapendaal & A. Mooij (2008). *Nationaal dreigingsbeeld 2008. Georganiseerde criminaliteit.* Zoetermeer: Korps landelijke politiediensten, Dienst IPOL (afgekort als: NDB2008).

6 F. Boerman, M. Grapendaal, F. Nieuwenhuis & E. Stoffers (2012). *Nationaal dreigingsbeeld 2012. Georganiseerde criminaliteit.* Zoetermeer: Korps landelijke politiediensten, Dienst IPOL (afgekort als: NDB2012).

en Criminaliteitsbestrijding). Het resultaat was een notitie met een nieuwe opdrachtformulering en projectplanning voor het volgende Nationaal dreigingsbeeld. Deze notitie vormt de basis van het NDB2017[7].

In het NDB2017 wordt de georganiseerde criminaliteit geanalyseerd en worden verwachtingen daaromtrent geformuleerd voor de periode 2017-2021.

1.2 Theoretisch model

In overeenstemming met de opdracht is het NDB2017 toekomstgericht. Daarom wordt, net als in eerdere NDB's en in de vervolgstudie uit 2006, niet alleen de huidige stand van zaken van criminele verschijnselen onderzocht, maar gaat de aandacht ook uit naar maatschappelijke factoren die op criminele verschijnselen van invloed zijn of kunnen zijn. Deze worden aangeduid als criminaliteitsrelevante factoren. De invloed van deze factoren op aard, omvang en ernst van de criminaliteit kan zowel bevorderend als remmend zijn. Een voorbeeld van een bevorderende factor is de toenemende handelsstroom van China naar de Europese Unie: hierdoor nemen de mogelijkheden voor het verbergen van smokkelwaar toe. Bij remmende factoren kan bijvoorbeeld worden gedacht aan inspanningen op het vlak van de criminaliteitsbeheersing, zoals de intensivering van controles op de export van goederen.

De criminele verschijnselen die centraal staan in dit rapport, kunnen geordend worden vanuit drie invalshoeken: criminele hoofdactiviteiten, criminele werkwijzen en criminele samenwerkingsverbanden (csv's). Criminele hoofdactiviteiten zijn delicten die op zichzelf verdiensten genereren, zoals drugssmokkel en autodiefstal. Criminele werkwijzen zijn min of meer specifieke werkwijzen of modi operandi, zoals het gebruik van geweld en corruptie. Bij csv's gaat het niet alleen om de samenstelling van criminele groepen, maar bijvoorbeeld ook om de aard van de samenwerking binnen en tussen groepen. De criminele hoofdactiviteiten zijn de primaire invalshoek in dit NDB.

Ten slotte zijn de maatschappelijke gevolgen van een crimineel verschijnsel belangrijk. Hiermee bedoelen wij de gevolgen van een crimineel verschijnsel voor de Nederlandse samenleving, in hun totaliteit.

De (veronderstelde) causale verbanden tussen criminaliteitsrelevante factoren, criminele verschijnselen en maatschappelijke gevolgen zijn schematisch weergegeven in figuur 1.

7 Vanwege onvoorzien oponthoud bij de opstart van het project is de start een half jaar vertraagd. De oplevering valt daarmee in 2017, vandaar de titel NDB2017 in plaats van NDB2016.

Figuur 1. De (veronderstelde) causale verbanden tussen criminaliteitsrelevante factoren, criminele verschijnselen en maatschappelijke gevolgen

1.3 Doelstelling

De opdracht is in het NDB2017 een analyse te geven van de huidige en toekomstige Nederlandse situatie voor wat betreft de georganiseerde criminaliteit en van de belangrijkste kwetsbaarheden die de Nederlandse samenleving in dit opzicht vertoont. Het doel van deze analyse is tweeledig: (a) onderbouwing leveren ten behoeve van prioriteren en (b) signaleren. Ze moet onderbouwing opleveren voor het vaststellen van beleidsprioriteiten in de nationale aanpak van georganiseerde criminaliteit door politie, justitie en relevante partners. Met andere woorden, ze moet handvatten bieden voor het selecteren van criminele verschijnselen als speerpunt van beleid. Daarnaast moet ze leiden tot informatie over (andere) kwesties die in dit verband de komende jaren van belang kunnen zijn en waarvoor nadere informatieverzameling gewenst is; het NDB moet nieuwe ontwikkelingen signaleren en de vinger leggen op criminele verschijnselen waarvan de informatiepositie onvoldoende is ('witte vlekken').

1.4 Afbakening

Besturingsniveau

Het Nationaal dreigingsbeeld is primair bedoeld voor het strategische besturingsniveau. Mede aan de hand van dit rapport worden de nationale speerpunten van beleid bepaald. Deze nationale speerpunten gelden voor de, volgens de IGP-indeling, organisatorische niveaus 2, regionaal en bovenregionaal en 3, (inter)nationaal.[8]

Onderzoeksdomein

Het onderzoeksdomein wordt aangeduid als 'georganiseerde criminaliteit'. Dit domein betreft hier delicten die (1) tot stand komen in de structurele samenwerking tussen personen, (2) worden gepleegd met het oog op het gezamenlijk behalen van financieel of materieel gewin en (3) een strafdreiging hebben van vier jaar of meer[9]. Het kenmerk 'structurele samenwerking tussen personen' betekent dat er sprake is van (de intentie tot) herhaald

8 In de IGP-indeling behoren het nationale niveau en het internationale niveau beide tot niveau 3. In het geval van het Nationaal dreigingsbeeld wordt beoogd een bijdrage te leveren aan het bepalen van speerpunten van beleid op nationaal niveau en niet op internationaal niveau. *IGP* staat voor 'Informatiegestuurde politie'.

9 Conform de nota *De strafrechtelijke aanpak van georganiseerde misdaad in Nederland 2005 - 2010* (Openbaar Ministerie, 2004), waarin voetnoot 2 op pagina 38 verwijst naar de United Nations Convention Against Transnational Organized Crime met de stellingname dat als 'ernstig delict' wordt beschouwd het misdrijf dat met ten minste vier jaar vrijheidsstraf wordt bedreigd (United Nations, 2000: art. 2b).

plegen van een delict of misdrijf, en bovendien van enige consistentie in de samenstelling van het samenwerkingsverband.

Om een zo breed mogelijk overzicht te geven van relevante criminaliteitsvormen hebben wij het onderzoeksdomein voor het NDB ruimer afgebakend dan gangbaar is in omschrijvingen van georganiseerde criminaliteit. Het omvat namelijk niet alleen de traditionele vormen van georganiseerde criminaliteit, maar ook vormen die worden aangeduid als 'zware criminaliteit', 'middencriminaliteit' en 'organisatiecriminaliteit'. Dreigingen die zich manifesteren op de terreinen van de vermogenscriminaliteit, horizontale fraude, verticale fraude en milieucriminaliteit zijn daarmee ook relevant voor dit NDB, voor zover het hierbij gaat om structurele samenwerking tussen personen die gericht is op gezamenlijk financieel of materieel gewin waarvoor een strafdreiging geldt van vier jaar of meer.
Omdat het NDB bedoeld is voor het stellen van landelijke beleidsprioriteiten die gelden voor de organisatorische niveaus 2 en 3, besteden we geen aandacht aan lokale criminaliteitsproblematiek. Evenmin behoort ideologisch gemotiveerde criminaliteit tot het domein van het NDB, vooral omdat andere, gespecialiseerde instanties zich met dit onderwerp bezighouden.

Doorontwikkeling
De werkgroep die het NDB2017 heeft voorbereid, heeft na evaluatie van het vorige dreigingsbeeld besloten dat het NDB2017 zich zou moeten toespitsen op beleidsrelevante ontwikkelingen in de georganiseerde criminaliteit, en wel op ontwikkelingen die zich hebben voorgedaan sinds het verschijnen van het NDB2012. Dit betekent dat we afzien van een complete beschrijving van aard en omvang van criminele verschijnselen, voor zover beschrijvingen van min of meer vastomlijnde algemene aspecten van organisatie en uitvoering van deze verschijnselen zouden leiden tot dubbelingen met beschrijvingen uit eerdere dreigingsbeelden. Ook is besloten om in het NDB, nog meer dan voorheen, beargumenteerd toekomstige ontwikkelingen in de georganiseerde criminaliteit te schetsen. Ten slotte is het besluit genomen meer systematisch aandacht te besteden aan de schade die aan de Nederlandse samenleving wordt toegebracht.

Internationale dimensie
Voor het bepalen van beleidsprioriteiten in Nederland zijn ook internationale trends en ontwikkelingen van belang. Het onderzoek beperkt zich daarom niet tot de nationale context. Bij het formuleren van de verwachtingen over criminele verschijnselen die zich in Nederland zullen voordoen in de jaren 2017-2021, is mede gekeken naar de ontwikkelingen in het buitenland. Criminele innovaties in de Verenigde Staten bijvoorbeeld zouden ook in ons land hun intrede kunnen doen.
Bij de beschrijving van de gevolgen van criminele verschijnselen staan de gevolgen voor de Nederlandse samenleving centraal. We schenken ook aandacht aan de gevolgen voor andere landen, maar deze beschrijven we hoofdzakelijk naar aard en niet naar omvang; de nadruk ligt daarbij op het expliciteren van de soorten gevolgen.

Integraliteit
Voor zover mogelijk is er samenwerking gezocht met partners in de aanpak van vormen van georganiseerde criminaliteit met ernstige en ondermijnende gevolgen. Daarbij gaat het om bestuurlijke instanties, de Belastingdienst, bijzondere opsporingsdiensten, relevante inspecties, het Landelijk Informatie en Expertise Centrum (LIEC) en de Regionale Informatie en Expertise Centra (RIEC's).
Deze partners zijn betrokken bij de keuze van te onderzoeken thema's, in het bijzonder op de terreinen van milieu en fraude. Ook is voor de uitvoering van onderzoek een beroep gedaan op de bij hen beschikbare informatie, expertise en onderzoekscapaciteit.

Onderzoeksperiode en vooruitblik
Het onderzoek richt zich in eerste instantie op de ontwikkelingen die zich hebben voorgedaan sinds het laatstverschenen dreigingsbeeld, dat wil zeggen in de periode 2012-2016. Op basis daarvan worden verwachtingen geformuleerd met betrekking tot de nabije toekomst, de periode 2017-2021.

1.5 Onderzoeksvragen

De dreigingsbeelden van 2008 en 2012 moesten antwoord geven op respectievelijk zes en acht onderzoeksvragen. Dit resulteerde in tamelijk uitvoerige en gedetailleerde beschrijvingen van de onderzochte criminele verschijnselen: omvang, aard, betrokken individuen en groepen, werkwijzen et cetera. Een van de conclusies van het NDB2012 was dat er betrekkelijk weinig beweging zit in de basisstructuren van de georganiseerde criminaliteit in Nederland.[10] In voorgaande dreigingsbeelden zijn de algemene aspecten van de organisatie en uitvoering van criminele verschijnselen voldoende beschreven. De nadruk ligt daarom nu op veranderingen en ontwikkelingen die zich sinds het laatste NDB hebben voltrokken of zich de komende tijd zullen aandienen, en wel voor zover ze relevant zijn voor de strategische besluitvorming.

Voor de criminele verschijnselen die voor het NDB2017 zijn onderzocht, zijn de volgende algemene onderzoeksvragen geformuleerd:

1. Welke nieuwe ontwikkelingen[11] hebben zich met betrekking tot het criminele verschijnsel voorgedaan?
2. Wat zijn de huidige gevolgen van het criminele verschijnsel voor de Nederlandse samenleving?
3. Welke ontwikkelingen met betrekking tot het criminele verschijnsel zijn te verwachten voor de periode 2017-2021?
4. Wat zijn de te verwachten gevolgen van het criminele verschijnsel in 2021?

10 Een uitzondering werd gemaakt voor de steeds grotere rol die het 'alomtegenwoordige' internet speelt bij de georganiseerde criminaliteit.
11 Ontwikkelingen in aard en omvang die van belang zijn voor de strategische besluitvorming en die nieuw zijn sinds het vorige NDB.

De criminele verschijnselen zijn onderzocht in deelprojecten. Per deelproject zijn de algemene onderzoeksvragen nader uitgewerkt, al naar gelang de specifieke onderwerpen daartoe aanleiding gaven.

1.6 Deelprojecten

De vier onderzoeksvragen die in paragraaf 1.5 zijn aangehaald, werden door deelproject-teams onder de loep genomen. Er waren 21 deelprojecten met de volgende werktitels:

1. Handel in en smokkel van cocaïne
2. Handel in en smokkel van heroïne
3. Productie, handel en smokkel van synthetische drugs
4. Productie, handel en smokkel van cannabis
5. Uitbuiting in de prostitutie
6. Arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening
7. Orgaanhandel
8. Mensensmokkel
9. Illegale handel in en smokkel van vuurwapens en explosieven
10. Kindersekstoerisme en kinderpornografie
11. Productie en distributie van vals geld
12. Afpersing
13. Illegale kansspelen en matchfixing
14. Witwassen
15. Horizontale fraudevormen:
    - Acquisitiefraude
    - Hypotheekfraude
    - Beleggingsfraude
    - Faillissementsfraude
    - Fraude met betaalmiddelen
    - Fraude met online handel
    - Telecomfraude
    - Verzekeringsfraude
    - Voorschotfraude
16. Verticale fraudevormen:
    - Fiscale fraude
    - Accijnsfraude
17. Georganiseerde vermogenscriminaliteit:
    - Woninginbraak
    - Bedrijfsinbraak
    - Winkeldiefstal
    - Kraken op geldautomaten
    - Overvallen
    - Heling

18. Ladingdiefstal
19. Autocriminaliteit
20. Cybercrime
21. Nieuwe criminele verschijnselen

Elk deelprojectteam schreef een eigen plan van aanpak, op basis van dezelfde algemene onderzoeksvragen. Alle plannen van aanpak werden ter fiattering voorgelegd aan de NDB-projectleiding en de begeleidingscommissie. De uitvoering van de deelprojecten viel onder de verantwoordelijkheid van de projectleiding. Alle deelprojectteams stelden voor de projectleiding een rapportage op waarin de onderzoeksvragen werden beantwoord en die kon fungeren als bouwsteen voor het NDB2017. Het onderzoek naar verticale fraude resulteerde in twee deelrapporten.
Voor elk deelproject was een klankbordgroep samengesteld om de voortgang en kwaliteit van het deelproject te bewaken. Aan elke klankbordgroep is om een korte evaluatie van het deelproject gevraagd. Hoewel er ook kritische opmerkingen werden gemaakt, waren deze evaluaties overwegend positief en gaf elke klankbordgroep zijn fiat aan het rapport van zijn deelprojectteam. De begeleidingscommissie stemde op basis van de verslagen van de klankbordgroepen daarmee in.

Aan elk van de criminele verschijnselen die door de deelprojectteams zijn onderzocht, is in deel 2 of 3 van dit NDB een paragraaf of hoofdstuk gewijd. Voor de beschrijving van milieucriminaliteit is gebruikgemaakt van het *Dreigingsbeeld Milieucriminaliteit 2016*, dat in opdracht van de Strategische Milieukamer in de loop van 2016 werd opgesteld. Bij de bespreking van de afzonderlijke criminele verschijnselen wordt vermeld wie deel uitmaakten van het desbetreffende deelprojectteam. Hoe de klankbordgroepen samengesteld waren, is te zien in het *Bronnenboek NDB2017*[12].

1.7 Kwalificatie

Nadat de deelprojecten waren afgerond, brak de kwalificatiefase aan. De bedoeling van deze fase, die in juni 2016 begon, was om elk crimineel verschijnsel van een zogenoemde kwalificatie van dreiging te voorzien. De rapporten van de deelprojectteams vormden het basismateriaal voor de kwalificatie. Er werd een consensusgroep samengesteld die tot taak had om aan de hand van argumenten, ontleend aan de verschillende rapportages, te komen tot een eensluidend oordeel over de vraag in hoeverre de diverse criminele verschijnselen een dreiging vormen voor de Nederlandse samenleving. De groep bestond uit vijf beoordelaars en een voorzitter: drie medewerkers van de Dienst Landelijke Informatieorganisatie van de politie, een medewerker van de Politieacademie, een van de Dienst Landelijke Operationele Samenwerking en een van organisatieadviesbureau Twynstra Gudde.[13]

12 Meer over dit *Bronnenboek NDB2017* in paragraaf 1.10.

13 De precieze samenstelling van de consensusgroep is te vinden in bijlage 2.

Bij de samenstelling van de groep zijn onafhankelijkheid en bekendheid met de materie als eisen gesteld. Met name de eerste eis had tot doel te voorkomen dat bij de toekenning van de kwalificatie bepaalde (beleids)belangen een rol zouden spelen; ook de schijn van belangenverstrengeling moest op deze manier vermeden worden. Het belang van de tweede eis is evident: bekendheid met de materie is noodzakelijk om de onderliggende rapporten te kunnen beoordelen. Een en ander had als resultaat dat de leden allen een academische achtergrond hadden en in de onderzoekspraktijk werkzaam waren.

Het primaire doel van het kwalificeren van criminele verschijnselen is om te bepalen of er sprake is van een dreiging voor de Nederlandse samenleving in de komende vier jaar. De methode van kwalificeren die voor het NDB2017 is gevolgd, komt voor een groot deel overeen met de methode die is gehanteerd voor het NDB2012.

Als dreiging worden beschouwd criminele activiteiten ten aanzien waarvan gegronde aanwijzingen bestaan
- dat ze zich
  (a) de komende jaren zullen voordoen of zullen blijven voordoen
  (b) in de vorm van of in het kader van een meer dan eenmalige samenwerking van
  (c) twee of meer personen
  (d) die met elkaar financieel of materieel gewin willen behalen
- én dat ze in hun totaliteit ernstige gevolgen zullen hebben voor de Nederlandse samenleving.

Elk lid van de consensusgroep is voor elk crimineel verschijnsel nagegaan of op basis van de rapporten gesproken kan worden van gegronde aanwijzingen voor de vijf bovengenoemde aspecten.
Om te kunnen spreken van gegronde aanwijzingen moet een onderbouwing worden gegeven op basis van argumenten. Er hoeft niet per se empirisch bewijs voorhanden te zijn, de beoordeling moet aannemelijk kunnen worden gemaakt. De onderbouwing van hoe een aspect zich in de komende jaren zal ontwikkelen, kan bijvoorbeeld worden ontleend aan extrapolatie van bestaande gegevens, aan een redenering op basis van criminaliteitsrelevante factoren, aan een analogieredenering of generalisatie, of aan een combinatie hiervan. *Extrapolatie van bestaande gegevens over criminaliteit of criminele groeperingen.* Extrapolatie is bijvoorbeeld mogelijk op basis van het 'doortrekken' van cijfermatige trends. *Redenering op basis van criminaliteitsrelevante factoren*. Factoren (veelal SEPTED[14]) die, beargumenteerd, een rol spelen bij de totstandkoming, het blijven bestaan of het afnemen van een criminaliteitsprobleem, kunnen worden gebruikt voor het beschrijven van de verwachtingen ten aanzien van de ontwikkelingen van dat probleem in de toekomst.

14 SEPTED is een acroniem voor de zes dimensies waarlangs factoren gerangschikt kunnen worden: Sociaal-cultureel, Economisch, Politiek, Technologisch, Ecologisch en Demografisch.

Analogieredenering of generalisatie. Als, bijvoorbeeld, een crimineel verschijnsel zich nu niet in Nederland voordoet maar wel in de Verenigde Staten, kan er mogelijk een redenering worden opgebouwd die aannemelijk maakt dat ook Nederland in de komende jaren met het verschijnsel zal worden geconfronteerd. Of als een crimineel verschijnsel zich bijvoorbeeld al manifesteert in het zuiden van ons land, kan wellicht worden beargumenteerd dat het zich zal gaan voordoen in meerdere delen van Nederland of in het hele land.

Per crimineel verschijnsel werd door de leden van de consensusgroep – onafhankelijk van elkaar en voorafgaand aan de consensussessies – aan de vijf kenmerken een code toegekend. Als er gegronde aanwijzingen waren voor een bevestiging van een van de genoemde kenmerken, werd de code 'ja' toegekend. Waren er gegronde aanwijzingen voor een ontkenning, dan werd de code 'nee' toegekend. Ontbraken gegronde aanwijzingen, dan was de code '-' en als er tegenstrijdige aanwijzingen bestonden, werd de code '?' gegeven.
Vervolgens werd elk crimineel verschijnsel gekwalificeerd. Daarvoor waren vier kwalificaties beschikbaar: 'dreiging', 'geen concrete dreiging', 'witte vlek' en 'voorwaardelijke dreiging'. Voor de kwalificatie *dreiging* moeten alle vijf kenmerken de code 'ja' gekregen hebben. Voor de kwalificatie *geen concrete dreiging* volstaat één enkel 'nee'. In de resterende gevallen luidt de kwalificatie 'voorwaardelijke dreiging' of 'witte vlek'.
De kwalificatie *witte vlek* is van toepassing op criminele verschijnselen waarvan te weinig bekend is om tot een onderbouwd oordeel te kunnen komen. Dat kan het geval zijn doordat er in het NDB-traject geen onderzoek naar is verricht. Dergelijke verschijnselen kunnen bij het inventariseren van de criminele verschijnselen als 'bijvangst' naar voren komen, in de marge van een onderzoek waarin andere criminele verschijnselen centraal staan. Ook is het mogelijk dat er van een crimineel verschijnsel in het NDB-traject te weinig bekend is geworden over de te verwachten ontwikkeling in de komende jaren en/of over de ernst van de maatschappelijke gevolgen. Verder kan een verschijnsel het stempel 'witte vlek' krijgen wanneer de informatie zo tegenstrijdig is dat een verantwoorde kwalificatie niet goed mogelijk is.
Als *voorwaardelijke dreiging*, ten slotte, worden criminele activiteiten bestempeld die naar verwachting in de komende vier jaar alleen dan een dreiging zullen worden of blijven als aan specifieke geëxpliciteerde voorwaarden is voldaan.

Nadat ieder van de vijf beoordelaars voor elk van de criminele verschijnselen van de totaallijst (zie daarvoor hoofdstuk 2) de methode van kwalificeren had toegepast, werden de kwalificaties van criminele verschijnselen voor het NDB2017 vastgesteld in consensussessies. Het komen tot een gezamenlijk eindoordeel voor alle criminele verschijnselen in deze sessies heeft twee dagen in beslag genomen. De bijeenkomsten, die begin juni 2016 plaatsvonden, werden geleid door een onafhankelijke voorzitter. Onder zijn leiding is gediscussieerd over de aanwezigheid of het ontbreken van gegronde aanwijzingen voor dreiging. Dit leidde tot een intersubjectief oordeel over de ernst van de gevolgen van elk crimineel verschijnsel.

Soms bleek het lastig te beoordelen of er sprake was van gegronde aanwijzingen. Bij het benoemen van verwachtingen gaat het altijd om veronderstellingen en aannames. Dat betekent dat er altijd enige mate van onzekerheid is. Ondanks het subjectieve karakter van de methode van kwalificeren is de consensusgroep er telkens in geslaagd, op basis van beredeneerde argumentatie, tot een gezamenlijk oordeel te komen over de mate van dreiging van het criminele verschijnsel voor de Nederlandse samenleving in de komende vier jaar.

1.8 Aanvullende toelichting op de begripsafbakening van 'dreiging'

In de vorige paragraaf zijn vijf kenmerken genoemd waaraan een criminele activiteit moet voldoen, willen we deze als dreiging beschouwen. Hieronder geven we een aanvullende toelichting op de gegeven begripsafbakening.

- Verschijnselen die geen verwijzing naar (een) criminele activiteit(en) bevatten, komen niet in aanmerking voor de kwalificatie 'dreiging'. Een dreiging kan bijvoorbeeld niet uitsluitend de verwijzing naar een bepaald crimineel samenwerkingsverband zijn, naar een bepaalde categorie csv's of naar (een) criminaliteitsrelevante factor(en).
- Met de zinsnede 'de komende jaren' wordt gedoeld op de periode tot aan het verschijnen van het volgende NDB in 2021.
- Met de formuleringen 'meer dan eenmalige samenwerking' en 'van twee of meer personen' willen we aangeven dat het gaat om (de intentie tot) herhaald plegen én om enige consistentie in de samenstelling van een samenwerkingsverband.
- Een gevolg is pas relevant als het voorkomt in een substantieel deel van de gevallen waarin de betreffende criminele activiteit zich voordoet of als het ontstaat door de cumulatie van afzonderlijke gevallen van criminele activiteit. In de begripsafbakening wordt daarom gesproken over de gevolgen van criminele activiteiten 'in hun totaliteit'.
- De verwachte of geconstateerde gevolgen van criminele verschijnselen zijn een centraal concept binnen het NDB. Criminele verschijnselen hebben niet alleen negatieve gevolgen maar soms ook positieve, bijvoorbeeld als criminele verdiensten worden gebruikt om panden op te knappen. Daarom spreken we over gevolgen in plaats van over schade.
- Sinds het NDB2008 zijn enkele nieuwe inzichten toegepast wat de gevolgen van georganiseerde criminaliteit betreft. Vooral het rapport *Bad thoughts* van Dorn en Van de Bunt[15] over de bepaling van de (kosten van de) gevolgen is van invloed geweest. Op basis daarvan is vooral de wijze waarop in het NDB de indirecte gevolgen en de slachtoffercategorieën benaderd worden, aangepast.[16] Bij het bepalen van de verwachte gevolgen wordt een deel van de indirecte kosten buiten beschouwing gelaten, namelijk de responskosten. Dat zijn de kosten die ontstaan voor de overheid, bedrijven of burgers als zij, in reactie op criminaliteit, activiteiten ondernemen of juist nalaten om slachtofferschap te voorkomen. Het gaat bijvoorbeeld om preventieve maatregelen zoals *firewalls*, hang-en-

15 N. Dorn & H. van de Bunt (2010). *Bad thoughts. Towards an organised crime harm assessment and prioritisation system (OCHAPS).* Rotterdam: Erasmus University.

16 Anders dan Dorn en Van de Bunt kiezen wij ervoor de effectiviteit van beleidsmaatregelen buiten beschouwing te laten.

sluitwerk, inrichting van de openbare ruimte, detectiepoortjes en verzekeringspremies, om uitgaven voor opsporing en vervolging, en om kosten die samenhangen met de ten-uitvoerlegging van sancties. Responskosten blijven buiten beschouwing vanwege het gevaar van de cirkelredenering: door preventieve en repressieve maatregelen stijgen de kosten van het delict en daarmee gaat de prioriteit omhoog, waardoor er nog meer preventieve en repressieve maatregelen worden getroffen, de kosten verder toenemen evenals de prioriteit, enzovoort. Andere indirecte kosten dan responskosten worden gespecificeerd en meegenomen in de afwegingen. Zo kunnen de faillissementen van bedrijven die uit de markt zijn gedrukt door concurrerende bedrijven gerund door criminelen die onder de marktprijs werken tot de indirecte kosten worden gerekend.

- Ook gevolgen voor 'het imago' laten we niet meewegen. Een imago is geen constante eigenschap van het object, maar bestaat in de perceptie van de waarnemer. Daardoor kunnen er meerdere imago's van één object naast elkaar bestaan. Het gevoerde cannabisbeleid leidt bijvoorbeeld bij sommige personen tot een positief imago van Nederland, terwijl het anderen een doorn in het oog is. Evenmin valt goed te bepalen welk deel van een imago door de manifestatie van criminele verschijnselen wordt veroorzaakt. Alles bij elkaar zijn dit genoeg redenen om imagoschade niet mee te laten wegen. Mochten er echter specifieke kosten ontstaan in het verlengde van imagoschade, dan tellen we die specifieke kosten weer wel mee. Te denken valt aan een faillissement dat rechtstreeks het gevolg is van een beschadigd imago.
- Voor de bepaling van de ernst van de gevolgen heeft bij financiële schade de draagkracht van het slachtoffer geen rol gespeeld. Met andere woorden, de financiële schade van verzekeringsfraude voor verzekeringsmaatschappijen of die van winkeldiefstallen voor grote winkelketens heeft even zwaar gewogen als de schade van een overval op een sigarenwinkel of de diefstal van een auto. De voornaamste reden daarvoor is dat de schade van financiële instellingen en winkelketens verdisconteerd wordt in premies en consumentenprijzen, waardoor niet de instellingen en ketens de schade dragen maar de premiebetaler en consument. Dit neemt niet weg dat de gevolgen wel ernstiger kunnen zijn als er vanwege de financiële schade andere negatieve gevolgen zijn ontstaan. Dit is bijvoorbeeld het geval als een individu door de financiële schade huis en haard verliest en in psychische problemen geraakt.
- De bespreking van de gevolgen kunnen we verder structureren door, in navolging van Dorn en Van de Bunt, slachtoffercategorieën te definiëren en soorten gevolgen te onderscheiden:
  - *personen/individuen*: aantasting van lichamelijke of geestelijke gezondheid (fysiek letsel, psychosociale schade), vermogensschade door verlies van geld of goed (financiële schade) en overlast;
  - *bedrijven*: overlast en financiële schade;
  - *de overheid:* financiële schade;
  - *het maatschappelijke systeem:* ondermijning van rechtspleging en rechtsorde, van politiek en openbaar bestuur, van economische verhoudingen, van infrastructurele voorzieningen en verweving van de boven- met de onderwereld;
  - *de leefomgeving:* aantasting of bedreiging van milieu of leefomgeving.

Dit resulteert in soorten gevolgen zoals weergegeven in figuur 2.

Figuur 2. Gevolgen naar soort

Slachtoffer / soort gevolg	A. Gezondheid		B. Milieu	C. Overlast	D. Financieel	E. Ondermijning					
	A1. fysiek	A2. psychisch				E1. Rechtspleging en rechtsorde	E2. Politiek/ openbaar bestuur	E3. Economie	E4. Infrastructuur	E5. Verweving	E6. Normbesef
1 Individu			nvt			nvt	nvt	nvt	nvt	nvt	nvt
2 Bedrijfsleven	nvt	nvt	nvt			nvt	nvt	nvt	nvt	nvt	nvt
3 Overheid	nvt	nvt	nvt	nvt		nvt	nvt	nvt	nvt	nvt	nvt
4 Systeem	nvt	nvt	nvt	nvt	nvt						
5 Leefomgeving	nvt	nvt		nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt

Binnen alle deelprojecten is het schema tweemaal ingevuld aan de hand van een lijst met vragen en antwoordmogelijkheden (zie bijlage 3): eenmaal om de huidige gevolgen van het criminele verschijnsel te beoordelen en – ten behoeve van toekomstgerichte analyse – eenmaal om de te verwachten gevolgen in 2021 in te schatten. Deze gevolgen zijn van doorslaggevende betekenis geweest bij het toekennen van de kwalificatie. Om de ernst van de gevolgen vast te stellen is aan elk deelprojectteam gevraagd zijn oordeel daarover te beargumenteren. Het schatten van de ernst van de gevolgen is voornamelijk een subjectieve aangelegenheid. De consensusgroep heeft geprobeerd daaraan enige objectiviteit te verlenen door tot een intersubjectief oordeel te komen, namelijk door consensus te bereiken op grond van beschikbare argumenten. Op de subjectiviteit van de ernstscore bestaat één uitzondering, te weten de financiële schade. Binnen de consensusgroep is de (arbitraire) afspraak gemaakt dat een jaarlijkse totale schade van 100 miljoen euro de overgang markeert van minder ernstig naar ernstig. Het komt overigens zelden voor dat de schade uitsluitend financieel is; over het algemeen is het een combinatie van gevolgen die tot de kwalificatie van dreiging leidt. Daardoor kan het voorkomen dat een crimineel verschijnsel tot dreiging wordt bestempeld bij een financiële schade van minder dan 100 miljoen euro.

1.9 Nieuw ten opzichte van het NDB2012

Om continuïteit te waarborgen is de lijst van criminele hoofdactiviteiten uit het vorige dreigingsbeeld uitgangspunt geweest voor het huidige dreigingsbeeld. Voorafgaand is een verkennend project uitgevoerd naar nieuwe criminele verschijnselen om vast te stellen of de bestaande lijst moest worden aangevuld. Dit verkennende project bracht enkele nieuwe criminaliteitsrelevante ontwikkelingen onder de aandacht, zoals de trend *Do-it-Yourself.* Nieuwe criminele hoofdactiviteiten kwamen in dit project niet aan het licht, zodat de bestaande lijst kon worden gehandhaafd. Niettemin zijn er enkele veranderingen aange-

bracht in vergelijking met 2012. Er zijn zes criminele verschijnselen onderzocht die in 2012 niet aan de orde zijn geweest. Dat zijn matchfixing, illegale kansspelen, orgaanhandel, heling, fiscale fraude en accijnsfraude. Om uiteenlopende redenen zijn ook enkele verschijnselen van de lijst afgevoerd: skimming, kunst en antiek, bedrijfsspionage, vervalste medicijnen en merkfraude. Ten slotte zijn diverse categorieën samengevoegd. De twee categorieën kinderpornografie zijn teruggebracht naar één categorie. De drie afzonderlijke kwalificaties voor varianten van cannabis zijn ondergebracht in één algemene kwalificatie.

In vergelijking met het gros van de criminele verschijnselen die in dit NDB worden beschreven, is gekozen voor een afwijkende behandeling van milieucriminaliteit en cybercrime. Dit is vooral gedaan omdat er een dermate grote variëteit aan verschijningsvormen van milieucriminaliteit en cybercrime bestaat dat de 'NDB-methode' voor deze terreinen minder geschikt is. Met betrekking tot veel van die vormen is weliswaar casuïstiek beschikbaar, maar ontbreekt betrouwbare kwantitatieve informatie. Daardoor zijn de mogelijkheden om de omvang te bepalen beperkt. Dit zou hoogstwaarschijnlijk resulteren in de kwalificatie 'witte vlek', en dat zou geen recht doen aan de (soms ernstige en verstrekkende) gevolgen van deze vormen van criminaliteit. Daarom hebben milieucriminaliteit en cybercrime geen kwalificatie van dreiging gekregen. We hebben ervoor gekozen deze beide onderwerpen elk in een apart hoofdstuk te behandelen. Daarin wordt duidelijk welke bedreigingen er uitgaan van milieucriminaliteit en cybercrime. Voor een nadere uitleg wordt verwezen naar de betreffende hoofdstukken in deel 3 van dit rapport.

1.10 Ten slotte

De behandeling van criminele verschijnselen in dit eindrapport is vrijwel geheel gebaseerd op de informatie uit het basismateriaal van dit NDB, de 23 onderzoeksrapporten. De informatie uit die rapporten hebben wij benut voor het opbouwen van een argumentatie om tot een kwalificatie te komen. We hebben die informatie voor een deel vrijwel letterlijk uit de deelrapporten overgenomen en voor een ander deel geïnterpreteerd. In het NDB worden aan criminele verschijnselen kwalificaties toegekend volgens een vaste procedure. Zoals we bij de bespreking van de methode uiteengezet hebben, is de kwalificatie van een crimineel verschijnsel gebaseerd op intersubjectiviteit. Dit betekent dat een andere groep beoordelaars tot een afwijkende kwalificatie zou kunnen komen. Daarom onderstrepen wij het belang van de argumentatie. Aan de argumenten die tot een bepaalde kwalificatie hebben geleid, moet met andere woorden meer waarde worden gehecht dan aan de kwalificatie zelf.

De bronvermelding in dit eindrapport blijft grotendeels beperkt tot een verwijzing naar de deelrapporten die als bouwsteen hebben gediend; de lezer treft in dit dreigingsbeeld geen bronnen- en literatuurlijst aan. De deelprojectteams hebben voor hun rapporten, die samen meer dan tweeduizend pagina's omvatten, een breed spectrum aan bronnen gebruikt: allerhande literatuur, interviews met materiedeskundigen, openbronnenmateriaal van bijvoorbeeld het internet, informatie uit expertmeetings, politiecijfers en cijfermatige gegevens van andere instanties. Het uitputtend vermelden van al dat bronnenmateriaal en de gebruikte

methodieken zou de omvang van dit toch al lijvige eindrapport buiten proporties doen toenemen. Hier volstaan we daarom met verwijzingen naar de onderliggende deelrapporten. Als in dit eindrapport naast het basismateriaal aanvullende bronnen zijn gebruikt, is dat in de tekst aangegeven.
In het afzonderlijke, digitaal toegankelijke *Bronnenboek NDB2017,* samengesteld door Irene Spijker, zijn alle bronnen opgenomen, zowel die van de deelrapporten als die van het eindrapport.

Dit eindrapport is een boek in vier delen. Het zwaartepunt ligt in deel 2. Daarin beschrijven we de criminele verschijnselen en geven we voor elk van die verschijnselen een beargumenteerde kwalificatie van dreiging. De bevindingen ten aanzien van milieucriminaliteit en cybercrime zijn in deel 3 ondergebracht. Deel 4 bevat de signaleringen en een nabeschouwing.

2 De kwalificaties in een oogopslag

Dit hoofdstuk bevat een overzicht van de kwalificaties die aan de onderzochte criminele verschijnselen zijn toegekend. Zoals in het vorige hoofdstuk is uiteengezet, waren er vier kwalificaties beschikbaar. Criminele verschijnselen die zijn gekwalificeerd als 'dreiging', zullen naar verwachting de komende vier jaar relatief ernstige gevolgen voor de Nederlandse samenleving hebben. Criminele verschijnselen waarvoor is vastgesteld dat de verwachte gevolgen naar verhouding minder ernstig zijn, hebben als kwalificatie 'geen concrete dreiging' gekregen. Is onvoldoende informatie bekend om tot een verantwoorde kwalificatie te komen of is er sprake van sterk tegenstrijdige informatie, dan beschouwen we het criminele verschijnsel als 'witte vlek'. De vierde mogelijke kwalificatie, de 'voorwaardelijke dreiging', is deze keer eenmaal toegekend.
In tabel 1 presenteren we een overzicht van de kwalificaties voor de criminele verschijnselen.

Tabel 1. Criminele verschijnselen en hun kwalificatie van dreiging

Illegale markten	
Handel in en smokkel van cocaïne	Dreiging
Handel in en smokkel van heroïne	Dreiging
Productie van, handel in en smokkel van synthetische drugs	Dreiging
Productie van, handel in en smokkel van cannabis	Dreiging
Seksuele uitbuiting	Dreiging
Arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening	Dreiging
Mensensmokkel	Dreiging
Orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering	Geen concrete dreiging
Illegale handel in en smokkel van vuurwapens en explosieven	Dreiging
Productie en verspreiding van kinderpornografie	Dreiging
Productie en verspreiding van vals geld	Geen concrete dreiging
Matchfixing	Geen concrete dreiging
Illegale kansspelen	Geen concrete dreiging
Fraude en witwassen	
Acquisitiefraude	Geen concrete dreiging
Hypotheekfraude	Geen concrete dreiging
Beleggingsfraude	Dreiging
Faillissementsfraude	Dreiging
Fraude met betaalmiddelen	Geen concrete dreiging
Fraude met online handel	Geen concrete dreiging
Telecomfraude	Witte vlek
Verzekeringsfraude	Dreiging
Voorschotfraude	Geen concrete dreiging
Accijnsfraude	Dreiging
Fiscale fraude	Dreiging
Witwassen	Dreiging
Vermogenscriminaliteit	
Woninginbraak	Dreiging
Bedrijfsinbraak	Geen concrete dreiging
Winkeldiefstal	Witte vlek
Kraken op geldautomaten	Geen concrete dreiging
Overvallen	Dreiging
Ladingdiefstal	Geen concrete dreiging
Afpersing	Witte vlek
Georganiseerde autocriminaliteit	Voorwaardelijke dreiging
Heling	Witte vlek

Deel 2

Beschrijving en kwalificatie van de criminele verschijnselen

1 Illegale markten

1.1 Inleiding

De behandeling van criminele verschijnselen in dit hoofdstuk en in de twee andere hoofdstukken van dit deel (fraude en witwassen, georganiseerde vermogenscriminaliteit) kent telkens als sluitstuk de kwalificatie van dreiging. De argumenten voor de kwalificatie ontlenen we aan de subparagrafen die daaraan voorafgaan. Telkens start de bespreking met een uiteenzetting van de ontwikkelingen in aard en omvang sinds het vorige dreigingsbeeld. Daarop volgt een beschrijving van de diverse gevolgen van het criminele verschijnsel. Ten slotte komen de verwachtingen voor de komende vier jaar aan bod voor wat betreft aard, omvang en gevolgen.

In dit hoofdstuk staan de activiteiten op illegale markten van goederen en personen centraal. Op de illegale goederenmarkten vindt handel plaats in drugs (cocaïne, heroïne, synthetische drugs, cannabis), organen, vuurwapens, kinderpornografisch materiaal en vals geld. De illegale markten rond personen betreffen de hulp bij illegale migratie (mensensmokkel), de uitbuiting bij het verrichten van arbeid (binnen de seksindustrie en daarbuiten), het manipuleren van sportwedstrijden en het aanbieden van illegale kansspelen.

1.2 Handel in en smokkel van cocaïne

1.2.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Cocaïne. Politie interne rapportage voor het Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar cocaïne dat in de eerste helft van 2016 is uitgevoerd voor dit dreigingsbeeld. De auteurs van het onderzoeksrapport zijn Fred Nieuwenhuis, Pim Dedert en Thomas Mulder, alle drie werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017*.
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Het onderzoek naar de cocaïnemarkt omvat het hele logistieke proces van de georganiseerde handel in en smokkel van cocaïne waar Nederland en/of Nederlanders bij betrokken zijn.

1.2.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Werkwijze

Cocaïne uit Zuid-Amerika wordt voor het leeuwendeel naar Europa gesmokkeld via commerciële (container)vaart. Dat blijkt uit inbeslagnames van cocaïne in Europa in de periode 2011-2013. Het overige deel wordt gesmokkeld met (kleine) privéboten, op lijnvluchten (in vracht, in koffers, in of op het lichaam) en op privévluchten.

Cocaïne bestemd voor Nederland en Europa komt vooral uit Brazilië, Ecuador, Peru en Venezuela. Als belangrijkste *transithubs* fungeren de Dominicaanse Republiek en Jamaica in de Caribben en Panama in Centraal-Amerika. De criminele relaties tussen Nederland en de Dominicaanse Republiek en Panama zijn de laatste jaren toegenomen. In vergelijking met voorgaande jaren is cocaïnesmokkel via West-Afrika als transithub afgenomen. West-Afrika speelt in vergelijking met traditionele transportroutes een marginale rol.

Als toegangspoort tot Europa gebruiken cocaïnehandelaars vooral logistieke knooppunten in Spanje, Portugal, Nederland en België. Cocaïne bestemd voor Nederlandse criminelen komt hoofdzakelijk binnen via de Antwerpse en de Rotterdamse haven, via Schiphol en via kleinere havens, zoals Vlissingen en Amsterdam.

Van alle Europese havensteden is Rotterdam verreweg de grootste met een containeroverslag van in totaal meer dan 12 miljoen containers (in 2014). Antwerpen is de derde grootste haven van Europa met bijna 9 miljoen containers. Vanwege de grote goederenstromen is het aannemelijk dat een groot deel van de naar Nederland gesmokkelde cocaïne via deze havens Nederland binnenkomt. Tegelijkertijd moeten we daarbij wel bedenken dat Nederland in Europees verband 'slechts' 10 tot 15 procent van de totale import en export van de EMU-landen (de negentien EU-lidstaten die de eurozone vormen) voor zijn rekening neemt. Het Nederlandse aandeel op het totaal van de import- en exportstromen binnen de Europese Unie is dus relatief beperkt. Mogelijk geldt dat ook voor het Nederlandse aandeel in de import van illegale goederen (lees hier: cocaïne) binnen de Europese Unie.

In de Nederlandse opsporingsonderzoeken komen de havens van Rotterdam en Antwerpen het meest naar voren als invoerhavens voor cocaïne. Op dit moment lijkt Antwerpen de preferente invoerhaven als we afgaan op inbeslagnamecijfers. In 2015 werd in Antwerpen ruim 15 ton cocaïne onderschept (meer dan in 2013 en 2014 bij elkaar); in Rotterdam was het iets minder dan 5 ton. Belgische justitie en politie vermoeden dat 70 tot 80 procent van de naar Antwerpen gesmokkelde cocaïne Nederland als bestemming heeft.

We zien een diversifiëring van smokkelmethoden. Verschillende criminele organisaties gebruiken een scala aan smokkelmethoden. Er wordt wisselend gebruikgemaakt van dekladingen, zogeheten *rip-offs*, dubbele bodems in containers, verstopplaatsen onder de waterlijn van schepen, groepage van containers, droppings op zee, luchtsmokkel en smokkel via zeiljachten. Indien de daarvoor benodigde expertise niet voorhanden is, wordt gebruikgemaakt van gespecialiseerde facilitatoren.
Cocaïne wordt, net als in het vorige dreigingsbeeld al werd opgemerkt, veelvuldig gesmokkeld onder dekladingen. Het gaat om etenswaren (vooral fruit) en partijen hout. Ook motoren of andere metalen voorwerpen worden wel als deklading gebruikt. Recent is ook cacao als deklading aangetroffen.

Bij een rip-off lift de cocaïne in tassen mee met containers of reguliere containerlading en wordt ze met hulp van binnenuit door 'uithalers' op haventerreinen opgehaald. Deze methode werd de laatste jaren veel gesignaleerd, maar daarin treedt een kentering op. Rip-off wordt de laatste tijd minder vaak gesignaleerd. Het is onduidelijk wat hiervan de oorzaak is. Mogelijk is rip-off minder in zwang als gevolg van robotisering op haventerreinen. Uithalers hebben daardoor minder kans de buit te bemachtigen. Ook kan het zijn dat rip-offs door corruptie binnen haventerreinen minder vaak worden opgemerkt of niet meer nodig zijn. Een andere mogelijkheid is dat rip-offs zijn verplaatst naar havens met minder toezicht. Ook kunnen nieuwe of andere smokkelmethoden aantrekkelijker zijn geworden.

Een fenomeen dat recent wordt gezien, is de smokkel van cocaïne in dubbele bodems, wanden of daken van zeecontainers. De cocaïne wordt in Zuid-Amerika ingebouwd en bij aankomst wordt de container na het lossen van de lading in een *empty depot* in de haven 'gerepareerd' of 'schoongemaakt' zodat de cocaïne eruit kan worden gehaald. Hierbij is hulp van binnenuit altijd noodzakelijk. Voor het uithalen van cocaïne uit zeecontainers die na aankomst in de haven direct naar afnemers in het achterland worden vervoerd, is geen hulp van binnenuit nodig. In dat geval wordt de cocaïne pas op de uiteindelijke plaats van bestemming uit de dubbele wand van de container gehaald.

Een andere populaire manier om cocaïne te verbergen is gebruik te maken van verstopplaatsen onder de waterlijn van schepen. In Rotterdam werd in 2016 in een onderwaterkast (een *inlet* voor koelwater) 55 kilo cocaïne aangetroffen. In Amsterdam is cocaïne aangetroffen in een aantal torpedo's en in een onderdeel van een scheepsroer.

De laatste tijd valt op dat er steeds meer cocaïne wordt aangetroffen in groepagecontainers uit Curaçao. Groepagecontainers vervoeren ladingen met verschillende *Bills of Lading* en/of ladingen van verschillende eigenaren.

Om controle en onderschepping in Nederland te voorkomen, worden pakketten cocaïne geregeld vanaf schepen in open water gedropt. Deze droppings op zee vinden meestal plaats voor de Zeeuwse kust. De gedropte cocaïne wordt overgeheveld op kleinere vaartuigen, zoals snelle motorboten of vissersschepen of wordt vastgemaakt aan een boei voorzien van gps. Op beide manieren is een keer een partij van 1200 kilo cocaïne in Nederland aangekomen. Een daarvan kon worden onderschept. Van de niet-onderschepte partij bleek achteraf dat die door dropping Nederland had bereikt. Droppings verlopen niet altijd volgens plan, zo blijkt uit het aanspoelen van verschillende partijen cocaïne langs de Nederlandse kust.
Via Schiphol worden verschillende smokkelmethoden toegepast. Soms komen grote partijen binnen via luchtvracht. Een voorbeeld hiervan is een partij van 600 kilo cocaïne die medio 2015 in beslag werd genomen. Kleine partijen cocaïne worden verzonden in postpakketten, gaan via passagiers in of op het lichaam of in de bagage, soms in vloeibare vorm.

Een enkele keer is sprake van 'vliegtuigplaatsing', zoals het geval waarbij 6 kilo cocaïne in een vliegtuigvleugel was verstopt. Die smokkelmethode is recent echter niet meer opgemerkt. Bij vliegtuigplaatsingen of vrachtzendingen is hulp van binnenuit vrijwel altijd noodzakelijk.
Naar verluidt worden privévluchten vanaf kleine luchthavens in Europa ingezet voor de smokkel van cocaïne van het Europese vasteland naar het Verenigd Koninkrijk. Ook in Nederland is dit incidenteel gebleken. Nederland heeft meerdere kleine luchthavens of landingsstrips en daar vindt nauwelijks controle plaats.

Verschillende opsporingsonderzoeken tonen aan dat criminelen de smokkel per zeilschip een geschikte smokkelmethode vinden. Er zijn signalen van internationale smokkel via de pleziervaart. De daadwerkelijke omvang is onbekend.

Gebruikelijke afschermingsmethoden die nog steeds veelvuldig worden toegepast, zijn het gebruik van (nep)bedrijven – al dan niet over de grens – en het gebruik van katvangers. De bedrijven worden gebruikt om de handel in cocaïne en witwassen van vermogen te verslui-eren, de katvangers om bedrijven op naam te zetten. Nieuwe afschermingsmethoden zien we terug op het vlak van de technologie. Het gaat bijvoorbeeld om het gebruik van satelliet-telefoons, beter versleutelde telefoons en computers, (peil)bakens die als contra-observa-tiemiddel dienen en stoorzenders die digitale communicatie van opsporingsdiensten verstoren.

Betrokken personen en criminele samenwerkingsverbanden

Nederlandse drugscriminelen zijn als kopers en verkopers van cocaïne actief in Europa (onder andere in Nederland, Spanje, Portugal, België en het Verenigd Koninkrijk) en in Zuid-Amerika (onder andere in Colombia, Brazilië, Panama en de Dominicaanse Republiek). Daarnaast fungeren Nederlandse criminelen als contactpersoon tussen Zuid-Amerikaanse leveranciers en afnemers op het Europese vasteland en in het Verenigd Koninkrijk. Omdat een groot deel van de cocaïne die via Nederland wordt aangevoerd bestemd is voor de Europese markt, worden in Nederland geregeld buitenlandse drugscriminelen gesigna-leerd. Het gaat daarbij onder meer om criminelen uit Oost-Europa en maffialeden uit Italië.

De gevestigde criminele orde die zich van oudsher met cocaïnehandel bezighoudt, ziet de machtsverhoudingen en de manier van werken veranderen. Andere groepen, zoals perso-nen van Turkse, Marokkaanse of Albanese afkomst, dienen zich aan op de cocaïnemarkt. Criminelen van verschillende etniciteit werken met elkaar samen. De huidige criminele samenwerking wordt niet meer bepaald door traditionele hiërarchische verhoudingen, maar door de vraag welke specialisten of personen op sleutelposities nodig zijn om de smokkel succesvol te laten verlopen. Ook is tegenwoordig vaker sprake van multi-ondernemerschap. Drugshandelaars handelen steeds meer op verschillende drugsmarkten, ook als die voor-heen tot het exclusieve domein van een bepaalde etnische groepering behoorden.

Oost-Europeanen spelen een steeds belangrijkere rol in het faciliteren van cocaïnetransporten. In Polen bouwden drie scheepswerven veertig smokkelboten van ruim 265.000 euro per stuk. Zij deden dit in opdracht van een criminele groep met vermoedelijk Nederlandse aansturing. Malafide wervingskantoren werven Oost-Europees personeel dat op vrachtschepen met een vaste lijnverbinding wordt ingezet om cocaïne te smokkelen. Ook komen Oost-Europeanen vaker in beeld als chauffeur en katvanger. In Oost-Europa worden rechtspersonen opgericht die facilitair zijn aan de cocaïnesmokkel. Dit houdt verband met een verschuiving van cocaïnetransporten naar Oost-Europa.

Hoewel verhalen over betrokkenheid van *outlaw motorcycle gangs* bij cocaïnesmokkel de ronde doen, valt dit niet hard te maken. De informatie beperkt zich tot signalen van betrokkenheid bij transport en afpersing van drugscriminelen. Recent kon een *captain* van een chapter in verband worden gebracht met een grote inbeslagname van cocaïne.

In de Rotterdamse haven zijn medewerkers van containerbedrijven, vrachtwagenchauffeurs en douanemedewerkers een onmisbare schakel geworden bij drugssmokkel. Criminelen hebben hun hulp nodig om de drugs van de haventerreinen af te krijgen en zijn bereid daarvoor flink te betalen. De afgelopen jaren heeft dit regelmatig geleid tot verdenkingen van (ambtelijke) corruptie, waarbij ook aanhoudingen plaatsvonden. Vergelijkbare gevallen zien we bij het 'binnenhalen' van cocaïne die via de lucht is gesmokkeld, bijvoorbeeld in vrachtzendingen of door vliegtuigplaatsingen. Voor het binnenhalen van cocaïne uit of van zee worden mensen in de visserij of de maritieme wereld ingehuurd.

Bij rip-offs zijn de uithalers vaak Albanezen die in cafés in Rotterdam geworven worden. Ook Marokkanen worden veel gezien als uithaler.

Subjecten van Zuid-Amerikaanse afkomst worden op of nabij haventerreinen in Nederland gesignaleerd. Zij begeleiden de drugstransporten namens de kartels uit Zuid-Amerika en zien toe op een adequate afwikkeling van de drugsdeal. Dit blijkt uit enkele tientallen opsporingsonderzoeken die sinds 2012 zijn uitgevoerd.

Omvang gebruik

In Europa is cocaïne na cannabis het meestgebruikte stimulerende middel. Er is sprake van een stabiele vraag. De vraag naar cocaïne daalt licht in landen met een hoog gebruik, zoals Denemarken, Italië en Spanje. In het Verenigd Koninkrijk en Rusland daarentegen neemt het gebruik toe. Het aantal cocaïnegebruikers in de Europese Unie wordt geschat op 3,6 miljoen. Zij consumeren ongeveer 91 ton cocaïne met een straatwaarde van 5,7 miljard euro.

Volgens het Trimbos-instituut is er in Nederland sprake van een redelijk stabiele gebruikersmarkt voor cocaïne.

Uit de Gezondheidsenquête/Leefstijlmonitor uit 2014 volgt dat er in Nederland 170.000 recente gebruikers zijn (gebruik in het voorgaande jaar) van wie 66.000 actuele gebruikers (gebruik in de voorgaande maand).[17] Of dat een toename of een daling is ten opzichte van de vorige peiling (in 2009) is niet te zeggen door methodologische verschillen tussen de onderzoeken. De Nederlandse consumptie wordt op basis van dit aantal gebruikers geschat op ruim 3,6 ton per jaar. Dat genereert een jaaromzet van 180 miljoen euro (bij een prijs van 50 euro per versneden gram).
Jaarlijks wordt er in Nederland voor ongeveer 10 ton aan cocaïne in beslag genomen. Het aanzienlijke verschil tussen de jaarlijkse inbeslagnames (circa 10 ton) en de voor de Nederlandse consumptiemarkt benodigde hoeveelheid cocaïne (circa 3,6 ton) maakt duidelijk dat Nederland voor de verspreiding van cocaïne een van de distributiecentra van Europa is. Bijna de helft van alle in beslag genomen cocaïne in 2015 (ruim 4,6 ton) werd door het *Hit and Run Cargoteam* (een recherchesamenwerkingsverband van de Zeehavenpolitie, Douane en de FIOD) in de Rotterdamse haven in beslag genomen. Omdat minder dan 1 procent van alle in Rotterdam binnenkomende containers door de douane (op basis van risicoanalyses) wordt gescand, kunnen we ervan uitgaan dat de in beslag genomen cocaïne een absolute ondergrens markeert. De werkelijke hoeveelheid cocaïne die de Rotterdamse haven binnenkomt, zal hier een veelvoud van zijn.
De onderschepte zendingen nemen in omvang toe. In 2016 zijn er meer grotere zendingen in beslag genomen dan voorheen. In de eerste drie maanden van 2016 waren dat er al vier: in januari in Cadzand 1200 kilo, in maart in Antwerpen twee inbeslagnames van bij elkaar zo'n 8000 kilo en in Rotterdam is in dezelfde maand een zending van 2900 kilo in beslag genomen. Deze vier zendingen zijn bij een consumentenprijs van 50 euro per gram bij elkaar 605 miljoen euro waard.

Op dit moment is het aanbod van cocaïne groot. In Colombia is, vergeleken met 2013, het cocagewas met 44 procent gegroeid en de cocaïneproductie met 50 procent. Een verdere stijging van de productie wordt niet verwacht, omdat een deel van de Colombiaanse productie zich heeft verplaatst naar Peru, Paraguay en Brazilië. Colombia, Peru en Bolivia zijn nog steeds de grootste productielanden van cocaïne.

Het grote aanbod van cocaïne is vermoedelijk de reden dat de groothandelsprijs in Nederland is gedaald van 35.000 naar 25.000 euro per kilo. De consumentenprijs is relatief stabiel. Ondanks inbeslagnames schommelt de prijs van cocaïne in Nederland al sinds 2008 rond de 50 euro per gram, ook nu de zuiverheid de laatste jaren verder lijkt toe te nemen. Deze ontwikkelingen wijzen op voldoende beschikbaarheid van cocaïne in Nederland.

17 M.W. van Laar & M.M.J. van Ooyen-Houben (red.) (2016). *Nationale Drug Monitor. Jaarbericht 2015* (3e herz. dr.). Utrecht: Trimbos-instituut.

1.2.3 Huidige gevolgen

De gevolgen van de cocaïnehandel vloeien voort uit het cocaïnegebruik en de ondermijnende activiteiten van drugscriminelen.

In 2014 klopten in Nederland 7500 drugsgebruikers aan bij de hulpverlening in verband met problematisch cocaïnegebruik. In de laatste jaren daalt die vraag naar hulp. Het aandeel jongeren daalt ook, van 16 procent in 2005 tot 9 procent in 2014. Of deze ontwikkelingen betekenen dat het probleemgebruik van cocaïne afneemt, is onbekend. Naar het totale aantal probleemgebruikers van cocaïne in Nederland is recent geen onderzoek gedaan. Afgezien van de problematische cocaïnegebruikers is het grootste deel van de 66.000 actuele gebruikers in Nederland een recreatief gebruiker. Zij ondervinden, in tegenstelling tot de probleemgebruikers, nauwelijks fysieke en psychische schade door het gebruik van de drugs.

Gebruikers van cocaïne staan bloot aan gezondheidsrisico's die met het gebruik gepaard gaan. Hoewel de zuiverheid van cocaïne in Nederland de afgelopen jaren is toegenomen (van 49 procent in 2009 naar 64 procent in 2015, afgaand op aangeboden monsters) wordt in toenemende mate levamisol, een ontwormingsmiddel voor dieren, als versnijdingsmiddel in cocaïne aangetroffen. In 2015 werd het in 70 procent van de aangeboden cocaïnemonsters aangetroffen. Veelvuldig gebruik van cocaïne die met dat middel is versneden, kan leiden tot ernstige bloedziekten en afwijkingen aan de bloedvaten.

In de periode 2005-2012 schommelde het aantal sterfgevallen rond de 22 per jaar. In 2013 en 2014 ging het om 24 sterfgevallen per jaar.

De gevolgen die samenhangen met de ondermijnende activiteiten van criminelen hebben vooral betrekking op toenemend gebruik van geweld en liquidaties. De handel in cocaïne gaat gepaard met *ripdeals,* gijzelingen, vuurwapengeweld en moord. Soms vinden schietpartijen of liquidaties plaats in woonwijken, op klaarlichte dag. Dat soort geweld heeft een grote impact op de omgeving.
De afgelopen jaren is meer zicht verkregen op *hitteams* die in opdracht van criminelen liquidaties uitvoeren in het drugsmilieu. In de periode 2013-2015 zijn 98 liquidaties of pogingen daartoe geregistreerd. Daarbij vielen 39 doden onder wie twee onschuldige personen die slachtoffer werden van een 'vergismoord'. 36 van de 98 geregistreerde liquidaties of pogingen daartoe hielden verband met cocaïnehandel.

Geweld wordt ook gebruikt tegen medewerkers in de transport- en logistieke sector als ze (onbedoeld) betrokken zijn bij het vervoer of het uithalen van cocaïne. Het uithalen van partijen cocaïne vanaf haventerreinen gaat steeds vaker met geweld gepaard.
Geweld en intimidatie is zichtbaar in stadswijken die fungeren als thuisbasis voor drugsdealers en drugsrunners. Openlijk patsergedrag door 'succesvolle' drugsdealers leidt in dat soort wijken tot onveiligheidsgevoelens onder burgers.

Ook kan er normvervaging optreden, als aanhoudende criminele uitwassen leiden tot een gedoogklimaat of een wegkijkcultuur. Verder kunnen 'kleine' criminelen worden geïnspireerd door 'succesvolle grote' criminelen die openlijk pronken met hun criminele roem.

Cocaïnehandel leidt ook tot verweving van onder- en bovenwereld. In de cocaïnehandel worden rechtspersonen misbruikt, omdat crimineel verkregen vermogen moet worden witgewassen. Daartoe richten criminelen dekmantelfirma's op of maken misbruik van bestaande bedrijven. Veelvuldig misbruik van rechtspersonen verstoort de concurrentieverhoudingen. In welke mate daarvan sprake is, is onbekend.

De financiële schade van de cocaïnehandel valt uiteen in verschillende kostenposten. Het gaat vooral om kosten voor de verslavingszorg voor de naar schatting 7500 problematische cocaïnegebruikers, kosten voor ziekenhuisopnamen en kosten voor overheidsinstanties en bedrijven als gevolg van ziekteverzuim. Hoewel recente cijfers voor Nederland niet beschikbaar zijn, bedragen de kosten voor de verslavingszorg, zeer voorzichtig geschat, ten minste 15 miljoen euro per jaar. Al met al worden de totale kosten die uit de cocaïnehandel voortvloeien geraamd op enkele tientallen miljoenen euro's per jaar.

1.2.4 Verwachtingen

Als de trend van de afgelopen jaren doorzet, blijft het gebruik van cocaïne op de Europese drugsmarkt redelijk stabiel met een neiging tot lichte afname. Dat komt door toenemende vergrijzing waardoor de gebruikerspopulatie slinkt en doordat gebruikers overstappen op nieuwe psychoactieve stoffen die gemakkelijk verkrijgbaar zijn en het effect van cocaïne nabootsen. De verwachting is dat ook in Nederland het gebruik van cocaïne de komende jaren stabiel blijft. Experts verwachten weinig veranderingen ten opzichte van de afgelopen jaren.
Het effect van het vredesakkoord tussen de Colombiaanse regering en de guerrillabeweging FARC op de cocaïneproductie in Colombia is onduidelijk. Toch wordt niet verwacht dat de wereldwijde productie van cocaïne de komende jaren sterk zal afnemen. Een deel van de productie is al verplaatst naar Peru, Paraguay en Brazilië. De uitbreiding van het Panamakanaal leidt tot een grote toename in het internationale ladingvervoer en dat creëert nieuwe mogelijkheden voor cocaïnesmokkel.

Verwacht wordt dat de afhandeling van cocaïne die via de Rotterdamse haven naar Nederland komt zich naar het achterland verplaatst. Dat heeft te maken met de robotisering van de logistieke processen in de Rotterdamse haven, onder andere op Maasvlakte 2. Het volledig automatisch overladen van containers op schepen leidt ertoe dat criminelen hun cocaïne pas later in de logistieke keten kunnen onderscheppen, bijvoorbeeld bij *inlandterminals* in het achterland. Ook de verbeterde beveiliging van de Rotterdamse haven maakt dat criminelen hun smokkelwaar pas later in de logistieke keten kunnen uithalen of oppikken.

Met de oplevering van de nieuwe zeesluis bij IJmuiden in 2019 zal naar verwachting het containervervoer gaan groeien en kan ook de smokkel van cocaïne via Amsterdam gaan toenemen. Een soortgelijke toename van goederenverkeer in de haven van Vlissingen (door de verplaatsing van de bananenterminal van Rotterdam naar Vlissingen) leidde recent tot meer cocaïnesmokkel via de Vlissingse haven. Of de haven van Antwerpen ook de komende jaren boven Rotterdam zal worden verkozen als preferente smokkelhaven, zoals nu het geval lijkt, valt lastig te voorspellen.

Verwacht wordt ook dat de verzending van cocaïne via de (pakket)post zal groeien. Op dit moment worden in Nederland ongeveer 5 miljoen pakketten gedistribueerd, over een aantal jaar zullen dat er ruim 6 miljoen zijn. Deze groei en de verdere automatisering van de postafhandeling maakt verzending van cocaïne via de post aantrekkelijk, omdat criminelen hun werkwijzen goed kunnen afschermen. Deze bedrijfsvoering via de post rendeert op basis van het *many-little*-principe: veel kleine partijen leveren ook veel geld op.

Technologische ontwikkelingen maken het steeds ingewikkelder om langs de logistieke smokkellijnen cocaïne 'uit te halen'. Ook worden steeds meer menselijke schakels in logistieke lijnen overbodig. Dat betekent dat de overgebleven schakels, de sleutelfiguren die knooppunten op logistieke lijnen bemannen, belangrijke functionarissen worden voor criminelen. Omdat het zonder hun hulp steeds lastiger wordt cocaïne Nederland in te krijgen, zullen criminelen hen vaker benaderen om tegen betaling mee te werken. Daartoe wordt ook gebruikgemaakt van *social engineering,* het via het internet benaderen van deze sleutelspelers. Verwacht wordt dat de bovenwereld, vaker dan voorheen, zal worden geconfronteerd met gevallen van corruptie. Om dat tegen te gaan, zijn er initiatieven onder meer om medewerkers van de Rotterdamse haven weerbaar te maken. Het havenbestuur en de (lokale) overheid vragen onder havenpersoneel aandacht voor het tegengaan van criminele uitwassen. Dat doen ze in programma's die gericht zijn op bewustwording van de risico's die de (digitale) integriteit van de Rotterdamse haven bedreigen. Ook wordt ingezet op een cultuuromslag.
Digitale hulpmiddelen zullen vaker door criminelen worden ingezet om in te breken in logistieke (bedrijfsprocessen)systemen. Daarvoor worden hackers en *hacktools* ingeschakeld.

Hoe het internet, en het darknet in het bijzonder, zich de komende jaren als verkoopkanaal voor cocaïne gaat ontwikkelen, is onduidelijk. De rol van de georganiseerde criminaliteit lijkt hierin vooralsnog beperkt. Vanuit Nederland zien we op het darknet vooral de verkoop van ecstasy. Als de verkoop van cocaïne via internet toeneemt, kan dit ertoe leiden dat het gebruik ervan laagdrempeliger wordt.

Verwacht wordt ook dat het geweld rondom de handel in cocaïne de komende jaren verder zal toenemen. Dat komt doordat nieuwe criminele groepen gaan concurreren met gevestigde criminele groepen bij een gelijkblijvende vraag. Met andere woorden, het marktaandeel van de gevestigde orde komt onder druk te staan.

Groepen die marktaandeel proberen af te pakken, zijn onder andere groepen van Nederlands-Marokkaanse afkomst en Oost-Europese samenwerkingsverbanden. De afgelopen jaren heeft hun komst al geleid tot een toename van gewelddadige incidenten, waaronder liquidaties. Incidenteel krijgen personen op sleutelposities in de logistieke keten ook vaker met geweld of dreiging met geweld te maken, omdat het uithalen van cocaïne op haventerreinen moeilijker is geworden.

1.2.5 Kwalificatie van dreiging

Nederland heeft een gebruikersmarkt van 170.000 personen die samen voor ruim 180 miljoen euro aan cocaïne gebruiken. De groothandelsmarkt (de verkoop en distributie van cocaïne naar andere Europese landen) is daar in omvang een veelvoud van.

Het gebruik van cocaïne leidt voor een deel van de gebruikers tot gezondheidsklachten. Door het versnijden van cocaïne met levamisol lopen frequente gebruikers een verhoogd risico op ernstige fysieke klachten. De handel in en smokkel van cocaïne gaat gepaard met veel geweldsincidenten. Conflicten die ontstaan binnen het criminele milieu als gevolg van het niet nakomen van afspraken en weggeraakte of onderschepte partijen leidden de afgelopen jaren tot tientallen liquidaties. Medewerkers in de transport- en logistieke sector lopen het risico te worden geconfronteerd met uithalers die met bedreiging en geweld hun smokkelwaar proberen te bemachtigen.

De jaarlijkse financiële schade loopt vermoedelijk in de tientallen miljoenen euro's. De behandeling van de 7500 problematische cocaïnegebruikers in de verslavingszorg vormt hier de grootste kostenpost. Van de ondermijnende effecten die gepaard gaan met de cocainehandel en -smokkel zijn verweving van onder- en bovenwereld, corruptie en oneerlijke concurrentie de voornaamste.

Voor de komende jaren worden geen grote veranderingen verwacht op de Nederlandse gebruikersmarkt. Ook de Europese cocaïnemarkt is qua omvang redelijk stabiel en Nederland is en blijft de komende jaren een belangrijke toegangspoort voor de smokkel van cocaïne naar Europa. Door voortschrijdende automatisering en robotisering in de afhandeling van containervervoer zijn criminelen voor hun cocaïnesmokkel steeds meer afhankelijk van hulp van binnenuit. Corruptie zal verder toenemen doordat de druk op medewerkers uit de logistieke sector en op medewerkers van toezichthoudende en controlerende instanties groter wordt. Ook het geweld neemt toe door de verwachte machtsstrijd tussen nieuwe criminele groepen en de gevestigde criminele orde. Gelet op de huidige gevolgen en de te verwachten ontwikkelingen in de nabije toekomst vormt de handel in en smokkel van cocaine een **dreiging** voor de komende vier jaar.

1.3 Handel in en smokkel van heroïne

1.3.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Handel in en smokkel van heroïne. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar de handel in en smokkel van heroïne dat ten behoeve van dit dreigingsbeeld is uitgevoerd in de eerste helft van 2016. De auteur van het onderzoeksrapport is Frank Boerman, werkzaam bij de politie. De bronnen die hij bij zijn onderzoek heeft gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

We bespreken hier de georganiseerde smokkel van en handel in heroïne die op Nederlands grondgebied of door Nederlanders in het buitenland plaatsvindt. Gekeken wordt naar alle activiteiten die ermee samenhangen, van de productie van grondstoffen voor heroïne tot en met de afzet van het eindproduct. Internationale trends en ontwikkelingen worden beschreven voor zover zij van invloed zijn op de ontwikkeling van de Nederlandse heroïnemarkt en de criminele samenwerkingsverbanden die daarop actief zijn.
De strafbaarheid van de smokkel van en handel in heroïne is vastgelegd in de Opiumwet, heroïne staat als harddrug vermeld op lijst I. Het bezit van, de productie van en de handel in heroïne is in Nederland strafbaar, het gebruik niet.

1.3.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

Indicaties voor de omvang van de handel in en smokkel van heroïne worden ontleend aan cijfers over vraag, aanbod en prijs. Het aantal gebruikers van heroïne in Nederland is relatief klein. In recent bevolkingsonderzoek naar drugsgebruik wordt het aantal 'ooitgebruikers' geschat op 40.000. Recente (laatste jaar) en actuele (laatste maand) gebruikers van heroïne komen überhaupt niet in het bevolkingsonderzoek naar voren, waarschijnlijk omdat incidenteel en 'recreatief' gebruik van heroïne nauwelijks voorkomt. Het gebruik van heroïne is niet populair in Nederland, deze drug heeft een slecht imago en staat bekend als een *loserdrug.* Uit onderzoek onder uitgaanspubliek blijkt dat het gebruik van opiaten daalt. De gebruikerspopulatie van heroïne bestaat vooral uit problematische drugsgebruikers. Uit recent onderzoek blijkt dat ook deze groep slinkt en veroudert. Over de periode 2008-2014 kromp de groep problematische opiaatgebruikers van ongeveer 17.700 naar 11.500 gebruikers. Was de gemiddelde leeftijd in 2000 nog 37 jaar, in 2010 steeg die naar 45 jaar en in 2012 naar 48 jaar. De verwachting is dat de populatie probleemgebruikers anno 2016 verder is gekrompen met een nog hogere gemiddelde leeftijd.

Ook in Europa daalt het aantal gebruikers van opiaten (inclusief probleemgebruikers) licht. Sinds 2009 daalde het aantal mensen dat in het voorgaande jaar minstens eenmaal opiaten had gebruikt van 3,3 miljoen naar iets minder dan 3 miljoen (in 2013). De jaarlijkse waarde van de Europese opiatenmarkt wordt geschat op minimaal 6,8 miljard euro. Daarmee is heroïne, na cannabis, de grootste illegale drugsmarkt in Europa.
Wereldwijd wordt het aantal opiaatgebruikers al jaren stabiel geschat op 16,5 miljoen.

Afgaand op het aantal gebruikers in Nederland is de geschatte omvang van de Nederlandse heroïneconsumptie hooguit 1,6 ton per jaar. Op groothandelsniveau gaat het dan om 800 kilo heroïne, omdat heroïne bijna altijd wordt versneden met andere stoffen, zoals cafeïne en paracetamol. Dit is een bovengrens, omdat het grootste deel van de probleemgebruikers in Nederland een beroep doet op de verslavingszorg en methadon verstrekt krijgt. In vergelijking met andere Europese landen is de gebruikersmarkt in Nederland klein. De grootste Europese gebruikersmarkten bevinden zich in het Verenigd Koninkrijk, Duitsland, Frankrijk en Italië.

In de afgelopen vier jaar betrof de hoeveelheid in beslag genomen heroïne met een link naar Nederland ruim 8 ton. Het gaat hier om een absolute ondergrens: handhavings- en opsporingsinstanties pakken maar een deel van de gesmokkelde heroïne en cijfers van geslaagde leveranties van duizenden kilo's heroïne die via 'terugrechercheren' aannemelijk konden worden gemaakt, zijn hier niet meegeteld. Deze hoeveelheid in beslag genomen heroïne overstijgt ruim de hoeveelheid die heroïnegebruikers in Nederland nodig hebben. In 2014 piekte het aantal kilo's heroïne dat in Nederland in beslag werd genomen. Er werd ruim 2800 kilo aangetroffen in enkele zeer omvangrijke partijen. Afgaand op de inbeslagnamecijfers stellen we vast dat Nederland voor de verspreiding van heroïne een van de distributiecentra in Europa is. Dat blijkt ook uit het feit dat de partijen heroïne die Nederland binnenkomen veel groter in omvang zijn dan de partijen uit Nederland die in het buitenland worden aangetroffen.

Tussen 2012 en 2016 fluctueert de groothandelsprijs voor heroïne tussen de 15.000 en 20.000 euro per kilo. Al met al lijkt de prijs voor heroïne in Nederland redelijk stabiel. Tegen de achtergrond van een licht dalende Europese gebruikersmarkt en een fors opgeschroefde opiumproductie in Afghanistan in het afgelopen decennium ligt het in de rede een prijsdaling te verwachten. Daar lijkt echter geen sprake van. Het is mogelijk dat het stabiele prijspeil van heroïne het resultaat is van prijsafspraken of beperkte concurrentie op de heroïnemarkt, maar feitelijk is daar niets over bekend. Wat dat betreft is de prijs als indicator voor de omvang van de heroïnemarkt in Nederland onbruikbaar.

Aard

Heroïne bestemd voor de handel in Nederland is hoofdzakelijk afkomstig uit Afghanistan. Ook heroïne bestemd voor de Europese markt is voor het overgrote deel gemaakt van Afghaanse opium.

De laatste jaren is duidelijk geworden dat duizenden kilo's heroïne uit Afghanistan naar de kuststroken van Iran of Pakistan worden getransporteerd om vervolgens met vracht- of containerschepen richting de oostkust van Afrika te worden vervoerd. Het gaat hier om de zogenoemde zuidelijke route. Vanaf het Afrikaanse continent gaat een deel van de heroïne door naar Europa. Daarbij worden verschillende routes en uiteenlopende smokkelmethoden gebruikt.
Een andere recente ontwikkeling is dat heroïne steeds vaker in zeecontainers rechtstreeks vanuit Pakistan of Iran, zonder tussenstop in Afrika, naar Europa gaat. Ook zien we steeds vaker dat zeecontainers eerst de hele wereld overgaan voordat vracht uiteindelijk wordt gelost. Daardoor is het lastiger vast te stellen of vracht afkomstig is uit landen die als risicovol moeten worden beschouwd. Al met al is de laatste jaren een diversificatie van smokkelroutes zichtbaar.

Desalniettemin blijft de Balkanroute voor de heroïnehandel in Nederland de belangrijkste aanvoerroute. Dat hangt vooral samen met het feit dat Turkse handelaars sinds lange tijd toonaangevend zijn in de heroïnehandel. Zij arrangeren vanuit Turkije transporten over een van de vele varianten van de Balkanroute. Daarbij speelt Griekenland een steeds voornamere rol. Een groot deel van de naar schatting 60 tot 65 ton heroïne die via de Balkan wordt gesmokkeld, gaat via Griekenland. Regelmatig wordt daarbij een link naar Nederland of naar Turkse criminele samenwerkingsverbanden in Nederland aangetroffen.
Daarnaast hebben grote inbeslagnames met een link naar Nederland recent een nieuwe route naar Europa onder de aandacht gebracht. Het gaat om een route vanuit Iran via Armenië of Azerbeidzjan naar Georgië en van daaruit verder over de Zwarte Zee naar Odessa in Oekraïne en Moldavië. Het zou hier gaan om een belangrijke transportroute van Turkse smokkelorganisaties die transport via Turkije willen vermijden.

Turken en Turkse Nederlanders domineren de Nederlandse heroïnemarkt. Ze beheersen een groot deel van de groothandel in heroïne. Daar komt bij dat ze de laatste jaren veelzijdiger zijn geworden. Ze ruilen de heroïne die via de Balkanroute vanuit Turkije naar Nederland komt tegen ecstasy en cocaïne die bestemd zijn voor de opkomende gebruikersmarkten in Turkije. Daarvoor drijft de huidige generatie Turkse handelaars handel met criminelen van andere nationaliteiten, zoals Colombianen en autochtone Nederlanders. Beter dan de vorige generatie is deze groep criminele entrepreneurs qua taal en contactuele vaardigheden in staat om zakenrelaties met hen aan te gaan en te onderhouden. Ook besteden ze meer taken uit. Het gaat om het *outsourcen* van delen van het transport vanuit Zuidwest-Azië naar Europa, het wegsluizen en witwassen van criminele opbrengsten, het uitvoeren van criminele afrekeningen en het inschakelen van personen die daarbij faciliteren (bijvoorbeeld door het regelen van vluchtauto's en wapens). En hoewel het aantal criminele afrekeningen in het afgelopen decennium gelijk is gebleven (met uitzondering van 2014), is het gebruik van excessief geweld toegenomen door het gebruik van automatische wapens. Experts spreken over een jongere generatie die meedogenlozer en onzorgvuldiger is, getuige de toenemende openbaarheid waarin de liquidaties gepleegd worden en de persoonsverwisselingen die

daarbij sinds 2012 vaker voorkomen. De huidige generatie Turkse criminelen investeert criminele verdiensten niet alleen in het buitenland, maar ook in Nederland. Experts betogen dat zij er steeds beter in slagen om door de aankoop van onroerend goed, bedrijven en horecagelegenheden een gezaghebbende plek in de Nederlandse samenleving te verwerven.

De laatste jaren zijn ook andere nationaliteiten zich nadrukkelijker met de heroïnehandel en -smokkel in Nederland gaan bezighouden. Zo exploiteren Albanezen voornamelijk met tussenhandel smokkellijnen naar het Verenigd Koninkrijk. Pakistanen exploiteren vergelijkbare lijnen met luchtvracht en postpakketten vanuit Pakistan naar het Verenigd Koninkrijk. Personen van Marokkaanse herkomst houden zich bezig met de tussen- en straathandel van heroïne en het versnijden en herverpakken van de drugs. Nederlandse subjecten vallen op vanwege hun rol bij het transport en de afzet van heroïne naar andere Europese landen. Irakezen en Pakistanen profiteren van de heroïnehandel door zich te laten inhuren voor het regelen van geldtransacties of het witwassen van criminele verdiensten.

In toenemende mate worden vormen van afscherming toegepast. Het gebruik van versleutelde BlackBerry's is gemeengoed geworden, evenals het gebruik van professionele peilbakens voor het volgen van potentiële liquidatie-slachtoffers. Ook zetten criminelen in op het verkrijgen van een van overheidswege verstrekt TIR-vignet of *Authorised Economic Operator*-label om minder transport- en douanecontroles te hoeven doorstaan. De afscherming door criminelen zien we ook terug in het toenemende aantal papieren verhuizingen en een vergrote mobiliteit. Steeds vaker weten criminele kopstukken te vluchten naar het buitenland als de opsporing te 'dichtbij komt'.

1.3.3 Huidige gevolgen

In Nederland schommelt het aantal sterfgevallen ten gevolge van overdosering bij opiaatgebruik rond de 50 per jaar. Jaarlijks komen daar nog eens 15 sterfgevallen bij door hiv/aids als gevolg van injecterend drugsgebruik. Dat aantal daalt doordat het injecterend gebruik sinds jaren afneemt. Sinds 2012 zijn er bovendien in ons land 10 liquidaties geweest die te relateren zijn aan de heroïnehandel.
Behalve in deze slachtoffers manifesteren de gevolgen van de heroïnehandel en -smokkel zich ook in de kosten voor methadonbehandeling voor de ongeveer 11.000 opiaatverslaafden in Nederland. Die bedragen naar schatting 50 miljoen euro op jaarbasis. Ook zijn er kosten gemoeid met verzuim door gebruikende werknemers, met ziekenhuisopnamen en met de afhandeling van liquidaties door politie en andere overheidsinstanties.
Andere gevolgen zijn de toenemende angst bij de bevolking door het toenemende zichtbare geweld in de openbare ruimte en de kans op onbedoeld slachtofferschap daarbij.
Voorts bestaat er een tendens onder Turkse criminelen om etnische verwanten in te schakelen voor hand-en-spandiensten door in te spelen op hun loyaliteitsgevoelens jegens de eigen etnische groep.
En dan is er nog sprake van verweving van onder- en bovenwereld, omdat criminelen machtsposities weten op te bouwen door sleutelposities te (laten) bezetten op logistieke of

financiële knooppunten die gebruikt worden bij de heroïnehandel. Het gaat onder andere om sleutelposities in havens, bij banken en bij dekmantelfirma's.
Daarnaast is het investeringsklimaat voor criminelen gunstig. Zonder argwaan te wekken zien steeds meer criminelen kans hun criminele verdiensten te investeren in onroerend goed in Nederland en het buitenland.

1.3.4 Verwachtingen

Van een oplossing voor het drugsprobleem door het aanpakken van het aanbod van heroïne hoeft weinig te worden verwacht. Hoewel het officiële beleid van de Afghaanse regering gericht is op het bestrijden en terugdringen van de papaverteelt, komt daar in de praktijk om verschillende redenen weinig van terecht. De taliban hebben het in verschillende delen van Afghanistan voor het zeggen en in die gebieden is papaverproductie toegestaan. Voor veel boeren bestaan nauwelijks alternatieve bestaansmogelijkheden en initiatieven voor de teelt van andere gewassen stranden. Bovendien leidt de teelt van alternatieve gewassen ertoe dat de hulpkrachten die nodig waren voor de intensieve papaverteelt werkloos worden en hun eigen papaverteelt beginnen. De Afghaanse opium- en heroïneproductie zal daarom in de periode tot 2021 op een hoog niveau blijven.

Op de Europese en de Nederlandse gebruikersmarkt worden geen grote verschuivingen verwacht. Een opleving van heroïnegebruik zoals momenteel in de Verenigde Staten, wordt in Nederland niet verwacht. De oorzaak voor de forse toename in de VS ligt in het brede legale gebruik van pijnbestrijding. De medicijnen die artsen voorschrijven, leiden tot verslaving. Na beëindiging van de medicatie gaan patiënten op zoek naar een vervanger, en die vinden ze in heroïne. Nederland kent echter een wat andere praktijk van pijnbestrijding en ex-patiënten zullen hier niet snel naar heroïne grijpen als alternatief, omdat heroïne in ons land het imago van een loserdrug heeft.

Als we kijken naar de productie en logistiek, zien we dat criminele samenwerkingsverbanden steeds flexibeler worden. Uit de recente ontdekking van twee laboratoria in Spanje waar morfine wordt omgezet naar heroïne blijkt dat de criminele groepen kansen zien om een deel van de productie van heroïne naar Europa te verschuiven. Ook brengen criminelen steeds vaker veranderingen aan in aanvoerroutes, afhankelijk van de weerstand die ze op hun smokkelroutes te verduren hebben. Verwacht wordt dan ook dat criminelen de instabiliteit op het hele Afrikaanse continent (gebrekkige opsporing en handhaving, corruptie) blijven benutten voor de smokkel van heroïne. Mogelijk neemt de heroïnesmokkel daardoor zelfs toe. Routes worden naar verwachting ook verlegd als gevolg van de intensievere controles van migratiestromen op sommige traditionele smokkelroutes. Hetzelfde verwachten we voor het gebruik van havens. Vanwege de toegenomen controles in grotere havens in Pakistan en Turkije wijken criminelen uit naar kleinere havens. De diversifiëring van smokkelroutes en -methoden zien we ook terug in de verwachte toename van smokkel per trein, ook als gevolg van toegenomen controles op luchthavens. Een smokkelroute die de aankomende jaren opgeld zou kunnen doen, is de route via de landen van de EEU, de *Eurasian*

Economic Union. Deze vrijhandelszone van Armenië, Wit-Rusland, Kazachstan, Kirgizië en Rusland leidt tot minder grenscontroles tussen die landen.
Of de afzet van heroïne via internet, in het bijzonder *darknet markets*, gaat toenemen is ongewis. Op dit moment zit de groei van internet als afzetkanaal voor drugs vooral in de verkoop van nieuwe psychoactieve stoffen en synthetische drugs. Wel kan het toenemend gebruik van internet de drempel om heroïne te gaan gebruiken verlagen en de verkrijgbaarheid van heroïne vergroten. Op die manier kan een nieuwe afzetmarkt voor heroïne ontstaan. Ook nadert het moment dat opiumproducenten in Afghanistan zelf online gaan en hun afzet via internet gaan regelen.

De vraag naar de verwachte gevolgen voor 2021 hangt vooral af van de vraag hoe de vraagmarkt voor heroïne zich de komende jaren ontwikkelt. De afgelopen jaren laten immers zien dat de aanbodkant continu evolueert. De productie en het aanbod van heroïne zetten zich onverminderd voort. De vraag naar heroïne zal verder afnemen tot 2021. Daarmee nemen de schadelijke gezondheidseffecten ook af. Wat niet afneemt, is de ondermijning, net zo min als de schade ten gevolge van de grootschalige handel door heroïnehandelaars die in en vanuit Nederland afzet van heroïne naar Europa organiseren.

1.3.5 Kwalificatie van dreiging

Het gebruik van opiaten in Nederland neemt al jaren af. Niettemin blijft het jaarlijkse aantal doden door overdosering en injecterend gebruik stabiel, ongeveer 65. Daar komen de slachtoffers ten gevolge van liquidaties in het criminele milieu bij. De kosten van de verslavingszorg voor de 11.000 opiaatverslaafden in Nederland bedragen naar schatting 50 miljoen euro per jaar.

Het overgrote deel van de naar Nederland gesmokkelde heroïne is niet bestemd voor Nederlandse gebruikers maar voor gebruikers in andere Europese landen. Hier gevestigde criminele samenwerkingsverbanden organiseren omvangrijke heroïnetransporten vanuit het buitenland naar Nederland. Vervolgens vindt afzet in kleinere partijen plaats naar de rest van Europa. Aanzienlijke criminele verdiensten worden witgewassen met behulp van ondernemingen en geïnvesteerd in de bovenwereld, zowel in Nederland als in het buitenland. Met het geld uit de drugshandel verkrijgen criminelen een positie in het legale bedrijfsleven.

In 2021 bestaat er naar verwachting nog steeds een grote Europese gebruikersmarkt.In Nederland blijven Turks/Nederlandse criminele samenwerkingsverbanden actief. Beheersing van de Turkse taal en goede connecties met toonaangevende criminelen in Turkije blijven naar verwachting belangrijke voorwaarden voor het realiseren van grootschalige heroïnetransporten. Het geweld dat gepaard gaat met deze drugshandel, inclusief liquidaties in de openbare ruimte, zal de komende jaren voortduren. Vanwege de maar langzaam afnemende gezondheidsschade en de blijvende ondermijnende effecten is de handel in en smokkel van heroïne een **dreiging** voor de komende vier jaar.

1.4 Productie van, handel in en smokkel van synthetische drugs

1.4.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Synthetische drugs en precursoren. Criminaliteitsbeeldanalyse 2016.* Dat rapport doet verslag van onderzoek naar synthetische drugs dat in de eerste helft van 2016 is uitgevoerd voor dit dreigingsbeeld. De auteurs van het onderzoeksrapport zijn Monique Bruinsma (Bureau Bruinsma) en Loek van Lier, die werkzaam is bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*

Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Tot het domein van de synthetische drugs rekenen we hier de volgende drie soorten stoffen:

1. synthetische drugs zoals die zijn opgenomen in de lijsten I en II behorende bij de Opiumwet;
2. de Nieuwe Psychoactieve Stoffen (NPS). Hiermee worden synthetische stoffen bedoeld met een psychoactieve werking die pas sinds kort op de drugsmarkt worden aangetroffen en nog niet onder de Opiumwet vallen;
3. geneesmiddelen die in Nederland als psychoactieve drug worden gebruikt.

1.4.2. Ontwikkelingen in aard en omvang sinds het NDB2012

Werkwijze

De belangrijkste grondstoffen voor de productie van amfetamine en MDMA (de werkzame stof in ecstasy) zijn de precursoren BMK en PMK. Door strafbaarstelling en strengere controle op de productie en export van BMK en PMK in China en Rusland zijn criminele samenwerkingsverbanden gaan zoeken naar alternatieven. Dit manifesteerde zich al ten tijde van het vorige dreigingsbeeld en is na 2012 verder geëvolueerd. Drugsproducenten vervaardigen tegenwoordig zelf hun precursoren BMK en PMK met stoffen die pre-precursoren genoemd worden. Stoffen die in beginsel niet onder internationale wet- en regelgeving vallen, zijn voor de producenten goedkoop en probleemloos in China te verkrijgen. In de jaren 2011 tot 2013 werd in Nederland een 'vloedgolf' aan de pre-precursor APAAN waargenomen. In december 2013 werd deze stof internationaal geregistreerd, waardoor bezit en import zonder vergunning illegaal werden. Als gevolg daarvan heeft APAAN plaatsgemaakt voor alternatieven zoals natriumzout van BMK-glycidezuur, APAA en andere niet-geregistreerde pre-precursoren van BMK. Ook voor de productie van PMK vindt men alternatieve stoffen, zoals het natriumzout van PMK-glycidezuur. Omdat het aantal legaal te verhandelen stoffen waarmee precursoren gemaakt kunnen worden groot is, ontstaat er een juridisch kat-en-muisspel.

Een nieuwe ontwikkeling is dat de smokkel van (pre-)precursoren nauwelijks meer georganiseerd wordt met hulp van in Nederland gevestigde Chinese criminele groeperingen. Nederlanders regelen het nu zelf: bestellingen vinden plaats via internet en verlopen hoofd-

zakelijk via zelf opgerichte chemische bedrijven in vooral Oost-Europa en Hongkong. Om de kans op controle te verkleinen voorziet men gevaarlijke stoffen van een foutieve goederenbeschrijving waardoor deze ongevaarlijk lijken. Door dergelijke 'mislabeling' ontstaan gevaarlijke situaties bij het transport met lucht- en zeevracht naar Nederland.

Naast de precursoren worden bij de synthetische drugsproductie ook diverse andere chemicaliën gebruikt. Voor de verwerving van deze stoffen wordt België nog steeds als hofleverancier gezien, maar komen Oost-Europese landen als Polen en Roemenië ook steeds meer in beeld. Op productieplaatsen worden chemicaliën en afvalproducten hoofdzakelijk aangetroffen in 'geneutraliseerde' verpakkingen. Zonder authentieke labels is de herkomst van stoffen niet te achterhalen, waardoor *backtracking* door opsporingsinstanties onmogelijk wordt en de criminele grondstoffenhandelaar zijn inkoopbron niet prijsgeeft aan concurrenten. Opvallend zijn de grote hoeveelheden aan chemicaliën die bij opslagplaatsen in 2014 en 2015 zijn aangetroffen. Dit wijst erop dat de criminele organisaties die zich richten op de chemicaliënhandel ten behoeve van de synthetische drugsproductie, internationaler, professioneler en grootschaliger zijn geworden.

Hardware in de vorm van tabletteermachines en stempels wordt tegenwoordig alleen nog maar in China gekocht en in 2014 is voor het eerst een compleet in China aangeschaft lab in Nederland aangetroffen. Grotere productieketels worden meestal door professionele ketelbouwers gemaakt, terwijl glaswerk en verwarmingsapparatuur in de regel van (inter)nationale groothandelaars wordt verkregen. Het gehele productieproces is professioneler geworden. Criminelen werken veel meer dan voorheen met gebruik van meet- en regeltechniek; er wordt nu ook gewerkt met speciale van kunststof vervaardigde reactieketels. De tijd van amateurisme lijkt voorbij. In relatief korte tijd is nieuwe hardware ontwikkeld voor de conversie van chemicaliën. Vaker dan voorheen worden chemici uit de legale branche om advies gevraagd. Recepten op kladpapiertjes worden nauwelijks meer aangetroffen. Veel kennis en kunde wordt verkregen van het internet.

Een nieuwe ontwikkeling is dat er criminele samenwerkingsverbanden in Nederland zijn die zich hebben toegelegd op de productie van mefedron. Mefedron werd vóór 2011 als NPS geïmporteerd uit China. Sinds de stof in 2011 verboden is, zijn criminele samenwerkingsverbanden deze zelf gaan produceren om de internationale markt te bedienen. Daarnaast zijn er signalen dat criminele samenwerkingsverbanden in Nederland het ook lucratief vinden om methamfetamine en captagon te produceren en te exporteren.

De verkoop via internet van synthetische drugs en NPS is de laatste jaren belangrijker geworden. Nederland speelt een rol als distributeur op deze digitale drugsmarkt. De producten worden vanuit Nederland in postpakketten verstuurd. De Australische douane heeft door deze postzendingen met voornamelijk ecstasy en NPS een honderdprocentscontrole op Nederlandse post ingevoerd – met als gevolg een toename van Nederlandse drugspostzendingen net over de grens, vanuit Duitsland. Verder is het aantal in de Verenigde Staten

onderschepte postpakketten met ecstasy afkomstig uit Europa toegenomen; dit duidt op meer verkoop via internet naar de VS. De al eerder ingezette trend van afzet van ecstasy naar Zuid-Amerika zet zich voort. Opvallend is nog de onderschepping eind 2014 van een partij ecstasypillen uit Nederland in Zuid-Afrika.

De geografische spreiding van productielocaties is ongelijk verdeeld over ons land. De productie van synthetische drugs speelt zich nog steeds hoofdzakelijk af in het zuiden van Nederland. Wel steeg het aantal dumpingen en lozingen in Gelderland van 9 in 2014 naar 16 in 2015, in Zuid-Nederland daalde dit aantal licht van 126 in 2014 naar 116 in 2015. Dit kan wijzen op een lichte verschuiving van het zuiden naar Gelderland. Verder zijn er recent diverse opsporingsonderzoeken in Den Haag geweest waarbij de chemicaliën en producenten uit Zuid-Nederland kwamen.

Betrokken personen en criminele samenwerkingsverbanden

In de loop der jaren is een redelijk helder beeld ontstaan van betrokken personen en netwerken. De toonaangevende criminele ondernemers van dit moment zijn personen die grotendeels al jaren meedraaien in de top van de georganiseerde synthetischedrugscriminaliteit en in bijna alle gevallen grootschalige productie en export financieren en organiseren. In veel gevallen gaat het om personen die oorspronkelijk afkomstig zijn uit de woonwagengemeenschap in Zuid-Nederland. Naast de bovenbeschreven groep oude bekenden lijkt de betrokkenheid toe te nemen van wat meer onervaren, over het algemeen jongere personen, die zelf het productieproces uitvoeren. De laboranten van weleer blijken steeds meer het proces aan te sturen.

De grootste ontwikkeling die na 2012 wordt waargenomen, is de toegenomen invloed van outlaw motorcycle gangs (OMG's) binnen de wereld van de synthetische drugs. Voor 2012 beperkte de betrokkenheid zich hoofdzakelijk tot de leden van één motorclub die synthetische drugs exporteerden. Daarna raakten leden van meer OMG's betrokken bij schakels van de logistieke keten, van productie tot afzet. Synthetischedrugscriminelen sluiten zich aan bij motorclubs, vinden op die manier bescherming voor hun criminele handelen en beschikken door de sterke internationale georganiseerdheid van dergelijke clubs tevens over een uitgebreid netwerk met nationale en internationale vertakkingen. Gelet op recent opsporingsonderzoek naar de smokkel van amfetamine spelen leden van OMG's een belangrijke rol in de afzet van die drugs naar Scandinavische landen. Er zijn aanwijzingen dat dit ook geldt voor de afzet naar Australië. Volgens deskundigen zijn leden van OMG's structureel betrokken bij afpersingen in het criminele circuit. Ook spelen zij een rol bij liquidaties, in 2015 is in elf liquidatieonderzoeken in Zuid-Nederland een relatie gelegd met leden van OMG's.

Nederlandse en Poolse criminelen zijn de laatste jaren meer gaan samenwerken. In Nederland verblijvende Poolse arbeiders worden in Nederlandse laboratoria gezien of zijn in een sleutelrol actief betrokken bij amfetaminesmokkel naar Polen. Er zijn plannen gesmeed

om in Polen een drugslaboratorium op te zetten. Verder speelt Polen nog steeds een rol in de smokkel van precursoren, chemicaliën en glaswerk naar Nederland.

Rechtspersonen worden gebruikt als dekmantelfirma ten behoeve van het criminele bedrijfsproces. Bedrijven worden ingezet voor het verkrijgen van de benodigde chemicaliën of voor het huren van locaties voor de opslag, de productie en het transport van de drugs. Een toegepaste werkwijze bestaat uit het misbruiken van de goede naam van andermans bedrijf door op naam van dat bonafide bedrijf bestellingen te doen. Ook worden bedrijven in het buitenland opgezet om daar de benodigde chemicaliën te bestellen. Dit gebeurt met name in Oost-Europese landen en in China.

Omvang van productie en gebruik in Nederland

De indicatoren voor de omvang van de productie van synthetische drugs in Nederland wijzen op een toename van de productie in de afgelopen periode. Het aantal aangetroffen synthetischedrugslaboratoria steeg van 30 in 2012 naar 59 in 2016. Het aantal onderschepte partijen pre-precursoren nam in die periode ook toe, evenals het aantal opslaglocaties en dumpingen.
De ecstasyproductie in Nederland is voor 2015 geschat op 50 tot 117 miljoen pillen. De totale hoeveelheid geproduceerde amfetamine in Nederland lag in dat jaar naar schatting tussen de 22 en 51 ton. Gezien de aangetroffen laboratoria lijkt de productie van methamfetamine gedurende de onderzoeksperiode in Nederland nog steeds beperkt van omvang, hoewel de inbeslagname in 2014 van 850 kilo methamfetamine die vermoedelijk in Nederland is geproduceerd anders doet vermoeden.
De grootschalige productie van synthetische drugs in het buitenland beperkt zich hoofdzakelijk tot België. Gebleken is dat Nederlanders daar actief zijn als producent of opdrachtgever. Ook in Polen is sprake geweest van enkele laboratoria.
De synthetische drugs die in Nederland of met hulp van Nederlanders in het buitenland worden geproduceerd, worden afgezet op gebruikersmarkten over de hele wereld. De belangrijkste afzetlanden van ecstasy zijn Australië, Turkije, Groot-Brittannië en Spanje. Amfetamine vindt zijn bestemming in Scandinavische landen als Finland en Zweden, maar ook in Groot-Brittannië en Spanje. Het gebruik van synthetische drugs in de wereld stijgt en hierdoor groeit de afzetmarkt voor in Nederland geproduceerde drugs.

Op de Nederlandse markt voor drugsgebruikers zijn al geruime tijd vijf soorten synthetische drugs dominant: ecstasy, amfetamine, GHB, ketamine en lsd. Hoewel de gegevens over het drugsgebruik onder de Nederlandse bevolking uit de meest recente metingen (2009 en 2014) van de *Nationale Drug Monitor* (NDM) niet met elkaar mogen worden vergeleken, menen deskundigen op grond van deelstudies dat het gebruik van in het bijzonder ecstasy en amfetamine in Nederland sinds 2009 is toegenomen. In 2014 lag het recente gebruik van ecstasy onder 15- tot 64-jarigen in Nederland rond de 2,5 procent en het actuele gebruik rond de 0,7 procent (respectievelijk ongeveer 270.000 personen en 80.000 personen). Het

recente gebruik van amfetamine lag in dat jaar rond de 1,3 procent en het actuele gebruik rond de 0,5 procent (respectievelijk ongeveer 140.000 personen en 60.000 personen).
Het gebruik van GHB, ketamine en lsd lag op een veel lager niveau dan dat van ecstasy en amfetamine. GHB had in 2014 naar schatting 50.000 recente gebruikers en 10.000 actuele gebruikers (respectievelijk 0,4 en 0,1 procent). Wat betreft de toe- of afname van GHB-gebruik spreken bronnen elkaar tegen; wel wordt een trend waargenomen dat problematisch GHB-gebruik zich heeft verspreid vanuit de Randstad naar het platteland. Ketamine wordt in ons land populairder. Dit geneesmiddel wordt door criminelen direct als eindproduct ingekocht en vervolgens als psychoactieve drug doorverkocht. Uit meerdere bronnen blijkt dat er in Nederland een aanzienlijke groep gebruikers is ontstaan voor dit middel: het aantal ketamine-gebruikers wordt in ons land ongeveer even groot geschat als het aantal GHB-gebruikers. Lsd wordt in Nederland veel minder gebruikt dan ecstasy en andere party-drugs.

Hoewel methamfetamine wereldwijd de meestgebruikte synthetische drug is, is het gebruik ervan in Nederland te verwaarlozen. Vooral in Azië, Noord-Amerika en Oceanië is de drug erg populair. Daar zit het gebruik van methamfetamine al jarenlang in de lift; de Australische premier verkondigde in 2015 zelfs dat zijn land in de greep is van een 'ice-epidemie'. Wereldwijd neemt het ecstasygebruik af, terwijl het in Europa juist toeneemt.
De interesse in de vele NPS-typen die in Europa worden waargenomen (zoals synthetische cannabinoïden en cathinonen) is bij Nederlandse gebruikers beperkt: volgens experts van het Trimbos-instituut en verslavingsinstellingen is het gebruik van dergelijke stoffen in Nederland marginaal. Een uitzondering hierop vormt 4fluoramfetamine (ook wel 4-FA of 4FMP genoemd). Deze stof, die als NPS in Nederland de bijnaam 'ecstasy-light' heeft gekregen, staat nog niet op de lijst van de Opiumwet. Het plan bestaat om de stof in de loop van 2017 aan de lijst met verboden middelen toe te voegen.

1.4.3 Huidige gevolgen

De synthetischedrugscriminaliteit in Nederland kent diverse ondermijnende aspecten. Allereerst zetten het geweld en de intimidatie door betrokken criminelen de rechtsorde onder druk. Het gebruik van automatische vuurwapens en explosieven op klaarlichte dag is hier een voorbeeld van. Ook ondermijnend is het feit dat via een mol binnen de politieorganisatie politie-informatie werd doorgespeeld aan een grote ecstasyhandelaar. Corruptie deed zich niet alleen voor bij de politie maar ook bij de douane in Antwerpen en Rotterdam. Verder zijn er door drugscriminelen beleidsambtenaren en handhavers onder druk gezet. Dan is er nog de vastgestelde verwevenheid van onder- en bovenwereld, die zich manifesteert door investeringen van drugswinsten in onroerend goed en bedrijven. Deze verweving breidde zich bovendien uit naar veel Oost-Europese landen waar bedrijven werden opgezet om chemicaliën te kunnen smokkelen ten behoeve van de Nederlandse drugsproductie. Voorts werden sommige leden van OMG's publieke personen, wat kan fungeren als een verkeerd voorbeeld en negatief doorwerken op het normbesef van burgers.

Er zijn risico's verbonden aan drugslaboratoria en opslagplaatsen, doordat met chemicaliën wordt gewerkt. Denk aan het gevaar voor omwonenden van laboratoria in woonwijken: ontploffingsgevaar, kans op het ontsnappen van gevaarlijke gassen en brandrisico. Uiteraard worden ook de direct betrokken criminele laboranten aan deze gevaren blootgesteld. Ook het vervoer van chemische stoffen onder valse stofnamen via zee- of luchtvracht komt steeds vaker voor en zorgt voor risico's. Pakketbezorgers kunnen rondlopen met gevaarlijke chemicaliën zonder dat zij dat weten en vliegtuigen worden geladen met brandbare stoffen zonder dat dit op de papieren staat aangegeven. Afvaldumpingen berokkenen schade aan het drinkwater en de voedselketen. Met het veilig ontmantelen van laboratoria en het opruimen van drugsafval is veel geld gemoeid. De maatschappelijke kosten gerelateerd aan de gevolgen van synthetischedrugscriminaliteit in Nederland zijn de afgelopen jaren toegenomen.

Schadelijke effecten voor de gebruikers van synthetische drugs hangen vooral samen met probleemgebruik en gezondheidsrisico's. De *Nationale Drug Monitor* (NDM) van 2015 constateert een toename van het aantal accidentele sterfgevallen door psychostimulantia ten opzichte van de jaren 2004-2012. De data hierover zijn onvolledig, maar ten aanzien van ecstasy is bekend dat er jaarlijks in Nederland tussen de één en negen doden vallen door het gebruik van deze drug. Ook is er vaker noodhulp nodig bij de eerstehulpposten van festivals en bij ziekenhuizen: het aandeel drugsgerelateerde gezondheidsincidenten veroorzaakt door synthetische drugs nam daar de afgelopen jaren toe. In 2009 ging het bijvoorbeeld in 14 procent van de 2525 drugsincidenten om het gebruik van ecstasy, in 2014 was dit in 36 procent van de 3797 drugsincidenten het geval. Ook de ernst van de intoxicatie na het gebruik van synthetische drugs nam in de onderzoeksperiode toe. In 2009 werd 7 procent van de ecstasy-incidenten als matig tot ernstig gekwalificeerd, in 2014 steeg dit tot 28 procent. Deze toename van de ernst van de intoxicatie door ecstasy wordt door de NDM van 2015 gekoppeld aan de steeds verder toegenomen gemiddelde concentratie MDMA in ecstasypillen. Het aantal incidenten door GHB-gebruik in Nederland wordt in de NDM ook als zorg benoemd: hier is het aantal gezondheidsincidenten ten opzichte van het aantal gebruikers ervan relatief hoog te noemen. GHB-gebruik leidt snel tot afhankelijkheid en abrupte stopzetting heeft heftige onthoudingsverschijnselen tot gevolg. Ondanks het grotere aantal acute gezondheidsproblemen door het gebruik van synthetische drugs is het aantal hulpvragen bij de verslavingszorg in verband met het gebruik ervan nog altijd gering te noemen, vergeleken met de zorgvragen in verband met andere drugstypen.

1.4.4 Verwachtingen

De omvang van de synthetischedrugsmarkt in Nederland in termen van productie en export van MDMA laat de komende jaren naar verwachting een verdere groei zien. In ieder geval zal de gebruikersmarkt zowel nationaal als internationaal nog steeds in omvang toenemen. Nederlandse criminelen hebben wereldwijd een stevige marktpositie en een goede naam wat betreft hun eindproduct. Ook is de aanschaf van grondstoffen en hardware voor hen vrij gemakkelijk. Innovatie en conversie zullen de komende jaren kernbegrippen blijven: door

creatief en innovatief gebruik te maken van steeds weer nieuwe grondstoffen en bijbehorende productiemethoden wordt bestaande wet- en regelgeving omzeild en wordt de opsporing en bestrijding van drugsproductie gefrustreerd. De verwachting is al met al dat Nederlandse criminelen hun kansen zullen blijven pakken. Hun criminele activiteiten in Oost-Europese landen zullen daarin meegroeien: van daaruit zullen zij waarschijnlijk een steeds groter deel van hun grondstoffen verwerven (in die landen zelf en/of direct gekocht in China). Verder zullen de digitale inkoop van grondstoffen en hardware en de verkoop van de eindproducten via internet een grotere rol gaan spelen.

Er zal mogelijk niet alleen sprake zijn van meer van dezelfde producten, maar ook van een toenemende gerichtheid op het op de markt brengen van nieuwe producten. Criminelen doen aan kansverkenning en richten zich op nieuwe buitenlandse lucratieve markten, zoals die van methamfetamine, captagon, mefedron en NPS. Gevreesd wordt voor smokkel van methamfetamine vanuit Nederland naar Australië, aangezien Nederlandse criminele samenwerkingsverbanden al beschikken over exportlijnen die kant op voor andere drugs, en omdat methamfetamine in Australië *booming business* is. Verder biedt de toenemende vraag naar ecstasy uit Zuid-Amerikaanse landen de kans aan Nederlandse criminelen om hun product te ruilen tegen cocaïne. En de komst van vluchtelingen uit Syrië en Afghanistan biedt mogelijkheden tot samenwerking met personen uit die landen om captagon te ruilen tegen heroïne. Ruilhandel biedt het voordeel dat de transacties met gesloten beurzen kunnen plaatsvinden, er zijn dan geen geldstromen die de aandacht van controlerende instanties kunnen trekken. Een zorgpunt blijft de betrokkenheid van leden van OMG's. OMG's zijn sterk internationaal georganiseerd en beschikken daardoor over een mondiaal netwerk. Door hun geweldgebruik en intimidatie vormen zij een moeilijk te bestrijden machtsblok.

Naast de al gevestigde criminele producenten komen er naar verwachting ook meer particuliere, zelfstandig werkende drugsproducenten. Deze particulieren gebruiken internet voor het aanbieden van synthetische drugs. De kwaliteit van hun eindproducten is minder goed te voorspellen.

Vanwege de groeiende markt en de stevige Nederlandse criminele scene zullen gezondheidsklachten, milieuvervuiling, overlast en ondermijning ook toenemen. De grotere productiecapaciteit zal meer verwevenheid van onder- en bovenwereld met zich meebrengen. De ondermijnende werking die uitgaat van deze georganiseerde criminaliteit zal vooral in het zuiden van het land gevoeld (blijven) worden.

In juli 2014 heeft het Europese Hof geoordeeld dat het zonder vergunning bereiden, opslaan, in- en uitvoeren van NPS niet langer onder de noemer van de Geneesmiddelenwet kan worden aangepakt door politie en justitie. In tegenstelling tot andere Europese landen ontbreekt het daardoor in Nederland aan adequate wetgeving. Mogelijk heeft dit voor Nederland een aanzuigende werking.

1.4.5 Kwalificatie van dreiging

De negatieve gevolgen van de productie van, handel in en smokkel van synthetische drugs zijn divers. Allereerst zijn er de gebruikers van ecstasy en amfetamine die met gezondheidsklachten hulp zoeken bij de verslavingszorg en de gebruikers die vanwege intoxicatie terechtkomen bij EHBO-posten op grootschalige evenementen of bij de spoedeisende hulp van ziekenhuizen. Deze gevallen van intoxicatie zijn meestal licht en van voorbijgaande aard, in enkele gevallen per jaar heeft intoxicatie niettemin de dood tot gevolg. Bij GHB-gebruikers komt intoxicatie relatief vaak voor en is vaker ernstig van aard. Daarnaast zijn er gezondheidsrisico's verbonden aan het vervoer van gevaarlijke stoffen en het verwerken van stoffen door criminele laboranten. Voor omwonenden van drugslaboratoria in woonwijken bestaat het gevaar van ontploffing, het ontsnappen van gevaarlijke gassen en brand. Personen die gedumpte afvalstoffen aantreffen lopen ook gezondheidsrisico's, evenals degenen die belast zijn met het opruimen ervan. Dumping of lozing van drugsafval heeft ook schadelijke gevolgen voor de bodemgesteldheid en het oppervlaktewater.

De maatschappelijke financiële kosten van problematisch gebruik liggen op de terreinen van arbeid, veiligheid, algemene gezondheidszorg en verslavingszorg. Aangenomen mag worden dat deze kosten zijn gestegen met het toenemende gebruik van synthetische drugs. Het ontmantelen van laboratoria en het opruimen van drugsafval kost jaarlijks miljoenen euro's. Voor milieuzorg en verslavingszorg tezamen liggen de kosten voor de overheid momenteel in de orde van grootte van tientallen miljoenen euro's.

Diverse aspecten van ondermijning doen zich hier gelden. Er is druk uitgeoefend op beleidsambtenaren en handhavers, ook zijn gevallen van corruptie geconstateerd. Verweving toont zich in de al dan niet bewuste betrokkenheid van de autobranche, chemiebedrijven, hardwarebedrijven, locatieverhuur en transportbedrijven. De omvangrijke illegaal verkregen winsten worden ook geïnvesteerd in bedrijven en onroerende goederen. Het normbesef van burgers in het zuiden van het land komt onder druk te staan, omdat zij het idee krijgen dat criminelen 'ermee wegkomen'.

Het gebruik van synthetische drugs zal de komende jaren waarschijnlijk verder toenemen. De sterke criminele infrastructuur voor de productie van synthetische drugs in ons land doet vermoeden dat daarmee ook de negatieve gevolgen verder gaan toenemen: Nederlandse producenten hebben wereldwijd een stevige marktpositie en de hier geproduceerde synthetische drugs vinden hun weg naar afzetmarkten in Europa en ver daarbuiten. Gelet op de negatieve gevolgen op het terrein van milieu, volksgezondheid, financiën en ondermijning die naar verwachting nog verder gaan toenemen, vormt de productie van, handel in en smokkel van synthetische drugs ook de komende jaren een **dreiging.**

1.5 Productie van, handel in en smokkel van cannabis

1.5.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Productie, handel en smokkel van cannabis.* Dat rapport bevat het verslag van een onderzoek dat voor dit dreigingsbeeld is uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Isabel Theunissen en Femke Vaes, beiden werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

De behandeling van cannabis in deze paragraaf spitst zich toe op de in Nederland geproduceerde hennep, de handel daarin en de smokkel daarvan. Hoewel hasjiesj formeel tot de cannabisproducten behoort, wordt daar betrekkelijk weinig aandacht aan besteed, omdat de productie ervan in vergelijking met die van hennep gering is.

1.5.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

Twee indicatoren voor de omvang van de cannabismarkt komen hier aan bod: consumptie en productie. Daarnaast wordt de export van Nederlandse hennep behandeld.

Cannabis is verreweg de meestgebruikte illegale drug in Europa. Meer dan 22 miljoen volwassenen hebben in 2015 cannabis gebruikt en 1 procent van de Europese volwassenen gebruikt dagelijks cannabis. Uit de *Nationale Drug Monitor* van 2014 blijkt onder meer dat 8 procent van de Nederlandse bevolking van 15 tot en met 64 jaar het voorgaande jaar cannabis had gebruikt (recent gebruik) en 4,6 procent de voorgaande maand (actueel gebruik). Vergeleken met het Europese gemiddelde ligt het percentage recente en actuele cannabisgebruikers in Nederland iets hoger. Alleen in Spanje (9,2% en 6,6%) en in Frankrijk (11,1% en 6,6%) is het gebruik hoger dan in Nederland. Onder de schooljeugd (15- en 16-jarigen) ligt het percentage actuele gebruikers met 27 relatief hoog. Alleen in Tsjechië (42%) en Frankrijk (39%) ligt dit percentage hoger. Estland (24%), Letland (24%), Spanje (27%), Slovenië (23%) en Polen (23%) liggen in de buurt.
De gemiddelde jaarlijkse consumptie per cannabisgebruiker in Nederland wordt op 69 tot 93 gram geschat. In Nederland geteelde hennep is veruit de meest favoriete cannabisvariant. De totale binnenlandse consumptie van in Nederland geteelde cannabis wordt in onderzoek van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) voor 2012 en 2013 geschat op een hoeveelheid die ligt tussen de 28 en 119 ton. In een criminaliteitsbeeldanalyse uit 2012 ligt de schatting tussen de 33 en 97 ton voor de periode 2008-2011.

Behalve consumptie zegt ook het energiegebruik iets over de productie. Het aantal ontmantelde kwekerijen daarentegen is geen indicator voor de productie; dit aantal zegt meer over de politiecapaciteit. In de periode 2012-2015 ligt het aantal ontmantelde kwekerijen jaarlijks tussen de vijf- en zesduizend. Het Platform Energiediefstal schat het aantal kwekerijen op grond van de hoeveelheid gestolen energie. In 2014 was dat 1 miljard kilowattuur. Met die hoeveelheid kunnen, bij een gemiddeld jaarlijks verbruik van 35.000 kilowattuur per kwekerij, in Nederland continu zo'n 30.000 hennepkwekerijen actief zijn. Dat zou betekenen dat ongeveer 20 procent van alle kwekerijen tegen de lamp loopt.

De criminaliteitsbeeldanalyse uit 2012 en het WODC-onderzoek uit 2014 doen onder een aantal aannames schattingen van productie, consumptie en export van in Nederland geteelde hennep. Die aannames houden rekening met de opbrengst per plant, het aantal planten, het aantal oogsten van een kwekerij per jaar en de kans op ontdekking van de oogst. Door te variëren in deze aannames ontstaat een drietal scenario's: een laag, gemiddeld en hoog scenario. In tabel 2 zijn de resultaten van beide studies samengevat. Hierin worden alleen het hoge en het lage scenario weergegeven.

Tabel 2. Vergelijking geschatte productie, consumptie en export van in Nederland geteelde hennep

	CBA 2012	WODC 2014
Productie (ton)	187 - 1196	171 - 965
Consumptie (ton)	33 - 97	28 - 119
Export (ton)	90 - 1163	53 - 937

Gegeven de marges lopen de beide schattingen betrekkelijk weinig uiteen. De ruime marges zijn te wijten aan de onbetrouwbaarheid van de beschikbare registraties en de onzekerheid omtrent de nauwkeurigheid van de aannames. Kortom, de schattingen zijn met zo veel onzekerheid omgeven dat er nauwelijks eenduidige conclusies uit getrokken kunnen worden.

Aard

Bij het beschrijven van de ontwikkelingen in de aard van de cannabisteelt passeert een ruim scala aan onderwerpen de revue.

Locaties in het buitenland

Verplaatsing van kwekerijen naar het buitenland is op zichzelf geen nieuwe trend. Wel vindt verplaatsing vaker plaats dan voorheen. Niet alleen de buurlanden België en Duitsland hebben hier last van, ook Spanje en Frankrijk zien kwekerijen opkomen die zijn opgezet met Nederlandse materialen, met behulp van Nederlandse kennis of die gerund worden door Nederlandse misdaadondernemers. In België bijvoorbeeld zou zelfs in 90 procent van de aangetroffen kwekerijen sprake zijn van een dergelijke Nederlandse betrokkenheid.

Kweekbenodigdheden

In het verleden werden kweekbenodigdheden hoofdzakelijk bij *growshops* gekocht. Artikel 11a van de Opiumwet maakt deze bedrijfsactiviteiten sinds maart 2015 strafbaar. Sinds de invoering van het artikel zijn verschillende growshops gesloten. In de praktijk blijkt echter dat veel growshops nog steeds actief zijn. Zij passen zich aan de nieuwe wetgeving aan door verschillende goederen vanaf verschillende locaties te verkopen, gebruik te maken van internet en door registratie achterwege te laten. Kwekers hebben (online) dus nog steeds toegang tot de vereiste kweekbenodigdheden. Het lijkt wel moeilijker te worden om in Nederland aan de benodigde materialen te komen en daarom worden deze ook uit het buitenland gehaald. Regelmatig worden transporten vanuit Duitsland onderschept.

Klimaat

Voor het kweken van cannabis is een goed regelbaar klimaat een groot voordeel. Een veelgebruikt klimaatbeheersingssysteem is de *opticlimate.* Dit is een watergekoelde airco waarmee het klimaat in een kwekerij kan worden beheerst. Het systeem kan circuleren, koelen, verwarmen, ontvochtigen en filteren. Hierdoor wordt het ideale kweekklimaat bereikt. Behalve de beheersing van het klimaat in de kwekerij zorgt het systeem voor een grotendeels geautomatiseerde kweek. Zo worden water- en voedingsstoffen automatisch toegevoegd. Hierdoor ontstaan zelfregulerende kwekerijen. Met camera's wordt het proces op afstand gevolgd. Dergelijke kwekerijen dienen eens in de vier tot vijf dagen door een persoon te worden bezocht. Klimaatbeheersingssystemen worden in toenemende mate bij kwekerijen aangetroffen. Grote kwekerijen hebben er dikwijls meerdere. De prijs voor een apparaat varieert van 2000 tot 6000 euro. Ook wordt steeds vaker apparatuur aangetroffen die het CO_2 -gehalte reguleert. Voordelen van het kweken met CO_2 zijn de verkorte kweektijd en een toename van de oogst met 20 tot 40 procent.

Naast een toename in het gebruik van klimaatbeheersingssystemen en CO_2-apparatuur wordt de kwaliteit van de gebruikte kweeklampen steeds beter. Het betreft lampen die in de professionele tuinderskassen worden gebruikt.

Een laatste ontwikkeling is het gebruik van geurmiddelen. Door het toevoegen van dergelijke middelen wordt de geur van hennep gemaskeerd. Ook kan de geur worden bestreden met ozonapparaten. Ozon is een natuurlijke luchtzuiveraar, zij het niet zonder risico's, want bij langdurige inademing of hoge concentraties is het schadelijk. De afgelopen jaren is sporadisch ozonapparatuur aangetroffen in een kwekerij.

Schoonmaken

We zien steeds vaker dat kwekerijen tussen twee kweekperioden grondig worden schoongemaakt. Sporen van eerdere oogsten worden zo veel mogelijk gewist. Criminelen willen voorkomen dat eerdere oogsten kunnen worden aangetoond, omdat bij een eventuele ontneming het wederrechtelijk verkregen voordeel wordt berekend en eerdere oogsten daarin meetellen. Daarom wassen criminelen de kweekpotten of vervangen ze die door nieuwe potten, plaatsen ze nieuwe doeken om de koolstoffilters en stoffen ze lampen af. Dit duidt op een zekere professionalisering.

Kwaliteit
Door verbeteringen in het kweekproces is de kwaliteit van hennep in veel Europese landen gestegen. Een gevolg hiervan is dat de vraag naar geïmporteerde hennep in een aantal landen is afgenomen. Deze landen zijn in staat zichzelf in grotere mate te voorzien van hennep.

Handelsstromen
De Balkanlanden, met name Albanië, Servië, Bulgarije en Kosovo, produceren hennep waarmee Centraal-, Oost- en Zuidoost-Europa worden voorzien. Via Griekenland wordt de hennep naar Italië, Kroatië, Hongarije, Tsjechië en Oostenrijk gedistribueerd. Er zijn aanwijzingen dat Albanese hennep met een laag THC-gehalte naar Nederland wordt geëxporteerd om hier vervolgens te worden gemengd met sterke hennep.

1.5.3 Huidige gevolgen

Volksgezondheid
Het gebruik van cannabis heeft diverse gezondheidsrisico's tot gevolg. Er is toenemend bewijs dat cannabisgebruik het risico op een latere psychotische stoornis vergroot. Dit risico neemt toe bij een hogere frequentie van gebruik. Van alle nieuwe jaarlijkse gevallen van psychotische stoornissen is tussen de 6 en 10 procent toe te schrijven aan cannabisgebruik. Chronisch en zwaar gebruik van cannabis wordt tevens geassocieerd met andere gezondheidsrisico's. Het verhoogt waarschijnlijk het risico op luchtwegklachten en longkanker. Daarnaast blijkt cannabisgebruik een indicator te zijn voor zwak psychosociaal functioneren. Dit hangt samen met allerlei andere factoren zoals het roken van sigaretten, het gebruik van alcohol of harddrugs, spijbelen, slechte schoolprestaties en schoolverzuim. Hoewel cannabis minder verslavend is dan vele andere soorten drugs, neemt het risico op afhankelijkheid toe bij langdurig frequent gebruik.
De verslavingszorg biedt hulp aan mensen die verslaafd zijn geraakt aan drugs, alcohol, medicijnen, gokken of andere gedragsverslavingen. Het Landelijk Alcohol en Drugs Informatie Systeem (LADIS) bevat geanonimiseerde gegevens over de hulpverlening.[18] Hieruit blijkt dat het aantal cliënten dat ingeschreven stond wegens een primair cannabisprobleem tussen 2005 en 2014 twee keer zo groot is geworden. Sinds 2011 is het aantal primaire cannabiscliënten redelijk stabiel en ligt het aantal op ongeveer 11.000 per jaar. Het aantal cliënten dat cannabis als secundair probleem noemt, schommelt rond de 5300 per jaar.
Het aandeel van cannabis in alle hulpverzoeken met betrekking tot drugsgebruik is tevens toegenomen in de loop der jaren. In 2005 had 17 procent van alle drugsgerelateerde hulpvragen betrekking op cannabis. In 2011 is dit percentage gestegen naar 33 procent. Sindsdien is het vrij stabiel gebleven.

18 De gegevens uit LADIS zijn te vinden in de *Nationale Drug Monitor. Jaarbericht 2015.*

Financieel

Er zijn op verschillende terreinen negatieve financiële consequenties van grootschalige cannabisteelt. Zo ontstaat vaak schade aan de panden waarin een kwekerij gevestigd is. Elk jaar worden zo'n honderd panden geregistreerd die schade oplopen door brand of lekkage. De registratie op dit punt is niet compleet, zodat aangenomen moet worden dat dit een ondergrens vormt. Ook de constructie van een pand kan worden aangetast door de aanleg van leidingen en een klimaatbeheersingssysteem. Deze kunnen ook vocht en roestvorming veroorzaken. Behalve serieuze schade aan gebouwen leveren de branden natuurlijk ook gevaar op voor personen, zowel voor de betrokkenen als voor de bewoners van aangrenzende percelen.

Een andere financiële schadepost betreft energiediefstal. Volgens het Platform Energiediefstal komen jaarlijks meer dan vijfduizend energiediefstallen aan het licht. Het overgrote deel daarvan betreft hennepkwekerijen. In de praktijk blijkt dat in bijna alle hennepplantages sprake is van een gemanipuleerde stroomtoevoer. Naar schatting wordt jaarlijks 1 miljard kilowattuur aan elektriciteit gestolen. Dit is ongeveer gelijk aan het jaarlijks energieverbruik van de huishoudens in een stad als Den Haag. Dit vertegenwoordigt een waarde van bijna 200 miljoen euro.

Ook het bankwezen ondervindt schade ten gevolge van de georganiseerde hennepteelt. Criminelen gebruiken valse gegevens zoals valse werkgeversverklaringen, loonstroken of identiteitsbewijzen om een hypotheek te verkrijgen. En vaak worden de financiële verplichtingen die gepaard gaan met een hypotheek niet nagekomen.

De kosten aan verslavingszorg voor de naar schatting 11.000 primaire cannabiscliënten lopen in de tientallen miljoenen euro's per jaar.

Geweld

Uit onderzoek van het EMCDDA[19] en Europol blijkt dat het gebruik van (extreem) geweld in de cannabissector de afgelopen drie jaar toeneemt, zowel binnen criminele organisaties als tussen criminele organisaties.

In de periode 2013 tot en met 2015 hebben in totaal 85 liquidaties plaatsgevonden en 13 pogingen daartoe. In tien gevallen is vermoedelijk sprake geweest van een conflict in relatie tot cannabiscriminaliteit. Het ging om vijf geslaagde liquidaties in 2013 en vijf in 2014. Naast het aantal aangetroffen doden ten gevolge van een liquidatie bestaat het vermoeden dat enkele vermiste personen geliquideerd zijn vanwege een conflict in de cannabisindustrie. De hieraan ten grondslag liggende conflicten kennen hun oorsprong meestal in gemiste inkomsten uit partijen verdovende middelen die zijn gript door concurrenten of in beslag zijn genomen door officiële instanties. De liquidaties of pogingen daartoe vinden in toenemende mate plaats in de openbare ruimte.

19 *EMCDDA* staat voor het European Monitoring Centre for Drugs and Drug Addiction.

Ondermijning
De productie en smokkel van cannabis en de handel daarin kunnen op diverse manieren leiden tot ondermijning van de Nederlandse samenleving. Zo vinden gevallen van beïnvloeding van de rechtsorde en het openbaar bestuur plaats. Voorbeelden hiervan zijn politiefunctionarissen die tegen betaling informatie doorspelen aan criminelen of gemeenteambtenaren die onterecht vergunningen verlenen. Ook trachten criminelen invloed uit te oefenen door het intimideren dan wel bedreigen van personen. Zo is sprake geweest van een opzettelijke brandstichting in een stadhuis, werden burgemeesters bedreigd en bedrijfsbusjes van energieleveranciers vernield. Er zijn situaties bekend geworden waarin criminelen uit de hennepbranche trachtten toe te treden tot de lokale politiek.

Economische verhoudingen kunnen verstoord worden door investeringen van crimineel geld in bedrijven. Bedrijven die op een legale manier werken, kunnen niet meer concurreren met bedrijven waarbij (tevens) sprake is van een illegale bedrijfsvoering. Doordat crimineel geld in deze bedrijven wordt geïnvesteerd, hoeven deze bedrijven niet op legale wijze winst te maken om te bestaan. Om de integriteit van vergunningaanvragers te beoordelen, wordt de Wet Bibob[20] toegepast. Op basis van deze wet kan een aanvraag voor een bepaalde vergunning geweigerd of een reeds afgegeven vergunning ingetrokken worden. In de praktijk blijkt dat criminelen de beoordeling van hun integriteit omzeilen door gebruik te maken van katvangers zonder antecedenten.

Een veelvoorkomende vorm van ondermijning is de verweving van onder- en bovenwereld. Deze verweving manifesteert zich vooral door gebruik van faciliteerders. Gedurende het gehele logistieke proces van hennepteelt en -handel worden dergelijke personen ingeschakeld. Het verwerven van panden, het aanleveren van kweekmateriaal, het inrichten van kweeklocaties en transport behoren tot die diensten. Hierbij kunnen onder andere makelaars, verhuurbemiddelaars, notarissen, voormalige growshops, advocaten, accountants en elektriciens worden ingezet. Doordat de faciliteerders zowel in de onder- als in de bovenwereld opereren, ontstaat verweving tussen beide werelden. Dit doet zich tevens voor bij het gebruik van dekmantelbedrijven. Deze worden gebruikt om criminele activiteiten af te schermen. Via dekmantelbedrijven worden bijvoorbeeld goederen voor het kweekproces aangeschaft. Daarnaast zijn voorbeelden bekend van bedrijven die opgericht werden om de persoons- en vervoersbewegingen rondom een pand waar een kwekerij is gevestigd aannemelijk te maken voor de omgeving. Transport- en garagebedrijven worden dikwijls gebruikt voor het transport van softdrugs. Voor de buitenwereld lijkt in deze bedrijven sprake te zijn van legale bedrijvigheid. In werkelijkheid houden zij zich echter bezig met het uitvoeren of ondersteunen van cannabisgerelateerde vormen van criminaliteit.
Behalve als afscherming van criminele activiteiten worden dekmantelbedrijven gebruikt om illegale opbrengsten wit te wassen. Een bekende manier is het mengen van crimineel geld met de inkomsten uit reguliere bedrijfsvoering.

20 Wet bevordering integriteitsbeoordelingen door het openbaar bestuur.

Cannabisgebruik lijkt door een groot gedeelte van de bevolking geaccepteerd te worden. Uit onderzoek van het Trimbos-instituut blijkt dat ongeveer 2,7 miljoen Nederlanders ooit cannabis gebruikt hebben. De morele acceptatie onder een aanzienlijk gedeelte van de bevolking in combinatie met de relatief lage prijs en de eenvoudige verkrijgbaarheid van cannabis laat zien dat de drempel om tot gebruik over te gaan laag is.
Toetreden tot de hennepteelt is voor een grote groep mensen verleidelijk. Betrokkenheid wordt in sommige wijken normaal gevonden en gerechtvaardigd, de opbrengsten zijn lucratief en de pakkans is klein. Daarnaast biedt de hennepteelt werk aan een groot aantal mensen. Gesteld kan worden dat een grote groep mensen veel geld verdient met de productie van en handel in hennep.

1.5.4 Verwachtingen

In de navolgende passages zullen enkele verwachtingen uitgesproken worden omtrent een aantal aspecten van cannabisteelt, -handel en -gebruik. Ook worden de verwachte gevolgen voor de periode 2017-2021 besproken.

Procesbeheersing
Het volledige kweekproces kan vrijwel geheel geautomatiseerd plaatsvinden. Er wordt in toenemende mate gebruikgemaakt van technische hulpmiddelen, waaronder klimaatbeheersingssystemen. Hierdoor wordt het aantal betrokken personen beperkt en wordt het aantal persoonsbewegingen rondom een kwekerij verminderd. De kans dat opsporingsdiensten een kwekerij ontmantelen of dat concurrerende partijen deze rippen, wordt daardoor kleiner. De apparatuur is eenvoudig verkrijgbaar. De verwachting is dat de toepassing van dit soort technologieën verder zal toenemen.

Rol van het internet
Internet speelt in toenemende mate een rol binnen de hennepteelt en -handel. Het verbod in 2015 op de handel in kweekbenodigdheden voor de hennepteelt via growshops heeft de rol van internet vergroot. Kennis en kweekbenodigdheden kunnen via internet worden verkregen. Ook de verkoop van het eindproduct vindt steeds meer plaats via internet. Dat biedt een virtuele locatie die voor eenieder toegankelijk is. De drempel voor de aanschaf van cannabis wordt hierdoor waarschijnlijk verlaagd. Daarnaast biedt de verkoop van cannabis via internet ruimte voor een ander type dealer. Er is weinig zicht op wat zich op internet afspeelt. Het is daarmee een relatief veilige handelsplaats voor criminelen.

Elektriciteit
Cannabisplantages gebruiken veel elektriciteit, die over het algemeen gestolen wordt. Netbeheerders hebben inmiddels de slimme meter geïntroduceerd. De komst van de slimme meter kan van invloed zijn op de manier waarop manipulatie van de stroomtoevoer plaatsvindt. Het manipuleren van een slimme meter is lastiger dan het manipuleren van een traditionele meter. Het is daarom goed voorstelbaar dat in de toekomst vaker aftakkingen voor de meter worden aangebracht, in plaats van dat de meter zelf wordt gemanipuleerd.

Hierdoor heeft het afsluiten van de hoofdzekering geen effect op de stroomvoorziening in het pand. Bij brand kan door het bluswater kortsluiting ontstaan, die de nodige risico's met zich meebrengt voor de brandweer.

Kweken in het buitenland
Het kweken van hennep door Nederlanders in het buitenland is geen nieuw fenomeen en zal zich de komende jaren in toenemende mate blijven voordoen. Daardoor zal het afzetgebied voor Nederlandse hennephandelaars kleiner worden en de Nederlandse export op lange termijn vermoedelijk afnemen. Hierdoor kan de concurrentie op de Nederlandse markt toenemen. Dit kan versterkend werken op de trend dat Nederlandse henneptelers en -handelaars hun activiteiten naar het buitenland verplaatsen. Daarnaast zijn er andere argumenten die het kweken van hennep in het buitenland voor Nederlandse telers aantrekkelijk maken. Het aldaar gehanteerde handhavingsbeleid, de eenvoud om een geschikte locatie te vinden en het kunnen opereren in anonimiteit zijn daar voorbeelden van. De verwachting is dat het kweken in het buitenland en het exploiteren van kennis en materialen door Nederlandse henneptelers de komende jaren nog verder toenemen.

Export van in Nederland geteelde hennep
Zowel in de criminaliteitsbeeldanalyse van 2009 als in die van 2012 wordt de verwachting geschetst dat de export van in Nederland geteelde hennep afneemt. De omvang van de export is zeer lastig te kwantificeren. Zoals beschreven, kennen de schattingen dusdanig ruime marges dat het niet goed mogelijk is de getalsmatige ontwikkeling van de export te bepalen. Kwalitatieve gegevens wijzen echter op een daling van de hennepexport in de komende jaren. Door toename van de productie en verbeterde kweekmethoden in het buitenland zijn de kwantiteit en kwaliteit van buitenlandse hennep gestegen. Volgens het EMCDDA en Europol is het THC-gehalte van in het buitenland geteelde hennep toegenomen. Hierdoor is het kwaliteitsverschil tussen in Nederland geteelde hennep en in het buitenland geteelde hennep verkleind. Europese landen zijn steeds beter in staat in hun eigen hennepbehoeften te voorzien. Hierdoor zal de vraag naar in Nederland geteelde hennep verminderen. Welke consequenties dit heeft voor de Nederlandse productie is onduidelijk. Vooralsnog zijn er geen aanwijzingen dat de binnenlandse productie is afgenomen.

Migrantenstromen
Onder de migranten vormen illegalen een kwetsbare groep. Ze zijn de Nederlandse taal niet machtig, beschikken dikwijls niet over hun paspoort en zijn financieel afhankelijk van anderen. Van deze kwetsbaarheid wordt gebruikgemaakt. Zo zijn bij de ingang van asielzoekerscentra vluchtelingen geronseld om activiteiten in de hennepteelt uit te voeren. Door de omvangrijke migrantenstromen mag aangenomen worden dat deze kwetsbare groep in toenemende mate het slachtoffer zal worden van dergelijke praktijken.

Wetgeving en beleid

Er is een tweetal min of meer recente ontwikkelingen op het gebied van wet- en regelgeving dat mogelijk effect zal hebben op de hennepteelt.

In de eerste plaats heeft een aanscherping plaatsgevonden van de zorgplicht van verhuurders. In het kader van goed verhuurderschap moet onder meer de identiteit van de huurder worden vastgesteld. Daarnaast mogen geen contante betalingen van de huur geaccepteerd worden. Ook moeten voldoende gegevens van de huurder bekend zijn, zodat in het geval van een calamiteit contact kan worden opgenomen. In sommige gevallen is tevens fysieke controle van een pand vereist. Hierdoor wordt het malafide huurders lastiger gemaakt om een pand te verkrijgen voor het uitvoeren van criminele activiteiten.

Een tweede ontwikkeling is het eerdergenoemde in werking treden van artikel 11a van de Opiumwet op 1 maart 2015. Met behulp van dit artikel kan worden opgetreden tegen faciliteerders van illegale hennepteelt, omdat voorbereidingshandelingen hiertoe strafbaar worden gesteld. Dit artikel treft vooral de growshops.

Het is nog te vroeg om aan te kunnen geven in hoeverre deze relatief nieuwe regels effect hebben gehad. Wellicht dat die effecten in de voor ons liggende periode zichtbaar worden.

Gebruik

Het ontbreekt ons aan overtuigende indicatoren die iets kunnen zeggen over het gebruik van cannabis in de voor ons liggende jaren. Er is wel een maatschappelijke en politieke discussie gaande over het reguleren of legaliseren van cannabisteelt, -verkoop en -gebruik. Deze discussie concentreert zich op de gevolgen van grootschalige hennepteelt en de discrepantie tussen het zogeheten voordeur- en achterdeurbeleid, ook wel het gedoogbeleid genoemd. De verkoop van cannabis is illegaal, maar wordt onder strenge voorwaarden gedoogd. Bedrijfsmatige teelt van en handel in cannabis wordt niet gedoogd, maar actief bestreden. Hier toont zich de paradox die geleid heeft tot de hierboven genoemde discussie, want hoe komen de verkooppunten aan hun handelsvoorraad? Zij zijn aangewezen op bevoorrading uit illegale bron. De uitkomst van de discussie is ongewis. Er zijn vele beleidsvarianten denkbaar tussen strafbaar stellen en legaliseren. Al die varianten zullen hun eigen gevolgen hebben voor de beschikbaarheid van en toegang tot cannabisproducten; die beschikbaarheid en toegang op hun beurt bepalen in ieder geval deels het gebruiksniveau. Hoe groter de beschikbaarheid, hoe meer gebruik.

Verwachte gevolgen

Over het algemeen zullen de gevolgen in de periode die voor ons ligt dezelfde zijn als in de periode die achter ons ligt. Die gevolgen liggen op het gebied van volksgezondheid, financiën, geweld en ondermijning.

Hierboven werden enkele verwachtingen uitgesproken die mogelijk van invloed zijn op de eerder beschreven gevolgen. Zo wordt verwacht dat de export van cannabis zal verminderen. Hoewel er geen precieze kwantitatieve gegevens voorhanden zijn, kan dit leiden tot een vermindering van de Nederlandse productie. Indien dit effect substantieel is, kan ook op andere gebieden, zoals energiediefstal, hypotheekfraude en schade aan gebouwen, een

daling optreden. De verwachting van exportvermindering wordt al een aantal jaren achtereen uitgesproken en tot nu toe zijn er geen aanwijzingen dat deze ook feitelijk tot een lagere productie heeft geleid.
De verkoop van cannabis via internet zal de drempel om te gaan gebruiken verlagen. Ook worden bij verkoop via internet de strenge voorwaarden die voor coffeeshops gelden (zoals de leeftijdsgrens, verbod op reclame-uitingen, ingezetenencriterium) ontdoken.
Het gebruik van klimaatbeheersingssystemen kan een bacteriologische besmetting van het water veroorzaken, doordat deze apparaten rechtstreeks op zowel de drinkwaterleiding als het riool worden aangesloten. Steeds vaker wordt het gebruik van dergelijke systemen geconstateerd, waardoor de kans op een bacteriologische besmetting van het drinkwater toeneemt. Zo'n besmetting kan een groot gevaar opleveren voor de volksgezondheid.
Door het gebruik van opticlimates wordt vermoedelijk steeds vaker de watertoevoer gemanipuleerd door het omkeren of verwijderen van de watermeter. Dit kan leiden tot vervuild water, omdat de kans bestaat dat vervuild water terug het leidingnet in stroomt. Door een toenemende professionalisering van de inrichting van hennepkwekerijen stijgt de kans op een besmetting van het water.
Het gebruik van ozon als geurmaskeerder heeft negatieve gezondheidseffecten vanwege zijn sterk oxiderende chemische eigenschappen. Blootstelling aan ozon kan direct leiden tot ademhalingsproblemen. Herhaalde en langdurige blootstelling kan leiden tot onherstelbare longschade.
Een laatste ontwikkeling met betrekking tot de gezondheidsrisico's vormt het THC-gehalte. Een toename van het THC-gehalte kan leiden tot meer gezondheidsproblemen, terwijl een afname de gezondheidsproblemen kan verminderen. Het percentage THC is vermoedelijk (mede) afhankelijk van het al dan niet plaatsen van cannabis met een THC-gehalte van 15 procent of hoger op lijst I van de Opiumwet. Er ligt een voorstel voor wetswijziging in het parlement, maar onbekend is of en wanneer dit voorstel aangenomen zal worden.

1.5.5 Kwalificatie van dreiging

De productie van, handel in en smokkel van cannabis gaat samen met een omvangrijke combinatie van negatieve gevolgen. Die variëren van gevaren voor de volksgezondheid en financiële schade van enkele honderden miljoenen euro's per jaar tot geweldgebruik. Bovendien zien we verschillende vormen van ondermijning: verwevenheid van de bovenmet de onderwereld en bedreiging en intimidatie van bestuurders. Ook zijn er geluiden dat met name in het zuiden van het land in sommige steden 'vrijplaatsen' zijn ontstaan waar criminelen een 'onaantastbare' en 'respectabele' status hebben verkregen. Hoewel er toekomstige ontwikkelingen in de hennepbranche op het gebied van professionalisering en automatisering te verwachten zijn, zullen zich de komende vier jaar geen grote wijzigingen voordoen. De gevolgen van de hennepteelt zullen in de periode 2017-2021 daarom ongeveer vergelijkbaar zijn met die in de periode 2012-2017. Voor de komende vier jaar wordt de hennepteelt als een **dreiging** voor de Nederlandse samenleving bestempeld.

1.6 Seksuele uitbuiting

1.6.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Mensenhandel, seksuele uitbuiting. Nationaal dreigingsbeeld 2017*. De auteurs zijn Jessica de Jong, Sandra ter Woerds, Joanne Valk en Lieke Galama, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017*.
Aan het eind van deze paragraaf wordt de kwalificatie van dreiging beschreven. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is beargumenteerd en vastgesteld in een andere context door een groep van beoordelaars (de consensusgroep).

Onder seksuele uitbuiting vallen zowel uitbuiting in de prostitutie als uitbuiting bij andere vormen van seksuele dienstverlening zoals webcamseks. Het zich beschikbaar stellen voor het verrichten van seksuele handelingen tegen betaling door derden is voor volwassenen in Nederland niet strafbaar gesteld. Het wordt strafbaar op het moment dat er sprake is van seksuele uitbuiting en/of dat deze handelingen worden verricht door minderjarigen.

1.6.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

De vraag hoe de omvang van seksuele uitbuiting zich in Nederland heeft ontwikkeld is, evenals vier jaar geleden, moeilijk te beantwoorden. Gevallen van seksuele uitbuiting vinden heimelijk plaats of hebben de schijn van legaliteit, waardoor deze vaak verborgen blijven voor de autoriteiten. Slachtoffers willen of durven zich niet bekend te maken of realiseren zich niet dat zij slachtoffer zijn. Bij buitenlandse slachtoffers kan sprake zijn van een taalprobleem, gebrek aan kennis waar ze terecht kunnen en wantrouwen richting de politie, veroorzaakt door ervaringen in eigen land en angst om Nederland te worden uitgezet. Daardoor is de aangiftebereidheid laag. Dit betekent dat met behulp van registraties maar een beperkt deel van de problematiek in beeld kan worden gebracht.

In Nederland is het Coördinatiecentrum tegen Mensenhandel (CoMensha) belast met de landelijke registratie van het aantal aanmeldingen van mogelijke slachtoffers van mensenhandel, waaronder ook seksuele uitbuiting. CoMensha spreekt bewust van ‘mogelijke’ slachtoffers, omdat niet van alle aangemelde personen is vast te stellen of zij ook daadwerkelijk slachtoffer zijn. De politie is de grootste melder. Ook niet-meldingsplichtige instellingen zoals hulpverlenings-, opvang-, vluchtelingen- en asielorganisaties, regiocoördinatoren, de advocatuur, particulieren en cliënten kunnen mogelijke slachtoffers aanmelden. Tabel 3 geeft een overzicht van deze mogelijke slachtoffers naar nationaliteit voor de jaren 2011-2014.[21]

21 De cijfers in tabel 3 hebben betrekking op slachtoffers van mensenhandel in het algemeen, niet enkel seksuele uitbuiting. 64-71 procent wordt uitgebuit in de seksindustrie.

Tabel 3. Meest voorkomende nationaliteiten van mogelijke slachtoffers mensenhandel[22]

2011		2012		2013		2014	
Nederland	337	Nederland	428	Nederland	455	Nederland	468
Nigeria	134	Bulgarije	303	Roemenië	193	Roemenië	216
Hongarije	121	Hongarije	217	Hongarije	172	Bulgarije	154
Polen	104	Roemenië	129	Bulgarije	123	Polen	99
Bulgarije	73	Nigeria	95	Nigeria	54	Hongarije	96
Sierra Leone	62	Polen	67	Guinee	51	Filipijnen	75
Guinee	58	Sierra Leone	60	Sierra Leone	33	Nigeria	42
China/Roemenië	80	Guinee	47	China	31	Guinee	35
Angola	19	Macedonië	27	Polen	22	Eritrea	32
Oeganda	14	Filipijnen	14	Filipijnen	16	Sierra Leone	22

Bron: CoMensha, Jaarverslagen 2011-2014

Er is vooral een toename van het aantal mogelijke slachtoffers uit Roemenië en een afname van het aantal mogelijke slachtoffers uit West-Afrika en China. Het aantal bij CoMensha aangemelde mogelijke slachtoffers van seksuele uitbuiting is sinds het vorige dreigingsbeeld verder toegenomen, van 782 in 2011 naar 1109 in 2014. De stijging van het aantal aanmeldingen hoeft niet te betekenen dat de omvang van seksuele uitbuiting is toegenomen, maar duidt erop dat bij de betrokken organisaties steeds meer mogelijke slachtoffers in beeld zijn gekomen en/of bij CoMensha worden gemeld.
Het aantal slachtoffers dat ten tijde van aanmelding bij CoMensha minderjarig is, is gelijk gebleven, maar CoMensha vermoedt dat een groot deel van de minderjarigen niet bij hen wordt gemeld. Experts geven aan dat in de praktijk een toename van minderjarige slachtoffers van seksuele uitbuiting wordt gesignaleerd. Dat hangt samen met de toegenomen aandacht voor deze kwetsbare groep en de aandacht voor de onvergunde branche, waar zij veelal werkzaam zijn. Ook de uitgebreide media-aandacht in 2014 en 2015 voor de Valkenburgse en de Schiedamse zedenzaak heeft geleid tot meer aandacht voor en daarmee meer zicht op minderjarige slachtoffers. In beide zaken werd een minderjarig meisje seksueel uitgebuit. Het Openbaar Ministerie heeft naar aanleiding van deze zaken actief ingezet op het vervolgen van klanten die zich schuldig maken aan seks tegen betaling met minderjarigen. Alleen al in de eerste helft van 2015 werden meer zaken (90) ingeschreven dan in de voorgaande veertien jaar tezamen (87).

Evenals vier jaar geleden is het overgrote deel van de verdachten van het mannelijk geslacht. Er is een kleine toename van het aantal verdachten van seksuele uitbuiting dat in Nederland is geboren, van 27 naar 34 procent. Het gaat bij deze verdachten vooral om Nederlandse mannen met een migratie-achtergrond: mannen met een Turkse, Marokkaanse of Antilliaanse herkomst.

22 Op het moment van schrijven (mei 2016) is het Jaarverslag 2015 nog niet verschenen, de publicatie wordt in juli 2016 verwacht. Desgevraagd geeft een medewerker van CoMensha aan dat de meest voorkomende nationaliteiten in 2015 “niet heel erg” afwijken van die in de voorgaande jaren.

Wel is de laatste jaren sprake van een groter aandeel vrouwelijke verdachten. Deze toename is mogelijk te verklaren doordat er in de opsporing meer aandacht is gekomen voor de dienstverlenende rollen die ook door vrouwen worden vervuld, zoals het regelen van de reis naar het buitenland of het tegen betaling beschikbaar stellen van een woning voor prostitutiewerkzaamheden. De vrouwen zijn vrijwel altijd de partner of zus van een van de verdachten of zijn zelf werkzaam (geweest) als prostituee of op andere wijze bekend met de prostitutiewereld. Soms zijn ze ook zelf slachtoffer (geweest) van seksuele uitbuiting. Daarnaast is in de opsporing meer aandacht gekomen voor tussenpersonen die (on)bewust bij het mensenhandelproces betrokken zijn en hand-en-spandiensten verlenen, bijvoorbeeld op het gebied van huisvesting en documenten. Dit kan zowel legale organisaties betreffen (criminele uitbesteding) als personen die zich binnen het netwerk van de verdachten bevinden.
Het gemiddeld aantal verdachten per opsporingsonderzoek en het percentage onderzoeken waarbij de opsporingsinstanties zicht hebben op een crimineel samenwerkingsverband is de afgelopen jaren gelijk gebleven. Volgens onderzoek van de Nationaal Rapporteur Mensenhandel is in ruim 37 procent van de onderzoeken sprake van een crimineel samenwerkingsverband. Van de meeste samenwerkingsverbanden (69%) is het aantal leden bekend, met een gemiddelde van 5,5. Bij twee derde van de samenwerkingsverbanden hebben de leden overwegend dezelfde nationaliteit. Veelal zijn het Nederlandse, Hongaarse of Bulgaarse samenwerkingsverbanden. Bij de Nederlandse samenwerkingsverbanden gaat het bij de helft van de criminele samenwerkingsverbanden om Nederlanders met een Marokkaanse of Turkse herkomst. De leden van de samenwerkingsverbanden zijn meestal op informele wijze aan elkaar gerelateerd, op basis van een familiale of vriendschappelijke relatie dan wel een partnerrelatie.
Experts vermoeden dat bij seksuele uitbuiting met Nederlandse slachtoffers over het algemeen minder georganiseerd te werk wordt gegaan dan bij seksuele uitbuiting met buitenlandse, vooral Midden- en Oost-Europese, slachtoffers. Dit vermoeden lijkt te worden bevestigd vanuit het dossieronderzoek dat ten behoeve van dit dreigingsbeeld is uitgevoerd. Bij seksuele uitbuiting van buitenlandse slachtoffers in Nederland is, evenals vier jaar geleden, vaak sprake van etnische en/of culturele verwantschap tussen daders en slachtoffers.

Aard

Het barrièremodel voor mensenhandel maakt de werkwijze van mensenhandelaars inzichtelijk en bevat de volgende elementen: rekrutering, entree en documenten, huisvesting, arbeid, binding, financiën en afscherming.

Het *rekruteren* van binnenlandse en buitenlandse slachtoffers vindt in toenemende mate plaats via internet en sociale media. Dit is een trend die al in eerdere dreigingsbeelden is gesignaleerd en die zich de afgelopen jaren verder heeft doorgezet. Via internet en sociale media wordt sneller een vertrouwensband opgebouwd dan via fysieke ontmoetingsplaatsen.

Het selecteren van slachtoffers via internet wordt *hawking* genoemd. Mensenhandelaars zoeken slachtoffers op sociale media en gangbare jongerensites met een chatfunctionaliteit. Als ze mogelijke slachtoffers gevonden hebben, volgt het inpalmen en inlijven.
Uit het dossieronderzoek blijkt dat verdachten meer dan voorheen seksueel getinte foto's of filmpjes van de slachtoffers maken of hun deze ontfutselen en daar de slachtoffers mee chanteren (*sexting*). Volgens de verwachting van vier jaar geleden ziet een aantal experts in de aangiften en verklaringen van (mogelijke) slachtoffers van seksuele uitbuiting dat minder vaak (zichtbaar) fysiek en excessief geweld wordt gebruikt om vrouwen te dwingen in de prostitutie te gaan werken; ronselaars hebben een voorkeur voor misleiding. Daartegenover staan de bevindingen dat er een verharding in de ronseltechnieken bij bepaalde verdachten, vooral (jonge) Nederlandse verdachten, is waargenomen, waarbij meisjes met geweld en drugs worden geronseld. Experts wijzen overigens op een mogelijk groot *dark number* voor wat betreft de daadwerkelijke geweldsomvang.

Sinds de toetreding van Hongarije, Bulgarije en Roemenië tot de Europese Unie is de *entree* voor slachtoffers uit deze landen eenvoudiger geworden. Om in Nederland in de prostitutie te mogen werken zijn *documenten* nodig, waaronder een basisregistratie personen en een inschrijving bij de Kamer van Koophandel. Vrouwen uit Bulgarije, Roemenië en Hongarije kunnen deze documenten nu zelf aanvragen met hun eigen identiteitspapieren. Toch komt vervalsing van (verblijfs)documenten onder Midden- en Oost-Europese slachtoffers nog steeds voor, bijvoorbeeld om minderjarigheid van het slachtoffer te verhullen of om te frauderen met belastingen.
Daarnaast is er sprake van een groeiend aantal migranten, asielzoekers en vluchtelingen afkomstig van buiten de Europese Unie die kwetsbaar zijn voor mensensmokkel en mensenhandel. Digitale middelen bieden in toenemende mate aan daders van mensenhandel mogelijkheden om op afstand controle uit te oefenen. Zo reizen buitenlandse slachtoffers ook wel zonder begeleiding en zijn mensenhandelaars niet altijd fysiek aanwezig in prostitutiegebieden.

Mobiliteit en vluchtigheid zijn kenmerkend voor *huisvesting* en *arbeid* van slachtoffers. Hier is sprake van een trend die zich verder heeft doorgezet sinds het vorige dreigingsbeeld. Slachtoffers worden sneller van de ene werklocatie naar de andere verplaatst, waardoor de periode van uitbuiting op iedere locatie korter is geworden. Er is een verschuiving opgetreden van huren via kamerbedrijven binnen de seksindustrie naar het huren van ruimten via vastgoedbedrijven of makelaars.
Een nieuw inzicht is dat bij mensenhandel met buitenlandse (Midden- en Oost-Europese) slachtoffers veelal sprake is van uitbuiting in de raamprostitutie, terwijl mensenhandel met Nederlandse slachtoffers doorgaans plaatsvindt in de thuisprostitutie, in clubs en in de escort. Het is niet duidelijk of hier sprake is van een nieuwe ontwikkeling, aangezien het vorige dreigingsbeeld zich enkel op buitenlandse slachtoffers heeft gericht die in Nederland zijn uitgebuit in de prostitutiebranche.

Mensenhandelaars maken misbruik van de economische, psychische of sociale kwetsbaarheid van slachtoffers om deze aan zich te *binden*. Daarbij wordt ook gebruikgemaakt van misleiding en geweld. Evenals vier jaar geleden blijkt dat slachtoffers van seksuele uitbuiting vaak niet zelfstandig invulling mogen geven aan de wijze waarop ze hun werkzaamheden uitvoeren en mogen ze klanten niet weigeren. De mensenhandelaars kiezen en regelen de werkplek en bepalen de werktijden. Uit de bestudeerde dossiers blijkt dat slachtoffers lange dagen (tussen de 12 en 19 uur) en lange weken maken. Ze moeten ook werken als ze moe, ongesteld of ziek zijn. De mensenhandelaars werven de klanten vaak via advertenties op internet of via hun eigen sociale netwerk (vrienden). Experts signaleren dat in advertenties waarin seksuele diensten worden aangeboden vaker dan voorheen een 24 uursbeschikbaarheid wordt vermeld. Daarnaast worden steeds extremere vormen van seksuele dienstverlening en onbeschermde seks aangeboden en prijzen worden verlaagd om meer klanten te werven.
Verder signaleren experts een verharding onder bepaalde groepen daders en een vergroting van kwetsbaarheid onder (Nederlandse) slachtoffers. Er worden in de praktijk meer minderjarige slachtoffers van seksuele uitbuiting gesignaleerd en een groeiend aantal slachtoffers heeft een licht verstandelijke beperking en is afkomstig uit een zorg- of jeugdinstelling, zoals ook naar voren komt uit het dossieronderzoek.

Geld dat met seksuele uitbuiting wordt verdiend, wordt vaker cash verplaatst in plaats van via banktransfers. Dat is een trend die ook in het vorige dreigingsbeeld is gesignaleerd. Daadwerkelijk zicht op de geldstromen naar het buitenland en op witwasconstructies ontbreekt. De herkomst van crimineel verkregen geld wordt vaker versluierd. Er wordt 'slimmer geïnvesteerd' door zaken op naam van anderen te zetten en een dubbele boekhouding bij te houden, waardoor het steeds moeilijker is om te bewijzen dat er sprake is van witwassen. Er is een afname van het aantal (waargenomen) verdachte financiële transacties met betrekking tot mensenhandel, terwijl de transacties die wel (zichtbaar) hebben plaatsgevonden hogere geldbedragen betreffen.

Verdachten hanteren verschillende methoden om seksuele uitbuiting *af te schermen* van de buitenwereld om op die manier 'onder de radar' te blijven van opsporingsinstanties. Uit de dossiers blijkt dat minder geavanceerde methoden, zoals het wisselen van telefoons of het gebruik van prepaidtelefoons, nog steeds veelgebruikte manieren zijn. Van slachtoffers wordt regelmatig hun telefoon afgenomen of deze wordt afgesloten. De maatschappelijke ontwikkeling waarbij telefonische communicatiekanalen plaatsmaken voor digitale kanalen is ook terug te zien in het veelvuldig gebruik van sociale media door verdachten en slachtoffers van seksuele uitbuiting. Het werken in de illegale onvergunde prostitutie is ook een vorm van afscherming. Slachtoffers kunnen in de onvergunde branche makkelijker worden onttrokken aan controles, wat het risico op uitbuiting vergroot. Een andere vorm van afscherming die de afgelopen jaren is toegenomen, is de grote mate van mobiliteit: het eerdergenoemde sneller dan voorheen wisselen van de ene naar de andere werk- en woonlocatie, waarmee de periode van uitbuiting op een bepaalde locatie korter is geworden.

1.6.3 Huidige gevolgen

Mensenhandel trekt een zware wissel op de gezondheid van slachtoffers. De uitbuiting in de prostitutie veroorzaakt bij vrijwel elk slachtoffer psychische schade. Honderden slachtoffers ondervinden lichamelijke schade, doordat ze te maken krijgen met (zware) mishandeling, het gedwongen afbreken van zwangerschap, seksueel overdraagbare ziekten, onthouding van medische zorg, gedwongen drugsgebruik en voedseltekort.

In 2015 zijn er door de politie ruim zevenhonderd meldingen van 'overlast van prostitutie' geregistreerd. Op basis hiervan kan slechts een ruwe schatting worden gedaan van de mate van overlast van seksuele uitbuiting voor individuen en bedrijven: het gaat jaarlijks waarschijnlijk om honderden individuen en tientallen bedrijven.

Financiële schade is er voor personen, bedrijven en de overheid. Naar schatting lopen alleen al de geregistreerde slachtoffers jaarlijks tientallen miljoenen euro's mis aan afgestane inkomsten. Op internationaal niveau wordt geschat dat ieder slachtoffer van seksuele uitbuiting circa 21.800 euro per jaar opbrengt. Met een vraagteken bij de betrouwbaarheid van deze schatting (voor Nederland) en uitgaande van de situatie dat alle bij CoMensha aangemelde mogelijke slachtoffers van seksuele uitbuiting in 2014 hun volledige inkomsten hebben afgestaan, bedraagt de minimale schade voor dat jaar 24 miljoen euro. We spreken hier over minimale schade, omdat volgens de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen het werkelijke aantal slachtoffers van mensenhandel een veelvoud zou kunnen zijn van het aantal zichtbare slachtoffers. Slachtoffers hebben vaak ook auto's en telefoons op naam staan. Schulden en overtredingen (boetes) die door anderen zijn gemaakt, worden op hen verhaald. Naar aanleiding van misstanden zijn de laatste jaren regelmatig legale seksinrichtingen en hotels waar seksuele uitbuiting heeft plaatsgevonden gesloten. Het aantal legale seksbedrijven is afgenomen en in de vergunde branche is sprake van een dalende omzet. Exploitanten van seksinrichtingen klagen over 'broodroof' als gevolg van de concurrentie vanuit de onvergunde prostitutie waar een groeiend aantal prostituees aan het werk gaat.
De financiële schade voor de overheid komt voort uit gemiste belastinginkomsten, ten onrechte uitgegeven uitkeringen aan Nederlandse mensenhandelaars die nauwelijks of geen legaal inkomen opgeven en uitkeringen en schadevergoedingen aan slachtoffers. Uitgaande van bovenstaande bedraagt de totale schade voor de overheid naar verwachting tientallen miljoenen euro's.
Verweving van onder- en bovenwereld manifesteert zich in de betrokkenheid van legale seksbedrijven en financiële dienstverleners bij seksuele uitbuiting. Experts spreken over tolerantie ten aanzien van het bestaan van prostitutie, waardoor de alertheid op misstanden zou kunnen afnemen.

1.6.4 Verwachtingen

De te verwachten ontwikkelingen omtrent seksuele uitbuiting zijn in sterke mate afhankelijk van de mate van toezicht op de prostitutiebranche. De Nationaal Rapporteur maakt zich ernstig zorgen over de verminderde inzet op mensenhandel door de politie, waar door ontwikkelingen zoals de vluchtelingenstroom en de dreiging van terrorisme een verschuiving in prioriteitstelling heeft plaatsgevonden. Als gevolg van die verminderde inzet wordt een verdere daling verwacht van het aantal verdachten en aangemelde mogelijke slachtoffers van seksuele uitbuiting. Dit alles gaat samen met het minder worden van de informatiepositie van de politie en het verlies van expertise binnen de politie, terwijl juist gezien de toestroom van de kwetsbare groep vluchtelingen het risico op uitbuiting toeneemt. De politiek heeft dit signaal opgepakt en eind 2016 extra middelen beschikbaar gesteld om de aanpak van mensenhandel de komende jaren te intensiveren.

De in de praktijk gesignaleerde toename van (aandacht voor) minderjarige slachtoffers zal naar verwachting doorzetten. Hier worden door experts verschillende redenen voor gegeven. Ten eerste zien zij een veranderende seksuele moraal en het toenemende seksueel overschrijdende gedrag op internet en sociale media bij de jeugd, wat chantagemogelijkheden met zich meebrengt. Ten tweede de verhoging van de minimumleeftijd van 18 naar 21 jaar om als prostituee werkzaam te mogen zijn, zoals voorgesteld in het Wetsvoorstel regulering prostitutie en bestrijding misstanden seksbranche (Wrp) dat is aangemeld voor plenaire behandeling in de Tweede Kamer. Als dit wetsvoorstel wordt aangenomen, wordt gezien de gemiddelde leeftijd van slachtoffers (18,3 voor Nederlandse en 21,1 voor Midden- en Oost-Europese slachtoffers) een toename van slachtofferschap van vrouwen onder de 21 jaar verwacht, omdat deze groep mogelijk naar het illegale circuit zal uitwijken, waar het risico op uitbuiting groter is. Er zijn al signalen dat er vervalste identiteitsdocumenten zullen worden gebruikt om de verhoogde leeftijdsgrens te omzeilen. Ten derde wordt er gewezen op de situatie in de zorg. Door bezuinigingen is er in jeugdzorginstellingen veelal geen 24 uursbegeleiding meer aanwezig, waardoor kwetsbare jonge vrouwen een verhoogd risico op slachtofferschap lopen. Sociaal zwakke jongeren, soms ook met een verstandelijke beperking, zullen in toenemende mate vanuit zorg- en begeleidwoneninstellingen worden geworven en uitgebuit.

Het rekruteringsproces zal de komende jaren nauwelijks veranderen. Het rekruteren via internet zal naar verwachting verder toenemen en mensenhandelaars hebben dankzij de digitale middelen een groter bereik, waardoor het eenvoudiger wordt slachtoffers uit verschillende landen te rekruteren.
Experts verwachten dat de gesignaleerde verschuiving van seksuele uitbuiting naar de onvergunde branche verder zal doorzetten en dat gaat hand in hand met de verwachte verdere verschuiving van de prostitutie van legaal en vergund naar illegaal en onvergund. Een ontwikkeling die hier naar verwachting een rol in zal spelen, is de beslissing omtrent de Wrp. Het wetsvoorstel bevat een fundamentele kanteling van het Nederlandse prostitutiebeleid: exploitatie van prostitutie is verboden, tenzij een vergunning is verleend.

In het huidige beleid is exploitatie van prostitutie juist toegestaan, tenzij vergunningplichtig bij gemeentelijke verordening. Mensenhandelaars zullen zich bij het tewerkstellen van (minderjarige) prostituees naar verwachting in toenemende mate gaan onttrekken aan het toezicht van handhavings- en opsporingsinstanties, waardoor de verschuiving van seksuele uitbuiting naar de onvergunde branche verder zal doorzetten. Een andere factor die mogelijk meespeelt in deze verschuiving is dat thuisprostitutie en escort minder kosten met zich meebrengen dan de vergunde branche. De invloed van digitalisering zoals het gebruik van internet en online diensten op de uitvoering van seksuele uitbuiting en op de verschuiving naar meer flexibele en anonieme vormen, thuisprostitutie en escort in het bijzonder, zal verder toenemen en kan de omvang van mensenhandel vergroten.

Mobiliteit en vluchtigheid zullen kenmerkend blijven voor de werkwijze van mensenhandelaars. Slachtoffers van seksuele uitbuiting zullen naar verwachting de komende jaren voor kortere perioden op eenzelfde locatie wonen en werken.

De investering van de politie in financiële expertise zal er mogelijk toe leiden dat mensenhandelaars de komende jaren meer maatregelen nemen om de geldstroom te versluieren. Net zoals voorheen zullen mensenhandelaars zich de komende jaren aanpassen aan veranderende omstandigheden.

Als gevolg van verschuiving van prostitutie van de vergunde naar de onvergunde branche zijn er de laatste jaren steeds meer overlastmeldingen van prostitutie vanuit woonwijken. Een verdere verschuiving naar onvergunde prostitutie leidt tot een toename van thuisprostitutie en escort, waardoor de overlast in woonwijken mogelijk verder gaat toenemen.

Verwachte gevolgen
Seksuele uitbuiting gaat geregeld gepaard met fysiek geweld en dat heeft ook de komende jaren grote gevolgen voor de slachtoffers, zowel fysiek als psychisch. Met de te verwachten verschuiving van de vergunde naar onvergunde prostitutie zullen er door het ontbreken van toezicht ook meer gevaarlijke gezondheidssituaties ontstaan. Ook door teruglopende verdiensten is het mogelijk dat seksuele diensten vaker onveilig worden aangeboden, waardoor meer risico's ontstaan op seksueel overdraagbare aandoeningen bij prostituees en hun klanten.
Met de verwachte verschuiving naar de onvergunde branche zullen ook de slachtoffers die seksueel uitgebuit worden op verschillende plekken worden ondergebracht en tewerkgesteld worden. Dat heeft mogelijk tot gevolg dat omwonenden meer hinder ondervinden.

De financiële gevolgen zullen naar verwachting vergelijkbaar zijn met de huidige gevolgen. Wel wordt een verschuiving verwacht in de financiële schade. In 2016 is het pilotproject Multidisciplinaire advisering slachtofferschap van start gegaan, dat als doel heeft de positie van slachtoffers te versterken. Mede hierdoor wordt verwacht dat het aantal uitkeringen van

schadevergoedingen aan slachtoffers gaat stijgen, waarmee de financiële schade voor de Nederlandse overheid zal toenemen en voor slachtoffers zal afnemen.

1.6.5 Kwalificatie van dreiging

Seksuele uitbuiting heeft ernstige gevolgen voor de Nederlandse samenleving, vooral vanwege de aantasting van de lichamelijke en geestelijke integriteit van de slachtoffers en het machtsgebruik waarmee de uitbuiting gepaard gaat. De slachtoffers lopen aanzienlijke gezondheidsrisico's als gevolg van fysiek geweld en onveilige seks. Naar verwachting verschuift de prostitutie de komende jaren verder naar de onvergunde branche door de verhoging van de minimumleeftijd van 18 naar 21 jaar om als prostituee werkzaam te mogen zijn. De gezondheidsrisico's voor prostituees en klanten zullen dan toenemen, evenals de overlast in woonwijken.

Seksuele uitbuiting wordt steeds vluchtiger en minder zichtbaar en grijpbaar onder invloed van digitale ontwikkelingen, het versluieren van de herkomst van crimineel geld en het subtiele en snelle inlijven van de slachtoffers. Er wordt een verdere toename verwacht van kwetsbare slachtoffers; minderjarigen en sociaal zwakkere jongeren, onder wie licht verstandelijk gehandicapten, zullen vaker worden geworven en uitgebuit. Ook vluchtelingen vormen een kwetsbare groep en door de toestroom van migranten zal het risico op uitbuiting in Nederland onder deze groep nieuwkomers naar verwachting toenemen. De financiële schade voor de slachtoffers en de Nederlandse overheid loopt jaarlijks in de tientallen miljoenen euro's. Voor de komende vier jaar zijn de verwachte gevolgen van deze vorm van slavernij in totaliteit dusdanig ernstig dat sprake is van een **dreiging** voor de Nederlandse samenleving.

1.7 Arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening

1.7.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Mensenhandel – Arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening*. Dat rapport bevat het verslag van een onderzoek dat voor dit dreigingsbeeld is uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Judith Roosblad, Marrit Ganzinga, Peter Plooij en Tamara Scholten, allen werkzaam bij de Inspectie van Sociale Zaken en Werkgelegenheid (Inspectie SZW). De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017*.
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Sinds 1 januari 2005 is mensenhandel buiten de seksindustrie strafbaar gesteld. Binnen het strafrechtelijke kader is het zogenoemde *non-consent*-principe van belang. Dit principe

houdt in dat eventuele toestemming van het slachtoffer van mensenhandel irrelevant is wanneer kan worden aangetoond dat voldaan is aan de wettelijke definitie van mensenhandel.
De Nationaal Rapporteur Mensenhandel maakt een onderscheid naar drie categorieën van uitbuiting buiten de seksindustrie, te weten arbeidsuitbuiting, gedwongen dienstverlening en criminele uitbuiting.
Arbeidsuitbuiting heeft betrekking op de uitbuiting die plaatsvindt in het domein van werk en inkomen. Onder gedwongen dienstverlening verstaat de Nationaal Rapporteur alle diensten die onder dwang moeten worden verricht en waar geen arbeidsverhouding aan ten grondslag ligt. Bij criminele uitbuiting worden personen gedwongen strafbare feiten te plegen. Daarnaast schaart de Nationaal Rapporteur ook het gedwongen aanvragen en vervolgens (in grote mate) afstaan van uitkeringen en voorzieningen (uitkeringsfraude) onder criminele uitbuiting.
In de tekst hanteren we de term *overige uitbuiting* om te verwijzen naar de drie categorieën van uitbuiting buiten de seksindustrie gezamenlijk.

1.7.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

Er is een drietal bronnen dat iets zegt over het aantal slachtoffers. In de eerste plaats de strafrechtelijke onderzoeken, zie tabel 4.

Tabel 4. Aantal strafrechtelijke onderzoeken naar type uitbuiting

Type uitbuiting	2007-2010	2011-2015
Arbeidsuitbuiting	12	41 (Inspectie SZW)
Gedwongen dienstverlening	1	7 (Inspectie SZW) 5 (politie)
Criminele uitbuiting		10 (Inspectie SZW) 22 (politie)
Totaal	**13**	**85**

Het aantal slachtoffers dat betrokken was bij de dertien onderzoeken uit de periode 2007-2010 bedraagt in totaal 91. Voor de periode 2011-2015 zijn veel meer slachtoffers bekend geworden. De 58 onderzoeken van de Inspectie SZW kenden alleen al 372 slachtoffers. Van de 27 politieonderzoeken ontbreekt informatie over slachtoffers. Bij ieder onderzoek zal echter minstens één slachtoffer betrokken zijn. Dit brengt het totaal op minimaal 399.
Het aantal meldingen van overige uitbuiting bij de inspectie van SZW bedraagt 351 over de periode 2011-2015 en stijgt ver uit boven de 85 uitgevoerde strafrechtelijke onderzoeken, omdat niet elke melding voldoende opsporingsindicaties heeft. Als strafrechtelijke vervolging niet mogelijk is, pakt de Inspectie SZW de overtreding van arbeidswetten bestuursrechtelijk aan. Deze aanpak past echter niet altijd bij het opzettelijke karakter van de overtreding of bij de maatschappelijke overtuiging dat er sprake is van uitbuiting. De

Inspectie SZW onderzoekt of zij die vormen op een andere manier kan aanpakken of dat de wetgeving moet worden aangepast.

Het is onbekend in hoeverre de toename van het aantal opsporingsonderzoeken veroorzaakt wordt door een daadwerkelijke toename in de omvang van het fenomeen overige uitbuiting. De prioritering ervan leidt tot meer aandacht en (dus) tot meer zaken.

Een tweede bron is CoMensha (Coördinatiecentrum tegen Mensenhandel). Dit registreert het aantal slachtoffers dat bij hen gemeld wordt door opsporingsinstanties, zoals de Koninklijke Marechaussee, de politie en de Inspectie SZW en overige organisaties, zoals de opvangvoorzieningen.
Deze registratie bevat 1072 (vermoedelijke) slachtoffers over de periode 2010-2014 (zie tabel 5).

Tabel 5. Aantal vermoedelijke slachtoffers van overige uitbuiting 2010-2014

Jaar	2010	2011	2012	2013	2014	Totaal 2010-2014
Aantal slachtoffers	128	250	257	178	259	**1072**

Bron: Nationaal Rapporteur Mensenhandel, *Mensenhandel in en uit beeld. Update mogelijke slachtoffers 2010-2014*

De derde bron is de Stichting Fairwork. Op basis van gegevens van de International Labour Organization (ILO) komt deze in 2012 tot een aantal van ruim 21.000 slachtoffers van arbeidsuitbuiting in Nederland. Dit aantal is omstreden, omdat geen rekening is gehouden met factoren die het aantal slachtoffers in een land beïnvloeden. Het gaat dan vooral om het feit dat Nederland in West-Europa, samen met vijf andere landen, op arbeidsmigranten van Oost-Europese origine de grootste aantrekkingskracht heeft als bestemmingsland. De schatting van 21.000 slachtoffers in Nederland zou daarom aan de lage kant zijn. De Nationaal Rapporteur Mensenhandel acht deze schatting niet betrouwbaar, omdat internationale schattingen niet zonder meer vertaald kunnen worden naar nationale schattingen en omdat slachtoffers niet evenredig naar inwonertal verdeeld zijn over landen.

We weten kortom niet precies hoeveel slachtoffers er zijn. Dat heeft een aantal oorzaken: niet alle uitbuiting komt ter kennis van de politie en de Inspectie SZW. Een deel van de slachtoffers is illegaal in Nederland, voor hen is aangifte doen niet de eerste optie. In veel zaken wordt slechts een deel van de slachtoffers geregistreerd en soms zien slachtoffers in formele zin (volgens de wettelijke criteria) zichzelf niet als slachtoffer. We kunnen wel concluderen dat het aantal strafrechtelijke onderzoeken en het aantal daarbij betrokken slachtoffers de laatste jaren sterk is toegenomen.

Aard

In deze paragraaf komen de volgende onderwerpen aan de orde:
- arbeidsuitbuiting
- criminele uitbuiting
- gedwongen dienstverlening
- nationaliteit slachtoffers
- criminele samenwerkingsverbanden

In de opsporingsonderzoeken naar *arbeidsuitbuiting* zien we zaken die we al langere tijd kennen, zoals koks in de Chinese horeca en Polen in de land- en tuinbouw. Het gaat vaak om zaken waarin de persoonlijke integriteit van het slachtoffer wordt geschonden. De slachtoffers verkeren in een kwetsbare positie, worden misleid, onderbetaald, zijn meervoudig afhankelijk en hun positie wordt misbruikt. In sommige gevallen is dit misbruik seksueel van aard. Het kenmerkende van deze zaken is dat er een werkgever-werknemerrelatie bestaat.

Dan is er de *criminele uitbuiting*, oftewel het dwingen tot criminele handelingen. De meeste opsporingsonderzoeken naar criminele uitbuiting zijn door de politie uitgevoerd. Bij deze zaken gaat het met name om gedwongen hennepteelt en drugstransporten. Daarnaast is een aantal gevallen van gedwongen winkeldiefstal en woninginbraak bekend en zijn er diverse onderzoeken waaruit blijkt dat kinderen het slachtoffer zijn van gedwongen criminaliteit, vooral winkeldiefstal en bedelarij. Het inzetten van kinderen is aantrekkelijk omdat de strafrechtelijke vervolging problematisch is. Een toenemende vorm van criminele uitbuiting is het gedwongen aanvragen van allerlei uitkeringen (bijvoorbeeld bijstand), subsidies (persoonsgebonden budget, sociale werkvoorziening) en toeslagen (zorg- en huurtoeslag). In de criminele uitbuitingszaken waarbij een verdenking is van fraude met het persoonsgebonden budget (PGB) of uitkeringsfraude zien we recent vooral Nederlandse slachtoffers. In vijf van de zes onderzoeken is sprake van Nederlandse slachtoffers. In totaal gaat het hierbij om minimaal 34 Nederlandse mannen en vrouwen, veelal in een kwetsbare positie veroorzaakt door psychische problemen en verslavingsproblematiek.

In gevallen van *gedwongen dienstverlening* wordt het slachtoffer onder dwang tot verschillende diensten aangezet, maar ontbreekt een daadwerkelijke werkgever-werknemerrelatie. In vijf onderzoeken die door de politie zijn gedaan, ging het om het gedwongen afsluiten van telefoonabonnementen. De slachtoffers waren meisjes die in handen waren gevallen van een loverboy en ook tot prostitutie gedwongen werden. Er bestaat een toenemende variëteit in de vormen waarin gedwongen dienstverlening zich voordoet. Zo heeft de Inspectie SZW zeven onderzoeken gedaan naar gedwongen dienstverlening die zich afspeelden in de huishoudelijke sfeer en het verrichten van allerlei klussen.

Bij een analyse van de opsporingszaken die tussen 2011 en 2015 hebben gedraaid, valt allereerst op dat bepaalde sectoren nauw zijn te relateren aan slachtoffers met een specifieke *nationaliteit*. In sectoren als de land- en tuinbouw, bouw, vleesverwerkingsindustrie en

uitzendbranche is met name sprake van slachtoffers uit Midden- en Oost- Europese landen, zoals Polen, Roemenië, Hongarije, Oekraïne, Bulgarije en Litouwen. In de horeca, binnenvaart en detailhandel bestaat een groot deel juist uit niet-Europese slachtoffers. In de (Chinese) horeca zien we vooral Chinese slachtoffers. Recent echter worden bij controles regelmatig Hongaarse werknemers aangetroffen in de Chinese horeca, die te maken hebben met onderbetaling en lange werkdagen of op een andere manier worden benadeeld. In genoemde gevallen is er onvoldoende indicatie voor een strafrechtelijk onderzoek naar arbeidsuitbuiting, maar het is wel een signaal dat er mogelijk een verschuiving plaatsvindt in slachtoffers in de Chinese horeca. In de binnenvaart is een aantal grote onderzoeken uitgevoerd waar Filipijnse slachtoffers bij betrokken waren. Tot slot zijn in de detailhandel (massagesalon, wasserette en textiel) onderzoeken afgerond met slachtoffers uit Nepal, India en China.

Volgens Europol bestaan de *criminele samenwerkingsverbanden* (csv's) die zich in de Europese Unie bezighouden met mensenhandel hoofdzakelijk uit kleinere verbanden van drie tot vijftien personen. De leden van deze csv's hebben vaak familiale of etnische banden. Csv's werken doorgaans onafhankelijk van andere criminele groepen en houden zich ook bezig met andere criminele activiteiten. De meest voorkomende nevenactiviteiten zijn vormen van fraude, zoals btw-fraude, uitkeringsfraude en identiteitsfraude.
Ook voor Nederland nemen de deskundigen een diversificatie van criminele activiteiten waar. Steeds vaker zien zij een combinatie van diverse vormen van uitbuiting, bijvoorbeeld seksueel en arbeid, of een combinatie van arbeidsuitbuiting en uitkeringsfraude. Dit komt overeen met het beeld dat uit de afgeronde opsporingsonderzoeken van de Inspectie SZW naar voren komt.
Deskundigen nemen verschillende trends waar in de mate waarin sprake is van georganiseerde criminaliteit in Nederland. Volgens sommigen neemt de mate van georganiseerdheid van de uitbuiting toe. Daarbij wordt geconstateerd dat er sprake is van een steeds professionelere aanpak: de csv's zijn schoolvoorbeelden van lerende organisaties die hun methoden steeds aanpassen aan de mazen van de wet en de gepleegde inzet van opsporing en opvolging.
Tevens lijkt er een tendens te zijn van uitbuiting waarbij één dader betrokken is en waarbij er sprake is van een afhankelijkheidsrelatie. Dit speelt met name bij criminele uitbuiting.

1.7.3 Huidige gevolgen

Uitbuiting buiten de seksindustrie kent een breed scala aan schadelijke gevolgen. Zo zijn er gevolgen voor het individuele slachtoffer, maar ook voor de overheid en het bedrijfsleven. Daarnaast zien we gevolgen voor de leefomgeving en de maatschappij.

Uitbuiting vormt een ernstige schending van de mensenrechten die grote risico's met zich meebrengt voor de individuele slachtoffers. De individuele gevolgen kennen een grote varieteit. Soms is sprake van (seksueel) geweld, soms worden de eerste levensbehoeften onthouden en soms worden slachtoffers blootgesteld aan situaties die direct gevaar voor

hen opleveren. Daarnaast worden slachtoffers afhankelijk gemaakt door intimidatie en bedreigingen en worden ze vaak beperkt in hun bewegingsvrijheid. Ook ontstaat een zekere mate van economische afhankelijkheid, omdat er een groot verschil zit tussen dat wat verdiend wordt en dat wat de slachtoffers uiteindelijk overhouden.

Het *bedrijfsleven* ondervindt schade door arbeidsuitbuiting. Verstoring van de arbeidsmarkt en oneerlijke concurrentie zijn daarvan de meest pregnante vormen. Wanneer bedrijven het niet zo nauw nemen met de regels en werknemers onder het wettelijk minimumloon tewerk worden gesteld, kunnen andere bedrijven daar niet mee concurreren. Bovendien zorgt uitbuiting voor verdringing op de arbeidsmarkt en leidt dit fenomeen tot economische schade. De schatting is dat het bedrijfsleven enkele tientallen miljoenen euro's schade per jaar lijdt.

Ook de *overheid* ondervindt op verschillende manieren schade door overige uitbuiting. Zo worden de kosten van de zorg voor slachtoffers afgewenteld op de maatschappij. Ook garandeert de overheid uitbetaling van een eventuele schadevergoeding van de dader aan het slachtoffer als de dader in gebreke blijft. Omdat door verdringing meer mensen in een uitkeringssituatie terechtkomen, maakt de overheid kosten.
De overheid loopt inkomsten mis doordat er geen premies en afdrachten worden betaald voor illegale werkers of te weinig voor mensen die in werkelijkheid veel meer werken dan op papier. Omdat ten onrechte uitkeringen worden verstrekt en subsidies verleend, heeft dit negatieve financiële gevolgen voor de overheid.
Om een indicatie te geven van de bedragen waar het in de huidige onderzoeksperiode om gaat, is het wederrechtelijk verkregen voordeel in 37 onderzoeken van de Inspectie SZW berekend. In 29 gevallen gaat dit om het werkelijk verkregen voordeel, met een totaalbedrag van ruim 21 miljoen euro. In de overige acht gevallen zijn de bedragen schattingen. Deze schattingen behelzen nog eens een bedrag van ruim een half miljoen euro. Gemiddeld is het wederrechtelijk verkregen voordeel een kleine 600.000 euro per onderzoek.
De overheid lijdt niet alleen financiële schade, ook haar legitimiteit wordt aangetast. Het vertrouwen van burgers in de overheid neemt af wanneer zij in de directe omgeving dergelijke frauduleuze praktijken kennen waar (vermoedelijke) daders 'mee wegkomen'. Alles bij elkaar genomen wordt geschat dat de overheid enkele honderden miljoenen euro's schade oploopt door gemiste (belasting)inkomsten en de uitgave van onterechte subsidies en uitkeringen.

De gevolgen voor de *maatschappij* bestaan vooral uit economische gevolgen in de vorm van zwart uitbetaald geld dat in de legale economie terechtkomt en verweving van onder- en bovenwereld doordat allerlei facilitatoren bewust of onbewust diensten verlenen die uitbuiting mogelijk maken en bestendigen.

Tot slot heeft uitbuiting negatieve gevolgen voor de *leefomgeving*. Een zichtbaar, direct gevolg is de overlast die de huisvesting van slachtoffers van uitbuiting voor de omgeving veroorzaakt. In kleine panden worden te veel mensen gehuisvest.
Daarnaast kan worden gedacht aan negatieve consequenties en gevaarlijke situaties voor de leefomgeving, doordat er wordt gewerkt zonder vereiste diploma's en certificaten. Een concreet voorbeeld zijn de vervalste gezondheidsverklaringen in de vleesverwerkingsindustrie. Dit kan een gevaar opleveren voor de voedselveiligheid.

1.7.4 Verwachtingen

Demografische ontwikkelingen, zoals grote migratie- en vluchtelingenstromen, en ontwikkelingen op de arbeidsmarkt en in de economie, zoals verdergaande flexibilisering en globalisering, zullen ertoe bijdragen dat er grote groepen mensen komen die in een (financieel) kwetsbare positie verkeren en daardoor vatbaar zijn voor uitbuiting. Europol en Interpol verwachten hierdoor een toename van arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening.
Mensensmokkelorganisaties zullen zich actiever gaan bezighouden met mensenhandel en nauwe(re) samenwerkingsverbanden aangaan.
Een deel van de vluchtelingen zal geen verblijfsstatus krijgen. Nederland kent echter geen actief uitzetbeleid, waardoor uitgeprocedeerde asielzoekers in de Nederlandse samenleving blijven en een kwetsbare groep vormen. De verwachting is dan ook dat er een toename zal zijn van uitbuiting van bepaalde groepen, zoals uitgeprocedeerde asielzoekers uit zogeheten veilige landen.

Economische en arbeidsmarktgerelateerde factoren zullen hun invloed doen gelden. Zo is er de impact die de flexibilisering van de arbeidsmarkt heeft op de aard en omvang van uitbuiting. In de afgelopen jaren is het aandeel werkenden met een flexibele arbeidsrelatie in Nederland toegenomen. Was dit in 2003 nog geen 18 procent, in 2015 was dit gestegen tot 27 procent. Ook het aantal banen op oproepbasis is flink gestegen. Bij dergelijke banen wordt geen vaste arbeidsduur overeengekomen tussen werkgever en werknemer. Er wordt vooral meer op oproepbasis gewerkt in de handel, horeca en zorg. Naar verwachting zal de flexibilisering van de arbeidsmarkt de komende periode verder toenemen. De stijging van het aantal mensen in een precaire arbeidsrelatie zal ertoe leiden dat er meer mensen bij komen die zich in een kwetsbare positie bevinden en die mogelijk in een uitbuitingssituatie terechtkomen, met name daar waar de precaire arbeidssituatie gepaard gaat met armoede en schuldenproblematiek.
De toenemende globalisering zal een (nog) grotere nadruk op kostenverlaging en winstmaximalisatie met zich meebrengen. De vraag naar een zo goedkoop mogelijk eindproduct leidt tot lage lonen in de rest van de keten en de vraag naar goedkope arbeidskrachten. Dit kan leiden tot baanverlies en een wedloop naar de bodem op arbeidsvoorwaardengebied. Ook Europol voorziet dat de aanhoudende vraag naar steeds goedkopere producten en diensten, gecombineerd met een geïntensiveerde competitie tussen leveranciers, een sterke neerwaartse invloed zal hebben op prijzen en nieuwe mogelijkheden zal creëren voor

exploitatie. Volgens Europol zal dit leiden tot een verhoogd risico op uitbuiting van slachtoffers op de reguliere arbeidsmarkt.

Wat betreft politieke ontwikkelingen en ontwikkelingen op het gebied van wet- en regelgeving, bestaat een risico in de tendens van een verder terugtredende overheid. Minder regels en minder toezicht kunnen in bepaalde sectoren leiden tot een nieuwe gelegenheidsstructuur waarbinnen uitbuiting zal gaan plaatsvinden.

Vrijwel alle respondenten verwachten een toenemende professionaliteit van criminele organisaties. Een belangrijk aspect dat hierbij een rol speelt, is dat csv's lerende organisaties zijn die zich steeds aanpassen aan de mazen van de wet en aan de gepleegde inzet van de opsporing. Er zal dan ook een stijging te zien zijn in praktijken die uitbuiting verhullen en aan het oog onttrekken. Denk hierbij aan een stijging van de inzet van malafide bemiddelingsbureaus die via internet werkenden van binnen en buiten de Europese Unie werven en aan het verder 'uitnutten' van het Europese wettelijk kader van vrij verkeer van mensen en diensten. Ook zal het gebruik van een 'wettige voorgevel' met daarachter allerlei bedenkelijke constructies toenemen. Bij deze constructies valt te denken aan de inzet van sjoemelsoftware (het manipuleren van de boekhouding zodat een regulier beeld wordt gecreëerd), complexe bedrijfsstructuren (vestigingen in meerdere landen) en *windowdressing* (het gebruikmaken van reguliere huisvesting en schijnbaar reguliere arbeidsomstandigheden om niet op te vallen). Bij deze ontwikkelingen voorziet men tevens een toenemende verwevenheid van onder- en bovenwereld om deze maskerade te verhullen.
Verder verwacht een deel van de respondenten een toename van het combineren van uitbuiting met andere criminele activiteiten. Zo wijzen zij op het gebruik van dezelfde routes voor bijvoorbeeld de smokkel van drugs en handel in mensen, waar mogelijk dezelfde criminele organisaties achter zitten. Dit beeld wordt bevestigd door onderzoek van Europol. Rondom de migratiestroom is volgens Europol een criminele infrastructuur ontstaan die het hele Europese continent omspant. Bekende mensenhandelaars uit de seksindustrie en de slavenarbeid zijn overgestapt naar het smokkelen van migranten naar de Europese Unie.

1.7.5 Kwalificatie van dreiging

De drie vormen van uitbuiting die in deze paragraaf beschreven zijn, hebben een grote varieteit aan schade tot gevolg. Zowel individuele slachtoffers als bedrijfsleven en overheid lijden financiële schade. Deze schade loopt in de honderden miljoenen euro's. Daarnaast zijn er ernstige fysieke en psychische consequenties voor de slachtoffers. Hoewel we de precieze omvang van deze vormen van uitbuiting niet kennen, gaat het om minimaal honderden slachtoffers per jaar.
Deze vorm van georganiseerde criminaliteit gaat tevens gepaard met verschillende manifestaties van ondermijning zoals verwevenheid van boven- en onderwereld en aantasting van de integriteit van het bestuur.

De verwachting voor de komende jaren is dat de problematiek zal toenemen vanwege het ontstaan van nieuwe kwetsbare groepen binnen de migrantenpopulatie. Gelet op de ernst van de gevolgen, in het bijzonder voor de persoonlijke integriteit van uitgebuite personen, en de verwachte toename van het aantal gevallen, vormt uitbuiting buiten de seksindustrie een **dreiging** voor de Nederlandse samenleving.

1.8 Mensensmokkel

1.8.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Deelproject mensensmokkel. Input voor het NDB 2017*. Het onderzoek is uitgevoerd door de Koninklijke Marechaussee en de auteurs van de rapportage zijn Irma Tijssens en Claudia van der Grijn. De bronnen die zijn gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf wordt de kwalificatie van dreiging beschreven. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is beargumenteerd en vastgesteld in een andere context door een groep van beoordelaars (de consensusgroep).

Mensensmokkel is een niet op zichzelf staand probleem voor de Nederlandse maatschappij. Het is bij uitstek een internationaal delict omdat er sprake is van illegale grensoverschrijding. Het Schengenakkoord heeft destijds vrij verkeer van personen geregeld, waardoor de bewaking van de binnengrenzen is komen te vervallen en er een gezamenlijke buitengrens is ontstaan. Er is een uitzonderingsbepaling opgenomen die het in het kader van de nationale veiligheid en de openbare orde mogelijk maakt de grenscontroles tijdelijk in te voeren. De landen die deel uitmaken van het Schengengebied, waaronder Nederland, zijn samen verantwoordelijk voor het gemeenschappelijke beleid inzake het beheer van de buitengrens om de veiligheid binnen het Schengengebied te waarborgen.

Mensensmokkel is nauw verbonden met migratiestromen en speelt zich af in de context van de irreguliere migratie die plaatsvindt vanaf het land van herkomst tot aan een (Europees) bestemmingsland. Mensensmokkel zullen we daarom beschrijven vanuit deze bredere context. Dit betekent een domeinuitbreiding ten opzichte van het vorige dreigingsbeeld, omdat daarin enkel is ingegaan op de criminele activiteiten die in dit verband op Nederlands grondgebied plaatsvonden. De huidige omvangrijke migratiestromen en de hoge asielstatistieken maken het schetsen van een bredere context noodzakelijk om de problematiek te kunnen duiden.

Voor mensensmokkel wordt uitgegaan van de juridische afbakening. Het gaat hierbij om:

1. personen die anderen behulpzaam zijn bij het verschaffen van toegang tot (of doorreis door) Nederland of een andere lidstaat van de Europese Unie, terwijl ze weten of zouden kunnen veronderstellen dat deze toegang wederrechtelijk is (art. 197a lid 1 Sr);
2. personen die anderen uit winstbejag behulpzaam zijn bij een illegaal verblijf in Nederland (art. 197a lid 2 Sr).

1.8.2 Ontwikkelingen in aard en omvang sinds het NDB2012

De afgelopen jaren is de omvang van irreguliere migratiestromen naar het Schengengebied toegenomen. Migranten die zonder toestemming en geldige documentatie de Europese Unie binnenkomen, worden irreguliere migranten genoemd. Uit de jaarlijkse risicoanalyses van Frontex (het Europees agentschap waarin de lidstaten van de EU samenwerken om de Europese buitengrens te bewaken) blijkt dat het aantal geregistreerde illegale grensoverschrijdingen door migranten de afgelopen jaren sterk is toegenomen: van 72.000 in 2012 tot een recordhoogte van meer dan 1,8 miljoen in 2015.
Hoeveel irreguliere migranten er precies bij deze grensoverschrijdingen betrokken zijn, is niet bekend. Een migrant kan tijdens zijn reis meerdere keren geregistreerd worden, bijvoorbeeld zowel in Griekenland als op doorreis in Hongarije. Een deel van deze irreguliere migranten wordt door mensensmokkelaars de grens over geholpen. Hoe groot dit deel is, is lastig vast te stellen. De schattingen lopen uiteen van 66 tot 100 procent. Als we afgaan op de laagste schatting is er in 2015 bij meer dan een miljoen illegale grensoverschrijdingen gebruikgemaakt van een mensensmokkelaar.

In 2014 werd veelal de centraal-mediterrane route gebruikt, waarbij met bootjes vanuit Libië de oversteek wordt gemaakt naar Italië. De irreguliere migranten die reizen via de centraal-mediterrane route hebben over het algemeen de nationaliteit van een van de Afrikaanse landen, al nemen ook Syriërs regelmatig deze route. In 2015 werd meer de oostelijke mediterrane route gebruikt, via Turkije naar Griekenland, van waaruit de irreguliere migranten via de westelijke Balkanroute verderreizen naar bestemmingslanden in Europa. Irreguliere migranten via deze route hebben veelal de Syrische, Afghaanse of Iraakse nationaliteit. Belangrijke *hubs* bij deze routes zijn: Athene, Milaan, Turijn, Boedapest en Wenen.

De werkwijzen die door mensensmokkelaars worden gebruikt bij de maritieme oversteek naar het Schengengebied zijn de afgelopen jaren veranderd. Mensensmokkelaars nemen tegenwoordig meer risico's, waardoor steeds meer migranten verdrinken. De boten die worden gebruikt, zijn vaak onveilig, overvol en hebben te weinig brandstof om Europa te bereiken.

Een groot deel van de irreguliere migranten die in het Schengengebied aankomen, reist door naar de noordwestelijk gelegen lidstaten, waaronder Nederland. Nederland fungeert net als vier jaar geleden nog steeds als transitland voor migranten die het Verenigd Koninkrijk en

Scandinavië als eindbestemming hebben. Vergeleken met de situatie ten tijde van het vorige dreigingsbeeld is Nederland daarnaast ook steeds vaker een bestemmingsland. Het aantal asielaanvragen in Nederland is gestegen van minder dan 10.000 in 2012 tot 43.000 in 2015. De meeste aanvragen komen van Syrische en Eritrese asielzoekers. Nederland is vooral voor deze groep een belangrijk bestemmingsland. Deze asielzoekers hebben niet allemaal hulp gehad van mensensmokkelaars. Er is weinig bekend over reisbewegingen door Europa, maar gaan we uit van de eerdergenoemde schatting dat in 2015 bij minstens 66 procent van de illegale grensoverschrijdingen gebruik is gemaakt van een mensensmokkelaar, dan hebben ruim 28.000 asielzoekers in Nederland gebruikgemaakt van een mensensmokkelaar.

In Europa is het aantal aanhoudingen voor mensensmokkel gestegen van 10.000 in 2014 naar meer dan 12.000 in 2015. Het aantal aanhoudingen in Nederland door de Koninklijke Marechaussee is in 2015 gestegen naar meer dan 300. In de jaren ervoor waren het er jaarlijks ongeveer 200. Het aantal bij het Openbaar Ministerie aangedragen verdachten van mensensmokkel neemt de laatste jaren eveneens toe: van 155 in 2012 tot 224 in 2015. Er is echter geen sprake van een toename ten opzichte van de periode van het vorige dreigingsbeeld; in 2010 was het aantal verdachten 250.

Mensensmokkel lijkt meer dan voorheen een criminele markt die bepaald wordt door vraag en aanbod. De vraag naar hulp bij illegale grensoverschrijding is toegenomen en opportunistische gelegenheidssmokkelaars spelen hierop in en bieden zich aan. Door de toegenomen vraag en de daaraan gekoppelde marktwerking lijkt er sprake van een veranderde rol van zowel de mensensmokkelaar als de irreguliere migrant die heeft geleid tot een meer zakelijke instelling bij beide partijen over de te leveren diensten. De reis van bronland naar bestemming is vaak duur en irreguliere migranten reizen vaak van plaats naar plaats (hubs). Dit wordt ook wel aangeduid als een step-by-stepreis. Sociale media bieden de irreguliere migrant de gelegenheid om op een gemakkelijke manier voor elke stap opnieuw contact te zoeken met mensensmokkelaars en te onderhandelen over de volgende stap. Overigens zijn de irreguliere migranten dankzij de nieuwe communicatiemogelijkheden en smartphones ook in toenemende mate in staat om zelfstandig te reizen, zonder hulp van mensensmokkelaars.

1.8.3 Huidige gevolgen

Het is soms moeilijk vast te stellen of de gevolgen van mensensmokkel alleen zijn toe te kennen aan mensensmokkel of ook aan irreguliere migratie in algemene zin. Daarom stellen wij hier de gevolgen van irreguliere migratie in algemene zin aan de orde, om vervolgens waar mogelijk te specificeren naar de gevolgen die aan de bemoeienis van mensensmokkelaars kunnen worden toegeschreven.

Fysieke en psychische schade
Irreguliere migranten die voor hun reis gebruikmaken van mensensmokkelaars, lopen allerlei ernstige risico's. Bij de oversteek over de Middellandse en de Egeïsche Zee lopen ze het risico om door verdrinking te overlijden. De afgelopen jaren zijn er jaarlijks duizenden doden gevallen als gevolg van onveilige boten die worden ingezet door mensensmokkelaars. Wanneer alleen gekeken wordt naar de Nederlandse situatie, zijn er nauwelijks ernstige gevallen bekend van fysieke consequenties voor de gesmokkelde migranten op het laatste reisdeel binnen het Schengengebied.
Bij veel irreguliere migranten zal er sprake zijn van psychische gevolgen. Velen zijn gevlucht uit oorlogsgebieden en hebben traumatische ervaringen gehad in het land van herkomst. Tijdens de reis kunnen ze ook allerlei traumatische ervaringen hebben opgedaan waarvoor mensensmokkelaars verantwoordelijk zijn. Denk aan de migranten die de oversteek in een gammel bootje hebben overleefd, maar wel familieleden of medereizigers hebben zien verdrinken. Kortom, velen zullen in meer of mindere mate psychische problemen hebben, maar hoeveel en in welke mate is onbekend.

Overlast: hinder, angst en onbehagen
De komst van grote groepen irreguliere migranten zorgt voor angst en onbehagen bij delen van de Nederlandse bevolking. Mensensmokkel faciliteert irreguliere migratie, waardoor meer illegale migranten erin slagen een Europese bestemming, waaronder Nederland, te bereiken.

Financiële schade: bedrijfsleven en overheid
Op basis van diverse bronnen kan worden gesteld dat zowel het bedrijfsleven als de overheid te maken krijgt met een grote variëteit aan kosten als gevolg van mensensmokkel en irreguliere migratiestromen in meer algemene zin. Enerzijds zijn er kosten verbonden aan het verblijf van asielzoekers en anderzijds zijn er kosten verbonden aan mensen die hier illegaal verblijven en gefaciliteerd worden (denk aan illegale arbeid waardoor bepaalde premies en belastingen niet worden betaald). Hoewel niet alle kosten direct kunnen worden gerelateerd aan mensensmokkel en kosten moeilijk kwantificeerbaar zijn, maakt veruit het merendeel van de illegale migranten gebruik van mensensmokkelaars.
Eerder werd geschat dat (minstens) 28.000 illegale migranten die in 2015 naar Nederland zijn gekomen, hulp hebben gehad van mensensmokkelaars. Verder zal een deel van de irreguliere migranten in de illegaliteit belanden, omdat hun asielverzoek wordt afgewezen of omdat ze geen asiel hebben aangevraagd. De Inspectie SZW schat dat een illegaal ongeveer 60.000 euro per jaar kost. Er zijn schattingen dat er in Nederland 100.000 illegalen verblijven. Hoewel het onmogelijk is om exact aan te geven wat de geleden schade is als gevolg van mensensmokkel, gaat het om aanzienlijke bedragen: vermoedelijk om honderden miljoenen euro's of meer.

De grootste kostenpost voor het bedrijfsleven wordt veroorzaakt door de wachttijden die te wijten zijn aan de geïntensiveerde controles aan de binnengrenzen. Vooral de transport- en logistieke sector heeft hierdoor te maken met schades die kunnen oplopen tot miljoenen euro's. Andere financiële gevolgen van mensensmokkel voor die branche zijn de verbeurdverklaringen van ladingen omdat er migranten zijn aangetroffen, en schade aan materieel omdat zeilen van vrachtwagens kapot worden gesneden en sloten worden geforceerd. De brancheorganisatie Transport en Logistiek Nederland schat de schade voor de Nederlandse transportsector voor 2015 tussen de 100 en 150 miljoen euro.

De overheid maakt kosten voor opvang, inburgering, onderwijs en andere faciliteiten, terwijl een deel van de migranten op onrechtmatige wijze is binnengekomen en daar feitelijk geen recht op heeft. Dat zijn bijvoorbeeld irreguliere migranten die op basis van valse documenten of valse verklaringen asiel krijgen. Verder zijn kosten meegerekend die betrekking hebben op illegale tewerkstellingen. Hierbij valt te denken aan premies die niet worden afgedragen, maar ook aan oneerlijke concurrentie in bepaalde branches.

Ondermijning
Vooralsnog is er van schade als gevolg van ondermijning slechts in geringe mate sprake. Hierbij kan gedacht worden aan misbruik van legale procedures en het gebruik van valse documenten.

1.8.4 Verwachtingen

Er is sprake van een toenemende destabilisatie in grote delen van het Midden-Oosten en Afrika. De factoren die aan de conflicten ten grondslag liggen, zijn vaak complex van aard. Het wordt onwaarschijnlijk geacht dat deze regio's op korte termijn zullen stabiliseren. Er wordt daarom voor de komende vijf à tien jaar een toenemende (irreguliere) migratie richting Europa verwacht.

Voor een groot deel van deze migranten is Europa de bestemming waar ze naartoe willen. Gelet op de omvang van de asielinstroom in Nederland de afgelopen twee jaar, wordt Nederland waarschijnlijk ook de komende jaren als een aantrekkelijk bestemmingsland gezien.
Als reactie op de verhoogde instroom van irreguliere migranten worden er op Europees niveau en door de individuele lidstaten diverse maatregelen getroffen om de irreguliere migratie te beheersen. Die maatregelen dienen bij te dragen aan het tegengaan van mensensmokkel. Er worden barrières opgeworpen in de vorm van controles aan de binnen- en buitengrenzen. Tevens wordt er een restrictiever migratiebeleid gevoerd.

De getroffen maatregelen van de lidstaten zijn van invloed op de toekomstige mensensmokkelmarkt. De belangrijkste veranderingen naar aanleiding van deze ontwikkelingen zullen naar alle waarschijnlijkheid zijn: diversificatie van routes en werkwijzen, toenemende vraag naar mensensmokkelaars en een toenemende professionalisering.

Door de getroffen maatregelen, zoals het akkoord van 2016 tussen de EU en Turkije over het inperken van de migratiestroom naar Europa, zal het moeilijker worden te voorspellen hoe de stroom van irreguliere migranten zich zal gaan ontwikkelen. Vermoedelijk zal er een waterbedeffect ontstaan en zullen migratiestromen andere routes volgen. Belangrijke alternatieve opties zijn de centraal-mediterrane en de westelijke mediterrane route, reizen via Rusland, maar ook reizen via de Zwarte Zee.

Een restrictief beleid in Nederland en andere Europese landen leidt niet automatisch tot een afname van het aantal irreguliere migranten. De stroom asielzoekers blijft bestaan, omdat de omstandigheden in de herkomstlanden niet verbeterd zijn. Een restrictief beleid maakt het moeilijker om grenzen te passeren waardoor er meer behoefte ontstaat aan hulp van mensensmokkelaars. Dit geldt overigens niet alleen voor het fysiek passeren van grenzen. De inperking van de mogelijkheden tot gezinshereniging leidt eveneens tot meer vraag naar hulp van mensensmokkelaars. Dit kan zijn in de vorm van hulp bij het illegaal passeren van de grens, maar ook bij het vervalsen van de benodigde ondersteunende documenten.
Een restrictief beleid leidt mogelijk ook tot een toenemende vraag naar illegaal werk en illegaal onderdak. Als er meer afwijzingen van asielaanvragen, gezinshereniging en dergelijke plaatsvinden, bestaat de kans dat er meer afgewezen migranten in de illegaliteit terechtkomen. Of eerder al: dat de migranten, vanwege de beperkte kans op inwilliging van de asielaanvraag, al bij binnenkomst in de illegaliteit belanden. Een toenemende vraag naar illegaal werk en illegaal onderdak zal vrijwel zeker leiden tot meer mensensmokkel.

Door de omvang van de irreguliere migratiestroom in combinatie met alle beleidsmaatregelen die door de Europese Unie en de individuele lidstaten worden genomen, is de situatie waarin de migranten zich bevinden niet eenvoudig. Een en ander drijft de prijs voor hulp bij migratie op en stelt hogere eisen aan mensensmokkelaars: zij moeten beter geïnformeerd zijn en professioneler te werk gaan. Opdrijving van de prijs zal naar verwachting meer criminele organisaties aantrekken die koste wat kost gericht zijn op geld verdienen en zij zullen (nog) minder rekening houden met het welzijn van de migranten. Hierdoor zal vermoedelijk een verharding optreden met alle consequenties van dien voor de irreguliere migranten die zich in een afhankelijkheidspositie bevinden met weinig tot geen autonomie, overgeleverd aan de grillen van geharde criminelen, waardoor het risico op uitbuiting toeneemt.

Verwachte gevolgen
Met de verwachte professionalisering en verharding van de mensensmokkelmarkt, wordt in toenemende mate fysiek (en eventueel daaraan gekoppeld psychisch) leed verwacht voor de gesmokkelde migranten en worden meer risicovolle werkwijzen verwacht. Wanneer dat resulteert in daadwerkelijke (grote) incidenten in (de buurt van) Nederland, kan dat leiden tot meer gevoelens van angst en onbehagen onder burgers.

De maatregelen om mensensmokkel tegen te gaan hebben economische consequenties. De controles aan de binnengrenzen raken de transport- en logistieke sector, vooral vanwege vertragingen. De migratiedruk aan de buitengrens en de angst voor terroristische aanslagen vergroten de sociale en politieke druk om de binnengrenzen te blijven bewaken. De controles zullen daarom naar verwachting blijven aanhouden of worden uitgebreid en dat zal de huidige kosten voor het bedrijfsleven (100 tot 150 miljoen euro) verder doen toenemen. Het restrictieve beleid zorgt eveneens voor een verandering van werkwijzen, waarbij vermoedelijk steeds meer misleiding plaatsvindt en legale procedures vaker worden misbruikt. De irreguliere migranten maken dan misbruik van diverse voorzieningen, wat een extra kostenpost voor de overheid vormt. Ook de verwachte toename van de populatie illegalen leidt door meer illegale tewerkstellingen mogelijk tot hogere kosten voor de overheid door misgelopen premies.

Het restrictievere beleid leidt niet alleen tot professionalisering en verharding van de mensensmokkelmarkt, smokkelaars op die markt zullen ook vaker aangewezen zijn op corrumptieve contacten om grensoverschrijding toch te kunnen realiseren.
De verwachte toename in het misbruik van legale procedures en misleiding door het presenteren van een schijnwerkelijkheid zet de asielprocedure onder druk en zal in toenemende mate een ondermijnend effect hebben op de rechtsorde en rechtspleging.
Het groeiend aantal illegale werkers kan in bepaalde branches leiden tot oneerlijke concurrentie.

1.8.5 Kwalificatie van dreiging

Bij het bespreken van dit criminele verschijnsel doemen onmiddellijk indringende beelden op van vastgelopen vluchtelingen in overvolle opvangkampen en verdronken bootvluchtelingen. Dergelijke situaties doen zich op Nederlands grondgebied niet voor, maar er zijn wel degelijk gevolgen van mensensmokkel die zich binnen Nederland manifesteren.

De geleden schade voor de Nederlandse samenleving als gevolg van mensensmokkel bedraagt jaarlijks honderden miljoenen euro's. Zowel het bedrijfsleven als de overheid krijgt te maken met een grote variëteit aan kosten. Zo zijn er voor de overheid kosten verbonden aan asielaanvragen door irreguliere migranten, vanwege illegaal verblijf en door misbruik van procedures. Het bedrijfsleven heeft te maken met aanzienlijke kosten die te wijten zijn aan de geïntensiveerde controles aan de Europese binnengrenzen. Hoewel niet alle kosten direct kunnen worden gerelateerd aan mensensmokkel en sommige kosten moeilijk kwantificeerbaar zijn, staat vast dat het om aanzienlijke bedragen gaat.

De toegenomen irreguliere migrantenstroom heeft geleid tot maatregelen van de lidstaten om deze stroom in te dammen, onder meer door extra toezicht op de buitengrenzen van het Schengengebied maar ook daarbinnen. Dit heeft consequenties voor de toekomstige mensensmokkelmarkt. Het wordt complexer om Europa binnen te komen en de uiteindelijke bestemmingslanden te bereiken. Hierdoor ontstaat er bij vluchtelingen een behoefte aan professionele hulp van mensensmokkelaars om alsnog het gewenste doel te bereiken.

De geschetste ontwikkelingen zullen de negatieve gevolgen van mensensmokkel voor Europa en de Nederlandse samenleving in stand houden of verergeren. Door toename van professionele criminele groeperingen die winstmaximalisatie nastreven en de daarmee gepaard gaande verharding zullen meer vluchtelingen verdrinken en de gezondheidsschade voor gesmokkelde migranten zal toenemen. Een groeiende illegalenpopulatie leidt tot meer oneerlijke concurrentie. De kosten voor het bedrijfsleven zullen aanhouden, evenals de kosten voor de overheid. Het risico op corruptie, omkoping en misbruik van legale procedures wordt groter. De verwachte negatieve gevolgen van mensensmokkel zijn dusdanig ernstig dat dit criminele verschijnsel de komende jaren een **dreiging** vormt voor de Nederlandse samenleving.

1.9 Orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering

1.9.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek dat voor dit dreigingsbeeld is uitgevoerd in de eerste helft van 2016. De auteur van het onderzoeksrapport is Jessica de Jong, werkzaam bij de politie. De bronnen die zij bij het onderzoek heeft gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Orgaanhandel betreft het vrijwillig te koop aanbieden, daadwerkelijk verkopen of kopen van een orgaan. Belangrijk criterium daarbij is dat sprake moet zijn van een winstoogmerk. Orgaanhandel is in 1996 strafbaar gesteld in de Wet op de orgaandonatie (artikel 32) omdat door het winstoogmerk de vrijwilligheid van de donor niet kan worden gewaarborgd. Indien sprake is van dwangmiddelen die tegen een patiënt of donor worden gebruikt, betreft het mensenhandel met het oogmerk van orgaanverwijdering (hierna kortweg aangeduid als 'mensenhandel', tenzij dat een goed begrip van de tekst bemoeilijkt). Onder mensenhandel valt ook het misbruik maken van een kwetsbare positie van een patiënt of donor die heeft ingestemd met de koop of verkoop van een orgaan. Mensenhandel met het oogmerk van orgaanverwijdering is in 2005 strafbaar gesteld in het Wetboek van Strafrecht (artikel 273f).

Omdat orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering niet in eerdere edities van het Nationaal dreigingsbeeld aan bod kwamen, kijken we iets verder terug dan 2012. We kijken naar ontwikkelingen die zich hebben voorgedaan sinds mensenhandel met het oogmerk van orgaanverwijdering strafbaar werd gesteld in 2005.

1.9.2 Ontwikkelingen in aard en omvang sinds 2005

De vraag naar de omvang van orgaanhandel en mensenhandel laat zich lastig beantwoorden. Dat heeft een aantal oorzaken. Vaak heeft de handel op het eerste gezicht de schijn van legaliteit en blijven de criminele activiteiten die erachter schuilgaan verborgen. Daarnaast bemoeilijken het internationale karakter van de delicten en de vertrouwelijkheidsbeginselen van het medisch beroep het ontdekken en onderzoeken van misstanden. Ook maken de slachtoffers zich vaak niet bekend, onder andere uit angst voor strafrechtelijke vervolging of uitzetting (in geval van illegaliteit), uit wantrouwen richting de politie of door praktische belemmeringen, zoals taalproblemen of gebrek aan kennis over het bestaan van hulpverlenende instanties. Tevens krijgen orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering weinig aandacht van handhavings- en opsporingsinstanties. Dat hangt voor een groot deel samen met een gebrek aan kennis over deze vormen van criminaliteit. Dit alles leidt ertoe dat signalen niet altijd worden herkend, gemeld en/of geregistreerd. Het komt dan ook zelden tot opsporingsonderzoeken.

Sinds 2005 zijn er in totaal vijf meldingen geweest van mensenhandel met het oogmerk van orgaanverwijdering in Nederland. Daarvan kwamen er drie binnen bij CoMensha (een organisatie die zich inzet voor slachtoffers van mensenhandel) en twee bij de politie. Overeenkomst tussen de meldingen is dat ze alle vijf betrekking hebben op de gedwongen donatie van een nier waarbij de aangever vóór het verwijderen van de nier kans zag te ontsnappen. Geen van de meldingen resulteerde in een opsporingsonderzoek. Er bleken onvoldoende aanwijzingen voor mensenhandel of er ontbraken concrete opsporingsindicaties.

Voor een andere indicatie van de omvang is gebruikgemaakt van de bevindingen uit een enquête die in 2013 onder 241 medisch professionals in Nederland is afgenomen. In die enquête stelden zes professionals een vermoeden van mensenhandel te hebben gehad in de afgelopen vijf jaar en gaven drie professionals aan dat de donor hun had verteld te worden gedwongen een orgaan af te staan. In de enquête is ook gevraagd naar het voorkomen van orgaanhandel. Zeventien respondenten zagen in de afgelopen vijf jaar een patiënt van wie ze vermoedden dat zij in Nederland een nier kochten. Dertien respondenten vertelden te vermoeden dat donoren een nier hadden verkocht aan een patiënt in Nederland. Of en in welke mate daarbij sprake is geweest van dwang, wat feitelijk aangemerkt kan worden als mensenhandel met orgaanverwijdering als oogmerk, is niet te zeggen.

Door de jaren heen zijn, vooral in de media, meerdere incidenten gerapporteerd waarbij individuen in Nederland zich op websites aanbieden om tegen een vergoeding een orgaan af te staan. Onder het voorwendsel van altruïsme trachten deze aanbieders een orgaan te verkopen voor bedragen die variëren van enkele tienduizenden tot honderdduizenden euro's. Als gevolg van de gerapporteerde incidenten zoekt de Inspectie voor de Gezondheidszorg, verantwoordelijk voor de Wet op de orgaandonatie, sinds eind 2014 eens in de twee maanden handmatig naar online advertenties waarin een orgaan te koop wordt aangeboden. Dat heeft tot nu toe geresulteerd in vier processen-verbaal die geseponeerd

zijn in verband met de geestelijke gezondheidstoestand van de adverteerder, onvoldoende bewijs dat de advertentie door de verdachte is geplaatst of onvoldoende bewijs voor een financieel motief. Tot op heden heeft in Nederland, in 2015, één vervolging plaatsgevonden voor deze verschijningsvorm van orgaanhandel, waarbij de verdachte werd vrijgesproken.

Op grond van de geregistreerde meldingen van orgaanhandel en mensenhandel bij handhavings- en opsporingsdiensten, de enquêteresultaten en de gerapporteerde incidenten kan worden geconcludeerd dat orgaanhandel in Nederland voorkomt, zij het vermoedelijk in geringe mate. Een link met de georganiseerde criminaliteit kon in Nederland niet worden vastgesteld. In buitenlands opsporingsonderzoek is zo'n link wel geconstateerd. Volgens experts vereisen de activiteiten die nodig zijn om mensenhandel met het oogmerk van orgaanverwijdering succesvol te laten verlopen goedgeorganiseerde criminele netwerken. Uit de internationale opsporingsonderzoeken blijkt dat patiënten en donoren uit EU-landen in andere landen betrokken zijn bij transplantaties die door criminele organisaties worden georganiseerd. Of hier ook Nederlandse patiënten bij betrokken zijn, is onbekend, maar die mogelijkheid is niet uit te sluiten. Elk jaar zijn er Nederlanders die zich naar aanleiding van het tekort aan donororganen voor transplantatie vervoegen op buitenlandse illegale orgaanhandelmarkten. Van de 241 medisch professionals die in 2013 werden bevraagd naar hun ervaringen met orgaanhandel, gaven 110 respondenten aan in de afgelopen vijf jaar patiënten te hebben behandeld die een niertransplantatie in het buitenland hadden ondergaan. Honderd hiervan behandelden patiënten die buiten de EU waren getransplanteerd.

1.9.3 Huidige gevolgen

De gevolgen voor de Nederlandse samenleving van orgaanhandel en mensenhandel bestaan overwegend uit de fysieke schade die Nederlandse patiënten lijden ten gevolge van onzorgvuldig uitgevoerde, waarschijnlijk door criminelen gefaciliteerde, orgaantransplantaties in het buitenland. Naar schatting gaat het elk jaar om enkele patiënten die uit het buitenland terugkeren met medische complicaties. Op basis van het aantal aangiften beperkt het aantal donoren dat in Nederland slachtoffer wordt van mensenhandel met het oogmerk van orgaanverwijdering zich eveneens tot hooguit enkele personen per jaar. Bij mensenhandel met het oogmerk van orgaanverwijdering gaat het om een ernstige inbreuk op de lichamelijke integriteit. De gevolgen voor de Nederlandse samenleving op financieel gebied en voor wat betreft overlast en ondermijning zijn beperkt.

1.9.4 Verwachtingen

Door toegenomen internationale aandacht voor orgaanhandel en mensenhandel wordt verwacht dat het aantal registraties in de nabije toekomst, nationaal en internationaal, toeneemt. Het werkelijke aantal gevallen van deze vormen van handel zal waarschijnlijk ook toenemen. Dat komt door het aanhoudende tekort aan organen, de toenemende vraag naar organen en de groeiende welvaartsongelijkheid in de wereld. Internationale statistieken wijzen uit dat mensenhandel met het oogmerk van orgaanverwijdering een opkomende

trend is. Onbekend is welke rol de Nederlandse vraag- en aanbodmarkt voor illegale orgaantransplantaties daarbij inneemt.

Een toekomstige inwerkingtreding van de nieuwe wet op de orgaandonatie – die nog door de Eerste Kamer moet worden aangenomen – kan ertoe leiden dat wachtlijsten voor organen gedeeltelijk gaan afnemen. Door de wetswijziging zullen, naar verwachting, meer overleden donoren beschikbaar komen. Of de wet er komt, is op dit moment ongewis. Een eventuele invoering van de wet kan echter niet voorkomen dat patiënten die niet voor orgaanwachtlijsten in aanmerking komen en dus afhankelijk zijn van een levende donor, mogelijk hun toevlucht zoeken tot de illegale orgaanhandel.

Vluchtelingen die zich in de huidige asielstroom richting West-Europa en Nederland begeven, vormen een bijzondere risicogroep voor orgaanhandel en mensenhandel, omdat zij zich veelal in een kwetsbare positie bevinden. In Nederland en in andere Europese landen zijn er signalen dat (illegale) migranten worden uitgebuit als orgaandonor.

Sinds enkele jaren is er in Nederland discussie over de wenselijkheid om orgaandonoren financieel te compenseren om het aantal levende donoren te doen toenemen. In die discussie spelen overwegend ethische overwegingen een rol. Critici betogen dat het commercialiseren van het menselijk lichaam onvermijdelijk tot uitbuiting leidt. Een en ander heeft tot op heden nog niet tot besluitvorming geleid.

De verwachte gevolgen van orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering liggen in het verlengde van de huidige gevolgen. Ook in de komende vier jaar bestaan de verwachte gevolgen voor de Nederlandse samenleving vooral in fysieke schade voor de naar schatting enkele Nederlandse patiënten die jaarlijks uit het buitenland terugkeren met medische complicaties. Ook het aantal donoren met traumatische ervaringen naar aanleiding van slachtofferschap van mensenhandel zal naar verwachting beperkt blijven tot enkele personen per jaar. Al met al wordt verwacht dat het aantal gevallen van orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering in Nederland beperkt zal blijven.

1.9.5 Kwalificatie van dreiging

Jaarlijks sterven in Nederland circa tweehonderd patiënten doordat ze niet in aanmerking komen voor de wachtlijst, via de wachtlijst te lang op een overleden donor moeten wachten of doordat er geen orgaan van een levende donor beschikbaar komt. Hierdoor ontstaat een vraag die niet altijd langs de reguliere weg kan worden vervuld. Er is, met andere woorden, een markt voor de illegale commerciële handel in organen en mensenhandel. Hoewel de omvang zich moeilijk laat meten, lijkt de handel in Nederland op kleinschalig niveau plaats te vinden. In de afgelopen tien jaar is er een handvol meldingen geweest van orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering. Dat zal naar verwachting ook in de komende vier jaar zo blijven. Orgaanhandel en mensenhandel met het oogmerk van orgaanverwijdering vormen voor de Nederlandse samenleving derhalve **geen concrete dreiging**.

1.10 Illegale handel in vuurwapens en explosieven

1.10.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *De illegale handel in vuurwapens en explosieven. Deelrapport Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar vuurwapens en explosieven dat in de eerste helft van 2016 is uitgevoerd voor dit dreigingsbeeld. De auteurs van het onderzoeksrapport zijn Jorno Jon-Ming en Angelique Pronk, beiden werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017*.
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Het onderzoek naar vuurwapens en explosieven heeft betrekking op de hele logistieke keten binnen de illegale markt van vraag en aanbod. De vraag naar wapens bepaalt de aard en omvang van het aanbod. Daarom zijn ontwikkelingen in het *gebruik* van vuurwapens en explosieven ook onderwerp van onderzoek.

De focus ligt op nieuwe ontwikkelingen in vraag en aanbod sinds 2012 die een aantoonbare relatie met Nederland of Nederlandse verdachten hebben. Het onderzoek beperkt zich tot de conventionele wapens, de scherpschietende vuurwapens (inclusief omgebouwde gas- en alarmvuurwapens en schietpennen) en explosieven. Ook de handel in munitie en onderdelen en accessoires voor vuurwapens komt aan de orde. Niet-conventionele wapens, de zogenoemde massavernietigingswapens, blijven buiten beschouwing.

1.10.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Vraag

Sinds 2012 is een verdere toename in het gebruik van en de vraag naar automatische vuurwapens zichtbaar. In het vorige dreigingsbeeld werd de toename vooral gekoppeld aan een verharding in het hennepmilieu. Tot dan toe beperkte het gebruik van deze vuurwapens zich tot enkele incidenten, onder andere bij liquidaties en bij overvallen op gelddepots. Verwacht werd dat liquidaties gewelddadiger zouden worden en dat de gesignaleerde verharding in de toekomst ook op andere criminele markten te zien zou zijn. Die verwachtingen zijn uitgekomen.

Tussen 2012 en 2015 is een toenemend aantal liquidaties en liquidatiepogingen met automatische vuurwapens uitgevoerd. In eerste instantie concentreerden die zich in Randstedelijk gebied, maar daarna breidden die zich uit naar de rest van Nederland. Veel liquidaties vinden in het openbaar en overdag plaats en soms worden daarbij meerdere automatische vuurwapens gebruikt. Criminelen schromen niet om politie en burgers ermee op afstand te houden.

Aan veel liquidaties liggen conflicten in drugshandel en -smokkel ten grondslag. In de afgelopen jaren zijn daders en dadergroepen in beeld gekomen die zich toeleggen op het plegen van liquidaties met automatische vuurwapens.

Automatische vuurwapens worden de laatste jaren steeds vaker gezien bij de uitvoering van allerlei criminele activiteiten. Ze zijn bijvoorbeeld gebruikt bij het op afstand houden van omwonenden bij een plofkraak, bij een overval op een juwelier, bij bedreiging van een misdaadjournalist (door op zijn huis en auto te schieten) en bij het beschieten van een coffeeshop.

Verklaringen voor het toenemende en uiteenlopende gebruik van automatische vuurwapens worden onder andere gezocht in de precedentwerking die uitgaat van het gebruik. Criminelen willen niet achterblijven op gespannen markten waar criminele groepen zakendoen en elkaar te vuur en te zwaard beconcurreren als dat nodig is. Ook zou sprake zijn van *target hardening*. Criminelen beveiligen zich beter, onder andere met kogelwerende vesten en gepantserde auto's. 'Succesvolle' liquidaties vereisen dan ook meer vuurkracht.

Aanbod

In Europa is het terugbouwen van gedeactiveerde handvuurwapens en automatische vuurwapens, ook wel recyclen genoemd, op dit moment een van de meestgebruikte methoden om vuurwapens in het illegale circuit te brengen. In Nederland bestaat de laatste jaren een relatief groot aanbod van gerecyclede vuurwapens, vooral uit Slowakije. Naar verluidt zijn er in Slowakije vijftien wapenverkopers die gedeactiveerde vuurwapens verkopen. Deze vuurwapens zijn minimaal gedeactiveerd en in een handomdraai om te bouwen tot scherpschietende wapens. Waar de vuurwapens worden gereactiveerd, is niet altijd bekend. Soms blijkt uit opsporingsonderzoek dat reactivatie in Nederland moet hebben plaatsgevonden.

Sinds 2012 zijn er verspreid over heel Nederland bijna tweehonderd Slowaakse gerecyclede vuurwapens aangetroffen. Het gaat om AK-47-gelijkende aanvalsgeweren van het merk CZ, Skorpion-machinepistolen en pistolen van Glock, CZ en Grand Power. Bij verschillende grote wapenvondsten, liquidatieonderzoeken en kleinere inbeslagnames komt steeds dezelfde Slowaakse wapenverkoper naar voren. Die heeft in de afgelopen jaren meer dan 10.000 gedeactiveerde vuurwapens in heel Europa verkocht. Op basis van opsporingsonderzoek wordt geschat dat er in de jaren 2014 en 2015 ten minste een paar honderd, vooral automatische, vuurwapens uit Slowakije naar Nederland zijn gekomen.

Inmiddels is de handel in gedeactiveerde vuurwapens uit Slowakije bemoeilijkt door het aanscherpen van de wet in 2015. Dit laat onverlet dat het nog steeds mogelijk is om gedeactiveerde vuurwapens aan te schaffen die, zij het met iets meer moeite dan voorheen, relatief gemakkelijk zijn te reactiveren. Daarbij komen dezelfde vuurwapenverkopers in beeld als voorheen. Bovendien richten de Slowaakse wapenwinkels zich ook op de verkoop van vrij verkrijgbare Flobert-wapens, vuurwapens met een geringe vuurkracht en een klein kaliber.

In de eerste maanden van 2016 zijn deze wapens, die vergelijkbaar zijn met de Walther P99-pistolen, een aantal keer in Nederland aangetroffen, onder andere afkomstig uit Slowakije en Duitsland.

Hoewel geen toe- of afname zichtbaar is, blijkt uit politiesystemen en recente opsporingsonderzoeken dat de markt voor de ombouw van gas- en alarmpistolen tot scherpschietende vuurwapens aanzienlijk is. Drie criminele samenwerkingsverbanden zouden de afgelopen twee jaar ettelijke honderden alarmpistolen van Turkse makelij in Bulgarije hebben gekocht. De koop vond plaats via internet, de assemblage en ombouw in Nederland. De vuurwapens werden voor 30 euro ingekocht en voor het tienvoudige doorverkocht. Anno 2016 zijn de alarmpistolen nog steeds via Bulgaarse webshops verkrijgbaar. Daarnaast worden Nagant-gasrevolvers uit België regelmatig in Nederland aangetroffen. Die waren daar tot voor kort vrij verkrijgbaar en dat verklaart het relatief frequente voorkomen ervan in Nederland.

Duitsland en België zijn voorname bronlanden voor vuurwapens bestemd voor de Nederlandse markt. Dat blijkt uit rechtshulpverzoeken. Meer dan de helft van de ruim 1200 rechtshulpverzoeken tussen Nederland en België (451) en Duitsland (192) heeft betrekking op de handel in vuurwapens en explosieven. Bovendien zien we in verschillende opsporingsonderzoeken reisbewegingen van vuurwapenhandelaars naar België en verschillende partijen munitie afkomstig uit Duitsland.

Het samenstellen van scherpschietende vuurwapens uit vuurwapenonderdelen is een relatief nieuwe ontwikkeling. Zo bestelt men bijvoorbeeld in Oostenrijk de kast van het vuurwapen en in de Verenigde Staten het binnenwerk. Bestelling geschiedt via webshops of via het darknet. Door de gescheiden bestelprocedure is vaak geen verlof benodigd. Transacties voltrekken zich deels via TOR-netwerken. Het in elkaar zetten van de vuurwapens vereist weinig expertise. Tot begin 2016 zijn er in Nederland 31 ‘samengestelde’ Glocks aangetroffen. Ook is een aantal ontvangers van vuurwapenonderdelen geïdentificeerd.
Inmiddels is de internationale verzending van vuurwapenonderdelen uit de Verenigde Staten verboden, maar er zijn verschillende manieren waarop wapenhandelaars dat verbod omzeilen. Amerikaanse webshops verschepen onderdelen door zich voor te doen als een andere afzender of door *parcel forwarding services* te gebruiken waarbij onderdelen als zogenaamd andere goederen worden verstuurd. Ook worden onderdelen verstuurd via kennissen en vrienden.

De Balkanlanden zijn onverminderd bronlanden van illegale vuurwapens in Nederland, omdat er na de burgeroorlog in voormalig Joegoslavië nog steeds honderdduizenden vuurwapens voorradig zijn. In Nederlandse opsporingsonderzoeken en rechtshulpverzoeken komen met name Kroatië, Bosnië en Herzegovina en Servië naar voren als bronlanden van vuurwapens. Recent kwamen Kroatische en Bosnische wapenhandelaars in beeld. Zij handelden in vuurwapens, automatische vuurwapens, handgranaten, munitie en raketwer-

pers. Vermoedelijk is wapensmokkel vanuit Kroatië populair, omdat het land bij de Europese Unie hoort en goederen vrij de grens kunnen passeren.
Sinds 2012 wordt in Nederland een nieuw zelfbouwwapen aangetroffen: de pistoolmitrailleur van het merk R9 arms Corp. U.S.A., vermoedelijk van Kroatische makelij. Tot begin 2014 werden deze mitrailleurs alleen in Nederland aangetroffen. Nadien zijn er inbeslagnames geweest in Duitsland, België, het Verenigd Koninkrijk en Frankrijk. Daarbij bestond steeds een link naar Nederland.

De diefstal van legale vuurwapens vormt ook een bron van illegale vuurwapens. In 2013 ging het om ruim 360 vuurwapens, in 2014 waren het er ruim 300. Diefstal vindt plaats bij verlofhouders of erkenninghouders, thuis of op de schietvereniging, bij legale vuurwapenhandelaars of bij wapenwinkels.

Smokkelmethoden

De bestelling van vuurwapens via internet en het gebruik van post- en koeriersdiensten heeft sinds 2012 een grotere vlucht genomen. Bestellingen zijn sinds 2012 niet meer voorbehouden aan jongeren en personen die nog niet het niveau van zware crimineel hebben, maar worden ook gedaan door kleine én grote spelers in het criminele circuit. Bestellingen vinden plaats via reguliere webwinkels en via het darknet. Onbekend is hoe de handel via internet zich qua omvang verhoudt tot de reguliere face-to-facehandel.
Het is relatief eenvoudig om binnen de EU een vuurwapen op internet te bestellen en via post- en koeriersdiensten te laten afleveren. Dat geldt vooral voor gas- en alarmvuurwapens. Er vindt nauwelijks controle plaats op intracommunautaire goederen. De smokkel van vuurwapens en explosieven via postpakketten wordt soms gecombineerd met smokkel over de weg, als een soort risicospreiding. Opvallend is dat wapenhandelaars aan het einde van de smokkelketen met regelmaat gebruikmaken van particuliere opslagboxen.

Hoe munitie Nederland bereikt en waar deze vandaan komt, is, net als in 2012, onbekend. Wel weten we uit recente opsporingsonderzoeken en inbeslagnames dat een deel van de munitie uit het legale circuit wegvloeit. Verlofhouders mogen per keer 10.000 patronen bij een erkenninghouder aanschaffen. De controle op aanschaf en bezit van munitie is beperkt. Verder worden grotere hoeveelheden munitie voor Kalasjnikovs aangetroffen dan voorheen het geval was. Dat past bij het beeld van de toenemende handel in en gebruik van deze automatische vuurwapens.

Betrokken personen en criminele samenwerkingsverbanden

Een relatief kleine groep vuurwapenhandelaars importeert op grote schaal vuurwapens in Nederland. Velen zijn al jaren actief en kennen elkaar direct of indirect. Zij vormen een netwerk binnen Nederland en van sterke concurrentie of daaruit voortvloeiend geweld is geen sprake. Bij deze groep handelaars wordt relatief vaak een groot en divers wapenarsenaal aangetroffen. Het gaat om handvuurwapens, semiautomatische vuurwapens, automatische vuurwapens, antitankwapens en handgranaten. Bij de import spelen de contacten

van deze spelers met hun buitenlandse families of gemeenschappen een grote rol. In het vorige dreigingsbeeld werd gesproken over importeurs met Turkse en Portugese connecties, nu gaat het vooral om importeurs die connecties hebben met landen zoals Polen, Kroatië, Slowakije en, in mindere mate, de Antillen.

Er is weinig zicht op personen die na een wapenimport de tussenhandel verzorgen. Vaak blijft onduidelijk hoe een vuurwapen bij een organisatie of eindgebruiker terechtkomt. In opsporingsonderzoek worden bewoners van woonwagenkampen, leden van outlaw motorcycle gangs (OMG's), criminele groeperingen van Antilliaanse of voormalig-Joegoslavische origine en doorgegroeide criminele jeugdgroepen in verband gebracht met de tussenhandel. De doorgegroeide jeugdgroepen houden zich ook bezig met de handel in omgebouwde gas- en alarmpistolen en het plegen van liquidaties.
Naast traditionele criminele groepen zijn er groepen bij de tussenhandel betrokken waarvan de leden tot een breder netwerk behoren en een gelegenheidscoalitie vormen. Na de import dragen zij zorg voor de verdere afzet van de vuurwapens in Nederland. De groepsleden weten elkaar gemakkelijk te vinden, onder andere door het gebruik van digitale berichtendiensten, waaronder WhatsApp. Ook bij het 'leasen' van vuurwapens helpt het als je elkaar gemakkelijk kunt bereiken. Tegenwoordig worden vuurwapens vaker geleased, vooral door straatbendes.

Veel samenwerkingsverbanden die in wapens handelen, houden zich ook met andere vormen van criminaliteit bezig zoals de handel in verdovende middelen en het plegen van liquidaties.

Het lijkt erop dat kopers van vuurwapens zich steeds vaker laten bedienen door meerdere aanvoerlijnen, dit in tegenstelling tot de bevinding uit het vorige dreigingsbeeld. Toen werd geconcludeerd dat ieder samenwerkingsverband zijn eigen wapenleverancier heeft. Tegenwoordig beschikken sommige groeperingen die een wapen nodig hebben over contacten met verschillende aanbiedende partijen waarmee zij afwisselend zaken kunnen doen. Het gaat bijvoorbeeld om Antilliaanse groeperingen en groeperingen met relatief jonge verdachten. In de wapenarsenalen van deze groeperingen worden vaak vuurwapens van verschillende leveranciers aangetroffen.

Een nieuwe ontwikkeling is het werken met *parcel companies*. Vuurwapenhandelaars zetten deze bedrijven in als tussenschakel om pakketten vuurwapens vanuit de Verenigde Staten onherkenbaar door te sturen naar de uiteindelijke ontvanger. Door het gebruik van de parcel companies zijn vuurwapens moeilijker te ontdekken voor handhavings- en opsporingsdiensten. Ook nieuw is de inzet van *straw purchasers* in de Verenigde Staten. Het gaat om Amerikaanse burgers die in de Verenigde Staten vrijelijk een wapen kunnen kopen en dat namens vuurwapenhandelaars in Nederland doen. Zij sturen de vuurwapens naar Nederland via parcel companies.

Facilitatoren die geen onderdeel uitmaken van de groep vuurwapenhandelaars zien we vooral in de uitvoering van technische klussen, zoals het reactiveren van vuurwapens of het produceren van geïmproviseerde explosieve constructies – ook wel bekend als *Improvised Explosive Devices* (IED's) – voor het uitvoeren van plofkraken.

Omvang

Door het ontbreken van bruikbare bronnen is het niet mogelijk landelijk inzicht te geven in de ontwikkeling van de omvang van de vuurwapenhandel. Daarom is er in het onderzoek ten behoeve van dit dreigingsbeeld voor gekozen vier politie-eenheden te bevragen die de inbeslagnames van vuurwapens sinds 2012 op redelijk eenduidige en consciëntieuze wijze hebben geregistreerd. Het gaat om twee Randstedelijke politie-eenheden (Amsterdam en Rotterdam) en twee niet-Randstedelijke politie-eenheden (Zeeland-West-Brabant en Oost-Brabant).

In Amsterdam en Rotterdam zien we de laatste jaren een stijgende trend in het aantal in beslag genomen automatische vuurwapens. Het gaat vooral om machinepistolen en machinegeweren. Ook in Oost-Brabant en Zeeland-West-Brabant worden *overall* iets meer automatische vuurwapens (vooral machinepistolen) in beslag genomen, ook al is het verloop van inbeslagnames daar door de jaren heen grilliger. In die eenheden kunnen we niet spreken van een stijgende trend in het aantal in beslag genomen automatische vuurwapens. In de omvang van de handel in andersoortige wapens zien we geen noemenswaardige verschuivingen.

De prijzen van vuurwapens zijn door de jaren heen redelijk stabiel. Opmerkelijk is dat automatische machinepistolen nauwelijks duurder zijn dan semiautomatische pistolen. Aanvalswapens zoals Kalasjnikovs zijn soms lager geprijsd dan pistolen, terwijl de oorspronkelijke 'winkelwaarde' van Kalasjnikovs doorgaans hoger is dan die van pistolen. Deze prijsontwikkeling wijst op een groot aanbod van automatische vuurwapens.

Door het veelvuldig aantreffen van automatische vuurwapens registreert de politie sinds 2015 in beslag genomen munitie die onder andere gebruikt wordt in Kalasjnikovs. Eind 2015 werden in 36 verschillende opsporingsonderzoeken bijna vijfduizend stuks munitie aangetroffen.

Ontwikkelingen in aard en omvang van de illegale handel in explosieven

Voor ontwikkelingen die betrekking hebben op de handel in en het gebruik van explosieven kijken we naar commerciële springstoffen, militaire explosieven, zelfgemaakte explosieve stoffen en geïmproviseerde explosieve constructies (IED's).

Commerciële springstoffen, zoals TNT, PEP500 en PETN, worden incidenteel aangetroffen bij onderzoeken naar plofkraken, liquidaties of aanslagen. Het gaat dan om hoeveelheden van een paar honderd gram tot bijna 2 kilogram. Semtex wordt in Nederland vrijwel niet aangetroffen.

De handel in militaire explosieven gaat vaak hand in hand met de handel in illegale vuurwapens. Als militaire explosieven bij partijen illegale vuurwapens worden aangetroffen, gaat het meestal om handgranaten en antitankwapens. Sinds 2012 kwamen in totaal 41 incidenten met handgranaten aan het licht. Qua omvang lijkt het gebruik van en de handel in militaire explosieven niet te verschillen ten opzichte van 2012.

De op dit moment meest voorkomende zelfgemaakte explosieve stof is TATP. In Europa wordt deze stof veelvuldig aangetroffen bij terroristische aanslagen waarbij IED's gevuld met TATP veel slachtoffers maken. In Nederland komt het gebruik van TATP (of het werken met grondstoffen waaruit TATP kan worden vervaardigd) in een handvol opsporingsonderzoeken voor. Zelfgemaakte explosieve stoffen, zoals TATP, worden meestal verwerkt in IED's die gebruikt worden bij plofkraken en liquidaties.
Een recente ontwikkeling is dat er een alternatief voor TATP in de maak is, namelijk APAN (*Acetone Peroxide Ammonium Nitrate*). Deze stof lijkt in opmars omdat ze in het gebruik iets minder onbetrouwbaar is dan TATP.

Bestanddelen uit illegaal vuurwerk worden steeds vaker gebruikt bij het vervaardigen van explosieven. De kwaliteit en kracht van illegaal vuurwerk is in de loop der jaren exponentieel verhoogd. Flitspoeders uit *flashbangers* bijvoorbeeld zijn inmiddels net zo krachtig als springstof en worden daarom in toenemende mate verwerkt in IED's, zoals pijpbommen. Sinds 2012 zijn van de twaalf aangetroffen IED's er vier geproduceerd uit illegaal vuurwerk.

Samenvattend kunnen we stellen dat in de aard en omvang van de fabrieksmatige commerciële en militaire explosieven weinig noemenswaardige ontwikkelingen zichtbaar zijn. De grootste bedreiging voor de toekomst gaat uit van de steeds veranderende productie in IED's op basis van zelfgemaakte explosieven en illegaal vuurwerk. Regelgeving met betrekking tot precursoren die geschikt zijn voor de productie van zelfgemaakte explosieve stoffen kan niet voorkomen dat grondstoffen alsnog illegaal verkrijgbaar blijven. Bovendien bieden de flitspoeders uit illegaal vuurwerk een bruikbaar alternatief.

1.10.3 Huidige gevolgen

Bij de bespreking van de gevolgen ligt de nadruk op gevolgen die voortvloeien uit het gebruik van vuurwapens en explosieven. De illegale handel zelf levert namelijk weinig merkbare schade voor de samenleving op, terwijl door het gebruik – dat intrinsiek verbonden is met de handel in wapens – jaarlijks vele slachtoffers vallen.

In de afgelopen vier jaar varieert het aantal doden door vuurwapengeweld jaarlijks tussen de 35 en 58. In 2015 vielen er 41 doden door vuurwapengeweld. Onder hen bevinden zich ten minste vier slachtoffers van een vergismoord, omdat er sprake bleek van persoonsverwisseling. Het jaarlijkse aantal gewonden wordt geschat tussen de 150 en 200.

Jaarlijks lopen naar schatting honderden mensen psychische schade op ten gevolge van vuurwapengeweld of dreiging daarmee. Het gaat onder andere om slachtoffers en getuigen van straatroven en overvallen waar vuurwapens aan te pas komen. Dat zijn er ongeveer 900 per jaar. Daar komen slachtoffers en getuigen van openlijke geweldpleging, woningovervallen, afpersing en moord en doodslag bij. Bij liquidaties in de openbare ruimte ondervinden omstanders een traumatische ervaring, in het bijzonder als daarbij sprake is van excessief geweld door gebruik van automatische vuurwapens.

Vuurwapengeweld in het algemeen en van automatische wapens in het bijzonder, is strijdig met het geweldsmonopolie van de overheid en daardoor ondermijnt het de rechtsorde. In de samenleving leidt dat tot maatschappelijke onrust. Liquidaties versterken bij burgers heersende gevoelens van angst en onveiligheid. Politieambtenaren kampen met vergelijkbare gevoelens. Hun rol als hoeders van de rechtsstaat staat onder druk als criminelen (automatische) vuurwapens gebruiken. Daarmee is het gezag van de rechtsstaat in het geding.
Ondermijning in de vorm van verweving van onder- en bovenwereld zien we in de casuïstiek waarbij personen in de legale schietsport zakendoen met illegale vuurwapenhandelaars. Het gaat dan om het weglekken van legale munitie naar criminelen.
Minder in het oog springende gevolgen uiten zich vooral in de vorm van overlast. Jaarlijks ondervinden honderden personen en bedrijven hinder door afzettingen en ontruimingen na incidenten met vuurwapens en explosieven.

1.10.4 Verwachtingen

Voor de periode 2017-2021 voorzien we geen grote verschuivingen in de vraag. Vuurwapens zijn duurzame goederen en gezien de relatief lage prijzen en grote voorraden wapens in Europa is geen schaarste te verwachten. Recente inbeslagnames, tapgesprekken en analyses van gegevensdragers geven aanleiding te verwachten dat de vraag naar automatische vuurwapens de komende periode zal blijven. Op sommige criminele markten is het gebruik ervan gemeengoed geworden.

De liquidaties uit de afgelopen jaren kunnen de aanleiding zijn voor nieuwe liquidaties in de aankomende jaren. Represailles voor eerdere liquidaties kunnen het geweld met automatische vuurwapens aanwakkeren. Dit doet verwachten dat de vraag naar automatische vuurwapens de komende jaren in stand blijft. In het bijzonder de vraag naar aanvalswapens zoals de Kalasjnikov en machinepistolen zoals de Skorpion blijft naar verwachting groot.

De terroristische aanslagen in Europa hebben de afgelopen jaren geleid tot meer aandacht voor de handel in vuurwapens en explosieven. Vanuit de EU worden strengere regels voorbereid ten aanzien van het aankopen, bezitten en deactiveren van vuurwapens. Ook ligt er een actieplan ter bestrijding van de illegale handel en het gebruik van vuurwapens en explosieven. Gelet op de doorlooptijd van Europese besluitvorming zal het resultaat van deze inspanningen op de kortere termijn naar verwachting gering zijn. Concrete uitwerking van dit soort initiatieven vraagt om harmonisatie van wet- en regelgeving binnen de EU. Dat is

voor veel lidstaten een struikelblok. Verwacht wordt dan ook dat nieuwe Europese wet- en regelgeving om het aanbod van vuurwapens uit landen als België, Duitsland, Kroatië, Slowakije en Bulgarije tegen te houden, voorlopig niet geëffectueerd zal worden. Hetzelfde geldt voor het aanbod van vuurwapens en onderdelen uit de Verenigde Staten.

Ondanks nationale en EU-brede inspanningen om de handel in precursoren voor de productie van zelfgemaakte explosieve stoffen tegen te gaan, zullen deze de komende jaren naar verwachting makkelijk verkrijgbaar blijven. Dat is omdat er op de doorvoer van postpakketten weinig controle is en het handhavingsbeleid daarop veel ruimte laat. Ook verschillen in wet- en regelgeving tussen landen belemmeren de aankoop van precursoren in het buitenland niet. Daarnaast zien we ontwikkelingen waaruit blijkt dat precursoren vervaardigd worden uit nieuwe grondstoffen die (nog) niet als verdacht zijn aangemerkt.
Verwacht wordt ook dat illegaal vuurwerk zoals *flashbangers* en de flitspoeders die eruit ontsloten worden, in toenemende mate gebruikt zullen worden voor de productie van IED's. Die stoffen hebben, vergeleken met de handel in precursoren en explosieve (grond)stoffen, vooralsnog minder aandacht van politie en justitie.

Vanuit nieuwe conflictgebieden, zoals Oekraïne, Syrië, Mali en Libië wordt aanvoer van vuurwapens verwacht. Onbekend is om hoeveel wapens het zal gaan. Ook uit Rusland wordt aanvoer van wapens verwacht. Dat komt door de geplande afschrijving van 4 miljoen Kalasjnikovs door het Russische leger. We verwachten dat een onbekend deel daarvan op de illegale markt in Nederland zal belanden.

Vuurwapengeweld leidt tot ongeveer 150 tot 200 slachtoffers per jaar, van wie tussen de 35 en 60 dodelijk. Verwacht wordt dat het aantal slachtoffers door het gebruik van automatische vuurwapens ten minste gelijk blijft en mogelijk zelfs stijgt door aanhoudende spanningen in de verdovendemiddelenhandel of door gebruik van deze vuurwapens bij een terroristische aanslag. De verwachte ontwikkeling in het aantal slachtoffers hangt ook samen met de toegenomen beschikbaarheid van deze vuurwapens in Nederland.

1.10.5 Kwalificatie van dreiging

Door de illegale handel in vuurwapens en explosieven komen criminelen en terroristen in het bezit van deze wapens. Vooral vuurwapens worden in Nederland gebruikt bij uiteenlopende criminele activiteiten en ingezet voor criminele afrekeningen. Jaarlijks resulteert dat in Nederland in tientallen doden, honderden gewonden en honderden getraumatiseerden. Schietincidenten hebben een grote impact op de samenleving; in het bijzonder het schieten met automatische wapens in woonwijken en publieke gelegenheden veroorzaakt veel ophef, onrust en gevoelens van onveiligheid. Door openlijk en excessief geweldgebruik met vuurwapens wordt het gezag van de rechtsstaat aangetast omdat het geweldsmonopolie, dat bij de overheid rust, met voeten wordt getreden.

Het aantal aangetroffen commerciële springstoffen en militaire explosieven is klein en stabiel. Deze explosieven worden vooral gebruikt voor plofkraken. Het gebruik en de ontwikkeling van zelfgemaakte explosieve stoffen neemt de laatste jaren toe. In Nederland worden deze stoffen vooral verwerkt in IED's die gebruikt worden voor plofkraken en liquidaties. Flitspoeders uit illegaal vuurwerk worden gebruikt om pijpbommen mee te maken die veel schade veroorzaken.

Vooruitkijkend naar de komende vier jaar wordt verwacht dat de toegenomen vraag naar automatische vuurwapens verder doorzet. De harmonisatie van wet- en regelgeving in de EU-lidstaten op het gebied van vuurwapens laat op zich wachten. Er komt nieuwe aanwas van illegale vuurwapens uit conflictgebieden als Oekraïne, Syrië, Mali en Libië en ook de afschrijving van 4 miljoen Kalasjnikovs uit het Russische leger creëert illegaal aanbod. Een terroristische aanslag met automatische vuurwapens of explosieven blijft een reëel gevaar. Gelet op deze ontwikkelingen is de verwachting dat de gevolgen van de illegale handel in vuurwapens en explosieven minstens gelijk blijven aan de geschetste huidige gevolgen. Deze zijn dusdanig ernstig van aard dat de komende jaren sprake is van een **dreiging** voor de Nederlandse samenleving.

1.11 Kinderpornografie

1.11.1 Inleiding

In de loop van 2016 is ten behoeve van dit onderwerp een deelproject uitgevoerd onder de titel *Kinderpornografie. Nationaal dreigingsbeeld 2017-2021*. Daarvan is een (vertrouwelijke) rapportage gemaakt. De auteurs zijn Ben van Mierlo en Inge van Balen, die beiden werkzaam zijn bij de politie. De bronnen die zij daarbij gebruikt hebben, staan vermeld in het digitale *Bronnenboek NDB2017.*
De informatie die in deze paragraaf gepresenteerd wordt, is afkomstig uit het genoemde rapport. Een uitzondering moet gemaakt worden voor de afsluitende subparagraaf Kwalificatie van dreiging. De kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Het domein kinderpornografie is vanaf 2011/2012 geleidelijk uitgebreid naar de met kinderporno samenhangende internetgerelateerde zedendelicten zoals *grooming*. Feitelijk valt de afbakening tussen delicten die onder zeden vallen en delicten die onder de TBKK's (Teams Bestrijding Kinderporno en Kindersekstoerisme) vallen, beter te verduidelijken door een onderscheid te maken tussen delicten die alleen *hands-on* zijn geweest (= zeden) en niet op beeld zijn vastgelegd en delicten waarin (communicatie via) internet en beelden van seksueel misbruik (vastgelegd dan wel *streaming*) de hoofdmoot zijn (= kinderpornografie).
Het downloaden dan wel bezitten van kinderpornografie is een individuele handeling en zal daarom in mindere mate besproken worden.

1.11.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

Uit een analyse van politiedossiers van kinderpornozaken blijkt dat 8 procent van de verdachten in de onderzochte dossiers minderjarig is. De onderzoekers voeren als mogelijke verklaring hiervoor aan dat jongeren seksueel getinte foto's en video's van zichzelf en elkaar maken. In 2012 was 21 procent van de afbeeldingen die bij het Britse meldpunt CEOP (Child Exploitation and Online Protection Centre) binnenkwamen, door jongeren zelf geproduceerd materiaal. Jongeren zijn steeds vaker online en zij posten daarbij soms ook seksueel getinte foto's en filmpjes. Komen dergelijke afbeeldingen in verkeerde handen, dan kan dat leiden tot *sextortion*: het afdwingen van seksuele handelingen of afbeeldingen van slachtoffers, door te dreigen met de verspreiding van eerder verkregen beeldmateriaal. Europol signaleerde in 2015 een sterk groeiende trend op het gebied van sextortion van jongeren. In het algemeen kan gezegd worden dat de verdachten in de afgelopen jaren jonger zijn geworden.

De groei van het internet en andere technologische innovaties brengt met zich mee dat de opsporing in toenemende mate te maken heeft met verdachten die in grootschalige internationale kinderpornonetwerken kindermisbruik live streamen, of mensen chanteren met seksueel beeldmateriaal. We zien een verschuiving van individuele verdachten naar verdachten die binnen netwerken opereren. Een vorm van georganiseerde commerciële distributie van kinderpornografisch materiaal is bijvoorbeeld waargenomen via zogeheten *cyberlockers* of door gedeelde videolinks. Via een *pay-per-view-* of *pay-per-premiumservice*-constructie kunnen – tegen betaling – beelden van kindermisbruik worden gedeeld.

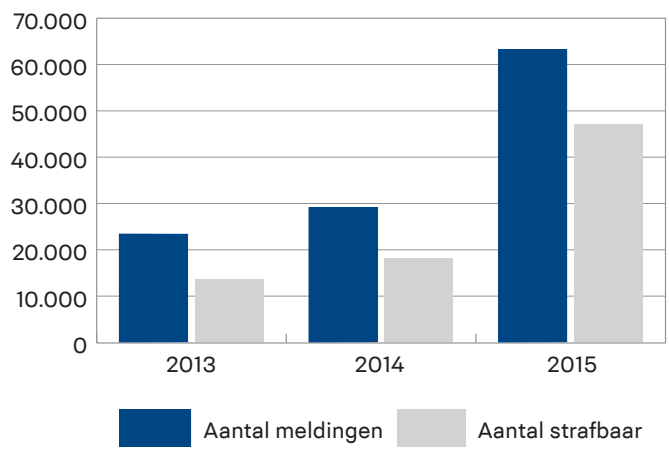
Hoewel steeds meer beeldmateriaal wordt verspreid via het TOR-netwerk, bestaat ook de indruk dat sommige gebruikers bewust (weer) gebruikmaken van P2P-netwerken (peer-to-peer) en daar toepassingen vinden om hun materiaal te verbergen en te verspreiden. Ook de steeds verder toenemende opslag in de cloud maakt het moeilijk te bepalen waar materiaal (juridisch en geografisch) digitaal is opgeslagen en om zicht te krijgen op de inhoud van dit materiaal. Omdat afschermingsmaatregelen en encryptie beter zijn geworden en meer waarborgen bieden tegen ontdekking, lijkt er minder schroom te bestaan om ook de ernstiger vormen van misbruik te delen.

Omvang

Bij het bespreken van de omvang, het aanbod van kinderpornografisch materiaal, kan de internationale component niet buiten beschouwing blijven. Door de rol die internet speelt bij de verspreiding van kinderporno, gaat het bijna per definitie om een internationaal probleem. Internet doet tijd en grenzen vervagen. De omvang van kinderpornografie is dan ook moeilijk vast te stellen. Ook het aandeel dat Nederland daarin heeft, is onduidelijk. Duidelijk is dat op internet vele miljoenen kinderpornografische afbeeldingen en video's staan. Recent onderzoek van Europol naar een van de grootste TOR-sites waarop kinderpornografisch materiaal werd gehost, toonde aan dat deze site, die twee jaar bestond, al meer dan 1,3 miljoen kinderpornografische afbeeldingen bevatte. Het TOR-netwerk groeit nog altijd. Steeds meer gebruikers schermen hun werkelijke identiteit af. Meer dan 80 procent van de sites op het

TOR-netwerk zou gerelateerd zijn aan pedofilie. Een FBI-onderzoek op TOR naar kinderporno heeft Europol meer dan 3000 zaken opgeleverd. Een van de kinderpornografische fora op deze TOR-omgeving had meer dan 215.000 leden.
Voor Nederland kunnen geen betrouwbare schattingen naar de omvang gedaan worden. De politieregistraties laten alleen een ondergrens zien. De indruk bestaat dat deze registraties betrouwbaarder zijn geworden sinds deze in een speciaal daarvoor ontwikkeld landelijk systeem worden gedaan. In de periode 2012-2015 werden 1986 verdachten aangehouden en werden 850 slachtoffers geïdentificeerd.
Een andere bron die iets zegt over de omvang is het Meldpunt Kinderporno op Internet. Dit meldpunt signaleert een grote stijging van het aantal meldingen. De grote toename wordt deels verklaard door een verandering in de manier van registreren. In 75 procent van de meldingen bleek het om strafbaar materiaal te gaan. Zie figuur 3.

Figuur 3. Aantal meldingen kinderpornografie 2013-2015



Volgens de overkoepelende organisatie waarvan het Meldpunt lid is (Inhope) stond Nederland in 2014 in de top 10 als het om landen gaat waar strafbaar materiaal wordt gehost (16%). Alleen in de Verenigde Staten (37%) en in Rusland (24%) werd in 2014 volgens Inhope meer strafbaar materiaal gehost. De absolute aantallen zullen volgens hen ook niet afnemen, maar alleen maar toenemen. Dit valt onder andere te verklaren door de toenemende wereldwijde internetdekking en de goede infrastructuur in Nederland.

Ook bij de politie is een sterke toename te zien van het aantal meldingen van strafbaar materiaal. Kwamen in 2013 nog circa 3500 meldingen bij het TBKK van de Landelijke Eenheid binnen, in 2015 is dit aantal toegenomen tot ruim 5500. Deze sterke toename wordt vooral veroorzaakt door meldingen van het National Center for Missing and Exploited Children (NCMEC) in de Verenigde Staten. (Hosting-)ondernemingen in de VS zijn verplicht om eventueel strafbaar materiaal dat zij op hun netwerk aantreffen te melden bij het NCMEC.

1.11.3 Huidige gevolgen

Tussen 2012 en 2015 zijn er door de TBKK's 850 slachtoffers geïdentificeerd in kinderpornozaken. Duidelijk is dat het dark number bij dit delict erg hoog is. Seksueel misbruik speelt zich vaak af binnen de familiesfeer. Uit onderzoek van de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen uit 2016 blijkt dat van de veroordeelde daders 36 procent een familielid van het slachtoffer is. Bijna een kwart van de daders is een ouder, broer of stiefbroer. In 13 procent gaat het om tweedelijns familie. Slechts in 7 procent van alle gevallen was de dader een volstrekt vreemde. Dit brengt met zich mee dat het delict vaak niet wordt aangegeven bij de autoriteiten. Psychisch en fysiek geweld speelt altijd een rol bij kinderpornografie. Slachtoffers ondervinden op het moment van het delict zelf fysieke pijn en psychische effecten (emotionele isolatie, angst en stress). Daarnaast worden zij telkens opnieuw slachtoffer wanneer het geproduceerde materiaal wordt gedeeld op internet. De langetermijngevolgen zijn depressie, PTSS (Post Traumatisch Stress Syndroom), laag zelfbeeld, het niet kunnen aangaan en/of onderhouden van emotionele en seksuele relaties, het vertonen van risicogedrag, verminderde arbeidsproductiviteit en een grotere kans om verzeild te raken in de commerciële seksindustrie.

Bij het bekend worden van (grootschalig) kindermisbruik – waarbij vaker wel dan niet sprake is van het vervaardigen van kinderpornografisch materiaal – ontstaat met enige regelmaat grote maatschappelijke onrust. Uit het recente verleden zijn voorbeelden bekend van vernielingen aan eigendommen en intimidatie van verdachten. Ook zijn er acties van buurtbewoners geweest om de huisvesting van een bekende veroordeelde in die buurt te voorkomen.
Na de zaak rondom Robert M. kijkt men anders naar het werk van mannen in de kinderopvang, op scholen en bij sportverenigingen.
Het is moeilijk te becijferen hoe hoog de maatschappelijke kosten zijn van slachtoffers die jarenlang fysieke of psychosomatische klachten ondervinden doordat zij in hun jeugd misbruikt zijn. Hun inzet op de arbeidsmarkt is minder en ziekte- en begeleidingskosten kunnen hoog zijn. De ontwrichtende werking van dit type delicten op het leven van (familie van) slachtoffers kan zo van grote invloed zijn op de maatschappij.

1.11.4 Verwachtingen

Wereldwijd neemt de internetdekking toe. Steeds meer mensen krijgen toegang tot internet, waarmee ook de toegankelijkheid van kinderpornografisch materiaal groter wordt. In 2015 was ongeveer 42 procent van de wereldbevolking voorzien van internet. Ruim 2 miljard mensen maken gebruik van sociale media. Deze aantallen groeien sterk. Het is waarschijnlijk dat hiermee ook een grote groep potentiële verspreiders of consumenten (betere) toegang tot het internet krijgt en gebruikmaakt van de mogelijkheden om materiaal uit te wisselen via fora en *boards.* Om toe te treden tot *rooms* in dergelijke fora, zoals VIP-rooms, is het noodzakelijk nieuw, nog niet eerder gezien, materiaal aan te leveren. De kansen op toenemend misbruik in die landen waar de internetdekking groeit, nemen daarmee aanzienlijk toe, net als de hoeveelheid beschikbaar materiaal. Ook de kans op *live distant child abuse* neemt door de grotere internetdichtheid toe. Met name voor mensen die in econo-

misch minder ontwikkelde landen leven, zal het deelnemen aan live distant child abuse een kans bieden om uit een achtergestelde positie te komen. Ook Nederlandse pedoseksuelen zullen van deze nieuwe mogelijkheden gebruikmaken.
De verschuiving van individuele verdachten naar verdachten die binnen netwerken opereren, zal doorzetten.
De hoeveelheid data die via dataverbindingen zal worden verstuurd, stijgt in de periode tot 2018 met 50 procent per jaar en zal in 2021 ten opzichte van 2015 zijn vertienvoudigd.
Een belangrijke ontwikkeling betreft de encryptie van dataverkeer en apparaten. De zogeheten *default encryption,* waarbij encryptie de standaard is, zal samen met de mogelijkheden die bijvoorbeeld de TOR-omgeving biedt, zorgen voor een omgeving die in zekere zin 'wetteloos' is. Hierdoor wordt het makkelijker dan wel mogelijk voor (nieuwe) doelgroepen via internet strafbaar materiaal uit te wisselen dan wel te verspreiden. De toepassing van end-to-end-encryptie zal ervoor zorgen dat het *unlocken* van datadragers en de toegang tot tablets, mobiele toepassingen en opslag voor het veiligstellen van bewijsmateriaal, zelfs voor producenten van deze apparatuur en providers niet meer mogelijk is.
Een ontwikkeling in de technische mogelijkheden van opsporing betreft de inzet van zogeheten *webcrawlers*. Deze bieden de mogelijkheid snel grote delen van het internet geautomatiseerd te scannen en informatie vast te leggen.
Op digitaal vlak zullen de komende jaren ook ontwikkelingen te zien zijn op het terrein van grootschalige data-analyse. Om onder andere aan de te verwachten toestroom van meldingen tegemoet te komen, zal vanuit deze techniek de keuze welke verdachten nadere aandacht verdienen, verder worden uitgediept. Keuzes in de aanpak worden op die manier ondersteund. Ook het zoeken naar onder andere criminele samenwerkingsverbanden in grote hoeveelheden data uit in beslag genomen materiaal kan zo worden verbeterd.
Een grotere aandacht voor het delict kinderpornografie en betere internationale samenwerking zullen ongetwijfeld leiden tot een (veel) groter aantal meldingen van kinderporno.
Er wordt verwacht dat de Nederlandse politie rond 2020 een aantal van ruim 20.000 meldingen per jaar zal ontvangen. Dit wil niet per se zeggen dat er ook sprake is van een feitelijke toename van het delict. Toch geven de bovenstaande verwachtingen voldoende reden om aan te nemen dat wereldwijd de productie, distributie en consumptie en daarmee ook de schadelijke gevolgen van kinderporno zullen toenemen. Of dit voor Nederland ook zal gelden, is onzeker.

1.11.5 Kwalificatie van dreiging

Er is sinds 2012 meer aandacht voor kinderpornografie waardoor ook het aantal meldingen is toegenomen. Bij het Meldpunt Kinderporno zijn in 2015 tienduizenden video's, afbeeldingen en websites gemeld en bij analyse blijkt dat het in driekwart van de gevallen om strafbaar materiaal gaat. In de opsporingsonderzoeken die naar kinderpornografie zijn uitgevoerd sinds 2012, zijn 850 Nederlandse slachtoffers geïdentificeerd. Het totale aantal slachtoffers is onbekend. Daarnaast is de verwachting dat het aantal meldingen bij de Nederlandse politie zal stijgen tot 20.000 meldingen per jaar in het jaar 2020.

Het gaat bij kinderpornografie om een zeer kwetsbare groep die slachtoffer wordt. De persoonlijke en psychische schade is groot. Telkens als het geproduceerde materiaal wordt gedeeld op internet, worden de afgebeelde personen opnieuw slachtoffer. De problemen die slachtoffers ondervinden, leiden tot verlies van arbeidsproductiviteit en kosten voor eventuele behandeling en begeleiding. Daarnaast gaan gevallen die aan het licht komen gepaard met grote maatschappelijke onrust.

De verwachting is dat het aantal slachtoffers verder zal stijgen vanwege het almaar toenemende gebruik van internet en sociale media. Ook zullen we *livestreaming* vaker gaan zien. Daarnaast beschikken daders over steeds betere mogelijkheden om zich af te schermen met behulp van TOR-netwerken en encryptie.
Met een toename van kinderpornografie zullen ook de eerder geschetste gevolgen verergeren. Daarbij komt nog dat er waarschijnlijk meer daders bij forensische poliklinische instellingen in behandeling moeten worden genomen en er meer kosten verbonden zullen zijn met de re-integratie van zedendelinquenten. Ook de kosten voor het bedrijfsleven stijgen als het moet voldoen aan de afspraken rond het leveren van abonneegegevens, de *Notice-and-Takedown*-procedure en de inbeslagname van servers. Al met al worden de verwachte gevolgen voor de komende jaren als ernstig ingeschat en wordt de productie en verspreiding van kinderpornografie gekwalificeerd als **dreiging**.

1.12 Productie en verspreiding van vals geld

1.12.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Vals geld; een rapportage tbv het NDB2017.* Dat rapport doet verslag van onderzoek dat begin 2016 is uitgevoerd voor dit dreigingsbeeld. De auteur van het onderzoeksrapport is Martin Grapendaal, werkzaam bij de politie. De bronnen die hij bij zijn onderzoek heeft gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

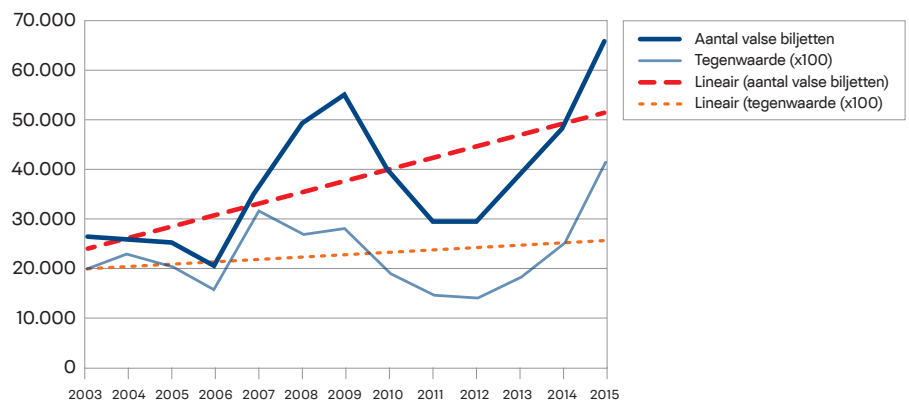
Geld is vals als munten of biljetten in hun geheel worden nagemaakt. Het namaken of vervalsen van geld is op zichzelf niet strafbaar volgens artikel 208 van het Wetboek van Strafrecht, maar wel als het de bedoeling is het als echt uit te geven. In deze paragraaf staan valse eurobiljetten centraal; valse biljetten van andere valuta en valse munten blijven hier buiten beschouwing. Ook *vervalst* geld valt buiten het domein. Anders dan bij vals geld is er bij vervalst geld geen sprake van nieuw vervaardigde biljetten: er worden aanpassingen gedaan op echte biljetten.
Resumerend bestaat het domein uit het in zijn geheel namaken van eurobiljetten en het opzettelijk verspreiden en uitgeven hiervan als echt en onvervalst. Als voorwaarde geldt dat de productie en de verspreiding van vals geld in of via Nederland plaatsvindt.

1.12.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

De belangrijkste ontwikkeling sinds het vorige dreigingsbeeld is de sterke stijging van het aantal gedetecteerde valse eurobiljetten: van 29.500 in 2012 tot 66.500 in 2015. Figuur 4 toont de ontwikkeling voor een wat langere periode en dan valt niet alleen de stijging op die is weergegeven door de lineaire trendlijn, maar ook de grote fluctuaties. Al naar gelang er illegale drukkerijen actief zijn, neemt het aantal valse eurobiljetten dat in omloop is af of toe.

Figuur 4. Aantal in circulatie aangetroffen valse eurobiljetten en hun tegenwaarde, 2003-2015



Bron: De Nederlandsche Bank

De tegenwaarde stijgt sneller dan het aantal valse biljetten door een toenemend aantal grotere coupures dat gedetecteerd wordt. In 2015 nam vooral het aantal gedetecteerde valse 500 eurobiljetten toe.

Het gaat hier om valse eurobiljetten die in circulatie zijn aangetroffen, dat wil zeggen dat er op enig moment mee betaald is. De tegenwaarde van deze valse biljetten is een goede indicator van de financiële schade. De Nederlandsche Bank vergoedt ingeleverde valse biljetten niet. Het overgrote deel wordt gedetecteerd door financiële instellingen (95%).

In de afgelopen jaren steeg in de gehele eurozone het aantal gedetecteerde valse eurobiljetten. Nederland schommelt al jaren zo rond de vierde, vijfde plaats in Europa wat betreft de aantallen aangetroffen valse eurobiljetten per miljoen inwoners.

Aard

Er zijn grofweg twee manieren om valse bankbiljetten te produceren. In de eerste plaats met de offsetdruktechniek en daarnaast met eenvoudige inkjetprinters of met officeprinters (tonerprinters). Over het algemeen heeft offset de voorkeur omdat deze techniek hoogwaardiger falsificaten oplevert dan de inkjetprinter. In heel Europa worden er dan ook meer offset geproduceerde biljetten in beslag genomen dan biljetten die met een inkjetprinter zijn geprint. In Nederland doet zich op dit punt een nieuwe ontwikkeling voor: er is een toename van het gebruik van de inkjetprinter bij de productie van vals geld. Deze nieuwe ontwikkeling zien we vrijwel uitsluitend in Nederland. Aangezien het printen met een inkjetprinter eenvoudiger en goedkoper is en kwalitatief mindere falsificaten oplevert, bestaat het vermoeden dat hier eerder opportunistische vervalsers actief zijn dan structureel actieve criminele groeperingen.

De offsetdruktechniek vereist hoogwaardig materiaal om geloofwaardige falsificaten te maken. Het gaat dan om papier, inkt en hologrammen die gebruikt worden om de echtheidskenmerken aan te brengen. Bij de toelevering van dit soort benodigdheden speelt China een steeds grotere rol.

De meeste in ons land aangetroffen valse eurobiljetten zijn afkomstig uit Italië, net als ten tijde van het vorige dreigingsbeeld.

In Nederland werden door Europol in de periode 2013-2015 vier incidenten gemeld: in Wijk bij Duurstede, Venlo, Arnhem en Alkmaar. Het ging hierbij zowel om verspreiders van vals geld als om producenten ervan. Verder is er een distributienetwerk opgerold in Hoevelaken, met vermoedelijk een Nederlandse bron. Recent heeft de Dienst Landelijke Recherche een onderzoek gestart naar de productie en verspreiding van een 500 eurobiljet van uitzonderlijk hoge kwaliteit.

De eerste stap in de distributieketen is het exporteren van de valse biljetten naar de landen waar ze uitgegeven worden. Dit gebeurt van oudsher door individuen die zich als zogenoemde *moneymules* lenen voor het per trein, vliegtuig of auto smokkelen van grote hoeveelheden valse biljetten. Tegenwoordig vinden valse bankbiljetten ook hun weg via handelsplatforms op het darknet. De gebruikelijke ‘wisselkoers’ bedraagt ongeveer 20 procent van de nominale waarde. De wisselkoers wordt gunstiger naarmate de bestelling omvangrijker is. De aangeboden biljetten worden betaald met bitcoins en verzonden met pakketpost.

De meestgebruikte manier om echt geld in ruil voor vals geld te krijgen, is het doen van kleine aankopen met valse biljetten met een hoge waarde. Dit is niet veranderd de laatste jaren en zal de komende jaren waarschijnlijk ook niet veranderen. Ook de slachtoffers blijven goeddeels dezelfde: kleine winkels, drogisterijen en warenhuizen. Andere gelegenheden zijn markten en bezorgdiensten omdat daar vaak geen detectieapparatuur aanwezig is.
Sommige landen rapporteren een toename van online aankopen die bekostigd worden met vals geld. Tweedehands goederen met een hoge waarde (zoals tablets en smartphones) worden online aangeschaft en de koper ontmoet de verkoper op een zondag of na sluitingstijd van de banken om met valse euro's te betalen. Pas de volgende dag ontdekt de verkoper dat hij is opgelicht. Het is niet bekend in welke mate valsemunters deze werkwijze toepassen in Nederland, het zou ook in ons land een aantrekkelijke modus operandi kunnen zijn.

1.12.3 Huidige gevolgen

De productie en verspreiding van vals geld heeft financiële schade tot gevolg en kan leiden tot ondermijning van het vertrouwen in het financiële stelsel.
In figuur 4 werd de (virtuele) tegenwaarde van de valse eurobiljetten weergegeven. In de periode van 2012 tot en met 2015 steeg die tegenwaarde met 300 procent van 1.390.000 naar 4.161.000 euro. Dit betreft directe schade voor particulieren en bedrijven die slachtoffer geworden zijn van valse euro's. De Nederlandsche Bank vergoedt, zoals gezegd, die schade niet. Wereldwijd werden in 2014 ongeveer 800.000 valse eurobiljetten uit de circulatie genomen met een tegenwaarde van zo'n 32.500.000 euro.
Er worden ook valse biljetten in beslag genomen voordat zij in roulatie komen, bijvoorbeeld wanneer een drukkerij of distributienetwerk wordt opgerold. Dan is er geen sprake van enige financiële schade. Zo zijn er in 2014 bij opsporingsacties 1.200.000 biljetten gedetecteerd voordat deze in roulatie kwamen. Deze biljetten vertegenwoordigden een virtuele tegenwaarde van 66.500.000 euro. Daarmee werd een even grote economische schade voorkomen.

De tweede categorie schade, ondermijning van het vertrouwen in het financiële stelsel, is moeilijk in cijfers tot uitdrukking te brengen. In zijn algemeenheid kan gesteld worden dat de kans op ondermijning toeneemt naarmate de kans op slachtofferschap toeneemt. In aanmerking genomen dat er zo'n 300 à 400 miljoen eurobiljetten in Nederland in omloop zijn, is die kans erg klein (1 op 30.000). Ook als de virtuele tegenwaarde afgezet wordt tegen de hoeveelheid geld die in Nederland in omloop is, moet – ondanks de waargenomen stijging in de laatste jaren – geconcludeerd worden dat het om een relatief klein en beheersbaar probleem gaat.

1.12.4 Verwachtingen

Verwachtingen over de ontwikkeling van vals geld ontlenen we aan ontwikkelingen in technologie, veranderingen in betaalgedrag, voorlichting over falsificaten en aan extrapolatie van trends.

Technische vooruitgang heeft geleid tot een veel betere kwaliteit van printers, waardoor met inkjetprinters en een dot-matrixfolie met betrekkelijk weinig moeite relatief goede falsificaten zijn te maken. Tegelijkertijd zien we dat de echtheidskenmerken van nieuwe generaties eurobiljetten steeds geavanceerder worden en moeilijker na te maken zijn. Deze twee factoren hebben min of meer tegengestelde effecten. Hoe dit per saldo uitpakt, is onbekend. Van belang is echter hierbij te bedenken dat printer- en fotokopieerfabrikanten hun producten van software voorzien die het onmogelijk – of althans een stuk moeilijker – moet maken ze te gebruiken om er vals geld mee te vervaardigen.
Een andere ontwikkeling betreft de toepassing van de *blockchaintechnologie.* Dit is de technologie achter de bitcoin en andere *cryptocurrency's*. Kort gezegd is een *blockchain* een openbaar en online register van transacties. Via de blockchain van de bitcoin kan nagegaan worden wie de eigenaar is en of de bitcoin niet twee keer wordt uitgegeven. De relatie met vals geld vinden we vooral bij de belangrijkste huidige toepassing, de cryptocurrency's of de virtuele munten. In feite valt dit onder de noemer girale betalingen: naarmate meer gebruikgemaakt wordt van virtuele munten en niet van tastbare biljetten, zal de aantrekkelijkheid van vals contant geld afnemen.
De blockchaintechnologie verkeert nog in een pril stadium, waardoor het problematisch is om verwachtingen uit te spreken. Voorlopig gaan we ervan uit dat deze technologie de eerstkomende vier jaar nog geen aardverschuiving met betrekking tot vals geld zal opleveren. Het is wel van belang de ontwikkelingen te volgen om tijdig het hoofd te kunnen bieden aan de hiermee gepaard gaande criminele verschijnselen.

Het betaalgedrag van consumenten verandert. Er wordt steeds minder vaak contant afgerekend en steeds vaker met de pinpas of varianten daarop. In 2015 is het aantal girale betalingen voor het eerst boven de chartale uitgestegen (3,23 versus 3,19 miljard transacties). Voor de totale bedragen die met beide soorten transacties gemoeid zijn, was dat al veel eerder het geval. Dit komt doordat de grotere aankopen doorgaans giraal worden afgerekend en de kleinere contant. Nieuwe toepassingen zullen de balans alleen maar verder doen doorslaan in het voordeel van digitale betalingen. Zo kan de consument sinds enige tijd contactloos betalen, waarbij hij alleen de pinpas langs een betaalautomaat hoeft te halen zonder een pincode in te voeren. Ook verschijnen de laatste tijd apps voor de smartphone om met gebruikmaking van het telefoonnummer en buiten de banken om, betalingen aan de contactpersonen uit het telefoonboek van de smartphone te doen. Verder verschijnen er in toenemende mate winkels in het straatbeeld die alleen girale transacties accepteren en nemen de online aankopen almaar toe (in 2015 met 20 procent). Kortom, er bestaat een onomkeerbare trend naar overwegend giraal betalingsverkeer.

Een derde factor die een rol speelt bij de ontwikkelingen rond vals geld, bestaat uit de vrijwel permanente voorlichtingscampagnes van De Nederlandsche Bank (DNB), de Europese Centrale Bank en andere belanghebbenden. De consument en ondernemer worden bewust gemaakt van de echtheidskenmerken en het belang van controle. Bij een toenemend aantal kassa's treffen we een scanner aan die de grotere coupures controleert op echtheid. Voor

het publiek heeft DNB een app ontwikkeld die – dankzij de goede camera waarmee de huidige smartphones zijn uitgerust – valse biljetten van echte kan onderscheiden.
De aanname is dat hierdoor valse biljetten sneller gedetecteerd zullen worden, waarmee de opbrengst ervan zal verminderen. Er is niet met zekerheid vast te stellen of deze aanname ook klopt. Bovendien kun je je afvragen of het publiek bij het aantreffen van een vals biljet zijn 'verlies neemt' en aangifte doet. Een even plausibele aanname is dat het publiek zich van den domme houdt en het valse biljet toch probeert uit te geven. Daarmee lijkt de app vooral gericht op het creëren van *awareness.*

Het doortrekken van de lijn uit figuur 4 van 2012 naar 2021 zou wijzen op een verdere toename van het aantal valse eurobiljetten. Het grillige verloop van de cijfers in de jaren voorafgaand aan 2012 toont dat het riskant is om een verwachting te bouwen op een toename gedurende enkele jaren. Dat blijkt ook uit de cijfers voor het eerste kwartaal van 2016. In 2015 werden in het eerste kwartaal zo'n 23.000 valse eurobiljetten gedetecteerd, in 2016 is dat gedaald naar zo'n 11.000 biljetten. Deze daling bevestigt nog maar eens het grillige verloop.

Er zijn geen duidelijke oorzaken aan te wijzen voor de stijging van de laatste jaren, noch zijn de te verwachten ontwikkelingen eenduidig. De combinatie van bovenstaande factoren echter – waarvan het veranderende betaalgedrag de meest ingrijpende lijkt te zijn – leidt tot de verwachting dat de komende jaren een daling te zien zullen geven, zowel in hoeveelheid valse biljetten als in de virtuele tegenwaarde ervan.

1.12.5 Kwalificatie van dreiging

Het aantal valse eurobiljetten fluctueert al naar gelang er illegale drukkerijen actief zijn. De financiële schade van de productie en verspreiding van vals geld in Nederland bedroeg de afgelopen periode jaarlijks enkele miljoenen. Deze schade komt voor rekening van particulieren en bedrijven die slachtoffer worden van valse eurobiljetten. De kwaliteit van het valse geld varieert van eenvoudige falsificaten die vervaardigd zijn met een inkjetprinter tot geavanceerde vervalsingen van eurobiljetten die nauwelijks meer van echt zijn te onderscheiden. In 2015 bedroeg het aantal gedetecteerde valse eurobiljetten 66.500. In deze omvang is de kans dusdanig klein om slachtoffer te worden van de verspreiding van valse biljetten, dat geen sprake is van aantasting van het vertrouwen in het financiële stelsel.

De komende jaren zal de hoeveelheid chartaal geld verder afnemen ten gunste van giraal betalingsverkeer en contactloos betalen. Door voorlichting komt er meer aandacht voor vals geld en vindt bij kassa's in toenemende mate controle op echtheid plaats. De verwachting bestaat dat het aantal valse biljetten en de virtuele tegenwaarde ervan zullen gaan dalen. Hiermee blijven de negatieve financiële gevolgen binnen de perken en is de productie en verspreiding van vals geld in Nederland voor de komende jaren **geen concrete dreiging**.

1.13 Matchfixing

1.13.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Illegale kansspelen en matchfixing. Nationaal dreigingsbeeld 2017*. Dat rapport doet verslag van onderzoek dat voor dit dreigingsbeeld is uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Sanne Poortman en Irma Vermeulen, beiden werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*

Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Matchfixing is het manipuleren van de uitkomst van een sportwedstijd of competitie door op oneigenlijke manieren het verloop of de uitkomst van de wedstrijd of competitie te bepalen. Matchfixing kan met twee verschillende oogmerken plaatsvinden: omwille van een sportief voordeel of omwille van een financieel voordeel. Manipulatie gericht op een sportief voordeel kent geen directe link met georganiseerde criminaliteit en blijft hier buiten beschouwing.

Matchfixing gericht op het behalen van financieel voordeel is vaak gokgerelateerd. Door omkoping moet een wedstrijdresultaat worden gegarandeerd waardoor hoge gokinzetten bij bookmakers of gokbedrijven grote winsten opleveren. Deze paragraaf beperkt zich tot matchfixing in voetbal en tennis, voor zover het georganiseerde criminaliteit betreft die de Nederlandse samenleving raakt. Het gaat om het fixen van wedstrijden door Nederlandse spelers of Nederlandse clubs (in binnen- of buitenland) en om het fixen van sportwedstrijden die op Nederlands grondgebied worden gespeeld.

1.13.2 Ontwikkelingen in aard en omvang sinds het NDB2012

In de uitvoering van matchfixing spelen twee, en soms drie, typen actoren een rol. Er is altijd sprake van een omkoper en een uitvoerder. De omkoper is de crimineel die de uitvoerder omkoopt of dwingt tot het manipuleren van een wedstrijd. De uitvoerder is bijvoorbeeld een sporter, scheidsrechter of jurylid. Als de omkoper niet direct in contact treedt met de uitvoerder, dan kan het zijn dat hij gebruikmaakt van een tussenpersoon, de *runner.* Dit kan een oud-speler, spelersmakelaar, sponsor, trainer of bestuurslid zijn.

Op het niveau van de individuele sporters, de sportclubs, de kansspelaanbieders en de sportwedstrijden onderscheiden we diverse risicofactoren voor matchfixing. We noemen een selectie.

Voor individuele sporters zijn de risicofactoren voor matchfixing bijvoorbeeld lage inkomsten, een gering carrièreperspectief of connecties met criminelen. Deze factoren vergroten de kans dat een sporter bij matchfixing betrokken raakt.

Sportclubs zijn een aantrekkelijk doelwit voor matchfixers als zij in financieel zwaar weer verkeren. Als deze sportclubs instemmen met een aangeboden fix kunnen zij hun schuldlasten soms al in één wedstrijd terugverdienen.
Op het niveau van de kansspelaanbieders vormen de *liquide* gokmarkten een risico. Gokmarkten waar veel en hoog wordt ingezet, zijn aantrekkelijke werkterreinen voor matchfixers omdat hun activiteit daar minder opvalt. Dat betekent dat sommige kansspelaanbieders op die markten meer risico lopen op het uitkeren van gokwinsten uit gefixte sportwedstrijden. Gebrek aan transparantie bij sommige kansspelaanbieders vormt ook een risicofactor voor matchfixing. Sommige kansspelaanbieders of eigenaren kunnen onbekend opereren. Dat betekent dat ook criminelen zich als kansspelaanbieder kunnen voordoen en vanuit die hoedanigheid gokuitslagen kunnen manipuleren of onder één hoedje kunnen spelen met een matchfixer.
Ten slotte zijn er op het niveau van de sportwedstrijden risico's voor matchfixing aan te merken. Het gaat om jeugdwedstrijden, oefenwedstrijden, vriendschappelijke duels en om wedstrijden uit de lagere regionen van de competities. Jeugdwedstrijden zijn relatief makkelijk te manipuleren doordat jonge spelers makkelijker te beïnvloeden zijn en doordat het toezicht op dergelijke wedstrijden meestal beperkt is. Van beperkt toezicht is meestal ook sprake bij oefenwedstrijden, vriendschappelijke duels en wedstrijden uit de lagere competities. Dat maakt ook die wedstrijden vatbaar voor matchfixing.

Matchfixing is een fenomeen met een mondiaal karakter. De in Nederland bekende onderzoeken en signalen van matchfixing hebben allemaal een internationale component. Dat komt doordat fixers vaak vanuit het buitenland werken en vooral op de Aziatische gokmarkt gokken op de door hen gefixte wedstrijden. Het is voor fixers op de relatief grote Aziatische gokmarkt aantrekkelijk om grote inzetten te plegen zodat zij ook grote winsten kunnen genereren.

In 2013 stellen onderzoekers dat matchfixing zich niet op grote schaal voordoet in Nederland. Dat baseren zij op onderzoek onder sporters en na bestudering van informatie van opsporingsinstanties. Van ruim zevenhonderd bevraagde sporters geeft 4 procent aan benaderd te zijn voor matchfixing, waarvan het grootste deel voor niet-gokgerelateerde matchfixing. Onbekend is welk deel heeft meegewerkt aan de matchfixing. De in het onderzoek aangehaalde opsporingsinformatie wijst incidenteel op (vermeende) matchfixingpraktijken.

Politie-informatie over de periode 2012-2015 levert drie gestarte opsporingsonderzoeken naar gokgerelateerde (elementen van) matchfixing op. Twee onderzoeken hadden betrekking op voetbal, een op tennis.
Het aantal opsporingsonderzoeken naar matchfixing zegt waarschijnlijk weinig over de werkelijke omvang, want matchfixing is een 'haaldelict'. Dit betekent dat de politie matchfixing zelf moet constateren; burgers en bedrijven melden gevallen van matchfixing nauwelijks bij de politie. Zolang matchfixing weinig aandacht krijgt van de politie, worden geen grote inspanningen geleverd om het verschijnsel aan te tonen. Waarschijnlijk doen zich

meer matchfixingzaken voor dan op het eerste gezicht lijkt. Daarvoor zijn aanwijzingen. Tot nog toe gaven die echter te weinig aanknopingspunten voor het starten van opsporingsonderzoeken.

De omvang van matchfixing in het voetbal is volgens geïnterviewde experts beperkt. Dat komt volgens hen doordat Nederland bestuurlijk gezien een relatief solide voetbalcompetitie heeft met degelijke lonen, goede financiële overbruggingsregelingen voor voetballers die hun carrière beëindigen en een hoge mate van transparantie in het beheer van clubs. In dat bestuurlijke klimaat zijn potentiële doelwitten van fixers (spelers, clubs) minder kwetsbaar voor matchfixingpraktijken.

De omvang van matchfixing in het tennis beperkt zich in de afgelopen vier jaar vooral tot een aantal signalen. ESSA, een organisatie die namens grote gokbedrijven gokfraude opspoort bij sportwedstrijden over de hele wereld, rapporteert voor 2015 73 verdachte tenniswedstrijden, waarvan er twee betrekking zouden hebben op Nederland.

De grootste gokmarkt bevindt zich in Azië; 70 procent van het wereldwijde gokken op voetbalwedstijden verloopt via Aziatische bookmakers. Voor tennis is het aandeel onbekend, maar waarschijnlijk gebruiken gokkers hiervoor met name de Europese gokmarkt. Omdat de Aziatische gokmarkt vele malen groter is dan de Europese, is het aantrekkelijk voor matchfixers om op die markt te gokken. Hun hoge inzetten vallen minder op in de grote bulk van andere inzetten. Bovendien genereren meer en hogere inzetten, vooral in de gokmarkten waar veel deelnemers en grote bedragen in omgaan, ook grotere winsten. Daar komt bij dat in het Aziatische systeem anoniem kan worden gegokt en de inzet ongelimiteerd is. Dat is in Europa niet zo.

Op de Aziatische en Europese online gokmarkten zijn ook Nederlandse wedstrijden interessant wedmateriaal. Deze gokmarkten groeien al jaren en blijven dat de aankomende jaren doen. De groei trekt nieuwe fixers aan en vergroot de kans op matchfixingpraktijken. Dat betekent ook een vergrote kans dat Nederlandse sportwedstrijden of competities met matchfixingpraktijken te maken zullen krijgen.

Fixers investeren in nieuwe strategieën om ook in de toekomst matchfixing te kunnen blijven voortzetten en lucratief te houden. Ze beschikken al over software die grote inzetten over meerdere kleine inzetten verdeelt bij bookmakers of gokaanbieders. Zo worden activiteiten van fixers minder snel opgemerkt door opsporingsdiensten en kunnen ze grote bedragen inzetten. Ook zouden fixers in georganiseerd verband algoritmen ontwikkelen die helpen om inzetten op de gokmarkt zo te timen dat het voor een gokaanbieder niet meer mogelijk is om bij onraad een wedstrijd te annuleren.

1.13.3 Huidige gevolgen

De huidige gevolgen voor de Nederlandse samenleving zijn beperkt. De benadeelden lijden vooral financiële schade. Het gaat om gokkers die schade lijden doordat ze gokken op wedstrijden die gemanipuleerd zijn. We moeten ons hierbij overigens wel realiseren dat gokkers ook kunnen verliezen als uitslagen niet gemanipuleerd worden. Het is onbekend hoe groot de groep gokkers is die schade lijdt ten gevolge van matchfixing. Kansspelaanbieders lijden schade omdat zij de fixers, die met voorkennis op hun spelaanbod hebben gewed, moeten betalen. Daar lijkt in Nederland echter nauwelijks sprake van, omdat de meeste fixers hun gok uitzetten bij buitenlandse kansspelaanbieders. De schade wordt in het buitenland geleden. Als gevolg van matchfixing kunnen ook sportclubs financiële schade lijden, bijvoorbeeld door een daling in het aantal toeschouwers en opzegging van sponsorcontracten. In Nederland lijkt dat niet het geval te zijn.

Kijkend naar de gevolgen op het vlak van de gezondheid, overlast of ondermijning zien we geen noemenswaardige effecten op de Nederlandse samenleving. Wel zien we dat door signalen van matchfixing en de aandacht hiervoor in de media het aanzien van bepaalde takken van sport onder druk komt te staan. Mochten die takken van sport in sterke mate besmet worden door matchfixing, dan zou de maatschappelijke betekenis van sport, onder andere op het gebied van educatie en gezondheid, kunnen afnemen. Vooralsnog is dat niet het geval.

1.13.4 Verwachtingen

Verwacht wordt dat het aantal matchfixingzaken in de komende vier jaar toeneemt, ook al is niet bekend in welke mate. Opsporingsdiensten bouwen meer kennis en expertise op, waardoor ze meer gevallen van matchfixing in het vizier krijgen. Ook het daadwerkelijke aantal gevallen van matchfixing zal toenemen. De wereldwijde gokmarkt voor tennis- en voetbalwedstrijden groeit door en daarmee neemt de geldstroom op gokmarkten toe. Dat maakt het fixen van en gokken op gefixte wedstrijden in Nederland en elders in de wereld aantrekkelijker. De recente verkoop van de uitzendrechten van de Nederlandse voetbalcompetitie aan China maakt de Nederlandse competitie aantrekkelijker voor matchfixing. Er zullen meer Chinezen op Nederlandse wedstrijden gaan gokken. Dat levert een hogere liquiditeit op de gokmarkt op en dat maakt Nederlandse competitiewedstrijden aantrekkelijker voor matchfixing.

Werkwijzen van matchfixing zullen gaan veranderen. Er worden nieuwe manieren van fixen ontdekt, waardoor fixers minder in de kijker lopen van fraudedetectiesystemen en opsporingsdiensten. De pakkans is laag. Dat hangt ook samen met het feit dat er vooralsnog weinig fraudedetectie plaatsvindt in de lagere sportcompetities, bij vrouwensporten en bij jeugdsporten. De kans om daar gemanipuleerde wedstrijden te detecteren, is vooralsnog klein.

Fixers breiden hun werkterrein steeds verder uit, niet alleen naar andere traditionele sporten, maar ook naar *e-sports*, videogame-competities waarbij individuen of teams tegen elkaar strijden. Wereldwijd gaan miljarden euro's om in de e-sportsindustrie. Omdat er op de uitkomsten van e-sports kan worden gegokt en de populariteit van deze sporten in Nederland aan het toenemen is, ontstaat een nieuwe markt voor matchfixing. In het buitenland zijn al gevallen van het manipuleren van e-sports geconstateerd.

Er schuilt een potentieel gevaar in de ontwikkeling dat zich steeds vaker (vermogende) buitenlandse investeerders aandienen die Nederlandse voetbalclubs financieel ondersteunen. Voorbeelden uit het buitenland laten namelijk zien dat daar soms ook investeerders bij zitten die zich met matchfixingpraktijken bezighouden. In een artikel in *de Volkskrant* van december 2016 wordt het voorbeeld gegeven van een Finse club.[23]
Het doel van de investeerders is om voetbalclubs over te nemen en corrupte spelers binnen de selectie te brengen, zodat gedurende langere tijd invloed kan worden uitgeoefend op de uitslagen van de wedstrijden. Daardoor kunnen ze volstaan met het inzetten van relatief lage bedragen op de gokmarkt, waarbij de kans op ontdekking minder groot is dan wanneer ze voor een paar gemanipuleerde wedstrijden fors 'moeten' inzetten.

Een ander potentieel gevaar voor matchfixing schuilt in het toenemende streven van fixers om meer individuen voor zich te winnen en lang aan zich te verbinden. Dit streven komt voort uit het feit dat de liquiditeit op de gokmarkt voor sommige individuele sporten groeit. Er valt, met andere woorden, geld te verdienen op een markt waar veel deelnemers en geld omgaan. Voor tennis is de groei op de gokmarkt het meest saillant, maar ook sporten als darts en snooker/poolbiljart zitten in de lift. Vergeleken met het fixen van groepssporten achten fixers hun kansen op het regelen van een fix in individuele sporten groter. Individuen zijn immers makkelijker te manipuleren dan groepen. Bovendien verdienen veel sporters in individuele sporten veelal stukken minder dan hun collega's in de hoogste divisie van het voetbal. Matchfixers spelen daarop in. Zo kan een sporter aan een fixer worden gebonden wanneer een transferbedrag voor de sporter wordt opgehoogd met een onofficieel fixbedrag, bijvoorbeeld door een malafide zaakwaarnemer. Een sporter die met zo'n transfer instemt, is direct in de greep van een matchfixer omdat openbaarmaking van betrokkenheid bij matchfixing meestal direct het einde van de sportcarrière betekent.

De verwachte gevolgen tot en met 2021 liggen grotendeels in het verlengde van de huidige gevolgen. De schade die wordt geleden, blijft vooral financieel van aard. Naar verwachting neemt de omvang van de schade toe door de toename van het aantal matchfixingpraktijken. Dat betekent dat meer gokkers en kansspelaanbieders schade lijden. Mogelijk lopen ook Nederlandse sportclubs financieel averij op. Anders dan nu het geval is, zal een deel van de toekomstige schade voor online kansspelaanbieders ook in Nederland worden geleden.

23 M. van Dongen & W. Feenstra (2016, 8 december). Matchfixers kopen Europese voetbalclubs voor witwassen en gokken met voorkennis. *de Volkskrant*. Geraadpleegd op http://www.volkskrant.nl

Dat komt doordat Nederlandse of in Nederland gevestigde online kansspelaanbieders door een nieuwe wet (Kansspelen op afstand) binnenkort legaal kunnen opereren in Nederland. Zij lijden schade als ze moeten uitkeren aan fixers. De overheid lijdt schade door derving van belastinginkomsten op de kansspelen. Door de verwachte toename in het aantal matchfixinggevallen en de berichtgeving over matchfixing bestaat een vergroot risico dat de beeldvorming over eerlijk spel negatief wordt beïnvloed. Bij een toenemend aantal mensen kan daardoor in de toekomst de indruk ontstaan dat er bij sportwedstrijden sprake is van vals spel.

1.13.5 Kwalificatie van dreiging

Op dit moment wordt de markt voor gokgerelateerde matchfixing met een link naar Nederland qua omvang als gering geschat. De informatie beperkt zich vooral tot signalen van matchfixing, in het voetbal en in het tennis.

De omvang van matchfixing gaat stijgen, hoewel niet bekend is in welke orde van grootte. Er is verhoogde aandacht voor het verschijnsel en gokmarkten worden groter, diverser en toegankelijker. Door een stijging in de vraag naar en het aanbod van gokwedstrijden neemt ook de vraag naar wedmateriaal toe. Dat betekent dat, naast voetbal en tennis, ook andere sporten te maken krijgen met matchfixingpraktijken.

Op dit moment blijven de gevolgen voor de Nederlandse samenleving beperkt tot vooral financiële schade. Het gaat in de eerste plaats om schade die Nederlandse gokkers lijden. Schade voor kansspelaanbieders wordt vooral in het buitenland geleden. Sportclubs, sponsors of de overheid lijden in Nederland, voor zover nu bekend is, nauwelijks financiële schade ten gevolge van matchfixingpraktijken. De toekomstige schade voor kansspelaanbieders en de overheid kan gaan toenemen als door de nieuwe wet Kansspelen op afstand online kansspelaanbieders op de kansspelmarkt worden toegelaten.

De huidige en de te verwachten gevolgen zijn vooral financieel van aard. De omvang van matchfixing is beperkt en zelfs met een toekomstige stijging in het aantal matchfixinggevallen zijn de financiële gevolgen nog niet bijzonder omvangrijk. Het is onwaarschijnlijk dat de stijging van dien aard is dat het de geloofwaardigheid van de sport aantast. Matchfixing wordt gekwalificeerd als **geen concrete dreiging**.

1.14 Illegale kansspelen

1.14.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Illegale kansspelen en matchfixing. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek dat voor dit dreigingsbeeld is uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Sanne Poortman en Irma Vermeulen, beiden werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.* Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Illegale kansspelen zijn kansspelen die vergunningplichtig zijn maar zonder vergunning conform Nederlandse wetgeving worden georganiseerd en/of aangeboden. Het gaat om illegale varianten van legale kansspelen en om kansspelen waarvoor geen legale variant bestaat. Ook het aanbieden en organiseren van online kansspelen is vooralsnog illegaal. Voor die spelen ligt een wetsvoorstel Kansspelen op afstand bij het parlement. Dit voorstel tot wijziging van de Wet op de kansspelen heeft als doel online kansspelen te reguleren, waardoor het illegale aanbod via internet aan banden kan worden gelegd.

De illegale kansspelen die in deze paragraaf aan bod komen, zijn de kansspelen waarvan verondersteld wordt dat die in enig georganiseerd verband kunnen worden aangeboden en waarbij anoniem grote sommen (zwart) geld kunnen worden omgezet. Dit is het geval bij de hier beschreven illegale bingo, illegaal poker, illegale lotto en (sport)toto, gokzuilen en online kansspelen.

1.14.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Bij *illegale bingo's* gaat het om bingo's waar hoge prijzengelden of cadeaus worden uitgekeerd en die met de nodige regelmaat (soms dagelijks) georganiseerd worden door een klein groepje mensen dat in een bedrijfsachtige structuur samenwerkt. Het gaat vaak om familiebedrijven. Meestal gokken de organisatoren erop dat de bingo door de gemeente wordt gedoogd omdat ze deze in besloten kring aanbieden. Om het illegale karakter van de bingo te verhullen, worden soms afschermingsmethoden gebruikt. De bingo wordt georganiseerd door iemand die dat zogenaamd ten behoeve van of namens een vereniging doet (die desnoods met dat doel wordt opgericht), de hoogte van het prijzengeld wordt niet bekendgemaakt en beveiligers worden geposteerd om pottenkijkers buiten de deur te houden. Een enkele keer zijn bij deze grootschalige bingo's organisatoren aangetroffen met criminele antecedenten, onder andere in de hennepteelt. Nu en dan is sprake van geweld tussen concurrerende illegale bingo-exploitanten naar aanleiding van onenigheid over wie waar bingo zou mogen aanbieden.
Over de omvang van het aantal illegale bingo's is weinig bekend. In de periode 2012-2015 werd bij de Kansspelautoriteit (KSA) 86 keer melding gemaakt van een illegale bingo (9

procent van het totale aantal meldingen van illegale kansspelen). De KSA schat dat het aantal illegale bingo's veel hoger moet liggen, maar heeft daar vooralsnog weinig zicht op. In onderzoek naar de aard en omvang van illegale kansspelen in Nederland, in 2009 uitgevoerd in opdracht van het WODC, wordt de inzet bij illegale bingo's in Nederland geschat op bijna 25 miljoen euro, de bruto spelopbrengst (ontvangen inzet minus uitgekeerde prijzen) op minstens 4,5 miljoen euro.[24]

Van de casinospelen is *poker* een van de meest populaire spelen waarvoor een illegale markt bestaat. Dat blijkt althans uit het eerdergenoemde onderzoek dat in 2009 in opdracht van het WODC werd uitgevoerd. Daarin wordt geschat dat er in Nederland ongeveer 200.000 spelers van illegaal poker zijn en dat de inzet ongeveer 21 miljoen euro bedraagt met een bruto spelopbrengst van ongeveer 4,5 miljoen euro. In de periode 2012-2015 heeft een groot deel van de meldingen bij de KSA betrekking op illegaal poker (259 meldingen van illegale pokerevenementen, bijna 28 procent van het totale aantal meldingen van illegale kansspelen). Er is geen recente informatie waaruit blijkt dat de georganiseerde criminaliteit in Nederland zich met de organisatie van illegale pokerspelen bezighoudt. Illegaal poker wordt vooral in cafés en bij mensen thuis georganiseerd. Deelnemers worden via vrienden en bekenden benaderd. Op sommige illegale pokerspelen pokeren criminelen met hun crimineel verkregen inkomsten.

Als we kijken naar de in Nederland georganiseerde *illegale lotto's en (sport)toto's* waarvoor uitslagen van de officiële Nederlandse trekkingen worden gevolgd, dan zien we trekkingen plaatsvinden, onder andere in cafés, snackbars en op campings. Sommige tabakszaken bieden naast legale ook illegale loten onder de toonbank aan. Illegale lotto komt in diverse Nederlandse gemeenten al jaren voor. Het wordt georganiseerd door enkele onafhankelijke groepjes, bestaande uit organisatoren en lotenverkopers. Elke groep bedient meestal een paar honderd spelers. Onder de spelers bevinden zich soms mensen die op hun beurt lotto's organiseren met de door hen aangekochte loten.
Enkele organisatoren van illegale lotto's zijn bekend in het lokale criminele milieu. Hoewel de verkoop van loten aan honderden deelnemers lastig te onttrekken is aan het zicht van de samenleving, worden de andere activiteiten zo veel mogelijk afgeschermd. Administraties worden verborgen, opbrengsten uit de spelen worden witgewassen in eigen ondernemingen en soms bezit men vuurwapens om die te kunnen gebruiken tegen eventuele rippers.
Net als bij de hierboven genoemde aantallen is er verder weinig bekend over de omvang van illegale lotto's en toto's in Nederland. De KSA kreeg in de periode 2012-2015 96 meldingen binnen, 10 procent van het totale aantal meldingen van illegale kansspelen. De jaarlijkse inzet bij illegale lotto's en toto's werd in het eerdergenoemde onderzoek uit 2009 geschat op ongeveer 13 miljoen euro, de bruto spelopbrengst op ongeveer 11 miljoen euro.

24 G.H.J. Homburg & E. Oranje (2009). *Aard en omvang van illegale kansspelen in Nederland.* Amsterdam: Regioplan Beleidsonderzoek.

Gokzuilen zijn illegaal en kennen geen legale variant. Via gokzuilen in cafés, koffiehuizen, belwinkels en afgeschermde locaties wordt gewed op sportwedstrijden. Het gaat meestal om locaties met een vaste klantenkring. Uitbaters van deze locaties verdienen maandelijks een paar honderd euro aan de huur van een gokzuil, aangevuld met een percentage van de omzet van de gokzuil. Sommige uitbaters worden onder druk gezet om gokzuilen te plaatsen.
In Nederland worden gokzuilen vooral in Turkse koffiehuizen aangetroffen. Uit onderzoek naar gokzuilen van 2015 blijkt dat het merendeel van de koffiehuisexploitanten bij wie de zuilen worden aangetroffen, antecedenten heeft op het gebied van drugscriminaliteit, het gebruik van geweld of het in vereniging plegen van (andere) strafbare feiten. In een opsporingsonderzoek kwamen dertig locaties in Nederland en Duitsland aan het licht waar gokzuilen waren geplaatst. Ander onderzoek laat zien dat criminele Turkse familienetwerken uit Duitsland in Nederland actief zijn in de exploitatie van gokzuilen. Zij houden zich ook bezig met de handel in hennep, synthetische drugs en witwassen.
Verder zijn er aanwijzingen dat een criminele groepering uit Duitsland en Nederland (van Turkse herkomst) ook gokzuilen exploiteert in België.

De KSA ontving 365 meldingen van gokzuilen in de periode 2012-2015 (39 procent van het totale aantal meldingen). Het aantal meldingen van gokzuilen bij de KSA is gestegen van 30 in 2012 naar 101 in 2015.
In het eerdergenoemde onderzoek naar gokzuilen zeggen de onderzoekers dat er jaarlijks gemiddeld 202 gokzuilen in Nederland worden aangetroffen. De omzet van die zuilen wordt geschat op bijna 37 miljoen euro per jaar. Afgaand op de opbrengsten die in enkele opsporingsonderzoeken naar voren zijn gekomen, variërend van enkele tonnen tot een paar miljoen euro, stellen experts dat deze geschatte omzet van 37 miljoen hoger zou kunnen zijn. Daarbij moet worden opgemerkt dat extrapolatie van opbrengsten op basis van enkele opsporingsonderzoeken weinig houvast biedt voor een betrouwbaar beeld van de werkelijke omzet van gokzuilen in Nederland.

Bij de *online kansspelen* is uit opsporingsonderzoek naar voren gekomen dat dubieuze online kansspelaanbieders voorwenden vergunde kansspelaanbieders te zijn of gebruikmaken van replicawebsites van officiële, vergunde kansspelaanbieders uit het buitenland. Kleine prijzen worden uitgekeerd, maar hoofdprijzen gaan naar medeplichtige organisatoren en ondertussen wordt er geroofd uit de pot met inleg. Een andere manier waarop criminelen online kansspelen exploiteren, is door buitenlandse goksites te misbruiken. In een geval werd daarvoor een goksysteem ontwikkeld waarbij via tussenpersonen anoniem en contant op voetbalwedstrijden op deze buitenlandse goksites gegokt kon worden.

Online kansspelen vinden vooral binnenshuis plaats en zijn niet zichtbaar voor een groter publiek. Enig idee van het aantal Nederlanders dat aan online kansspelen deelneemt en van de opbrengsten die ermee gepaard gaan, ontlenen we aan twee opsporingsonderzoeken. In een opsporingsonderzoek had een illegale kansspelaanbieder op enig moment meer dan

275.000 Nederlandse spelers. In de periode 2006-2013 bedroeg de geschatte omzet 105 miljoen euro, de bruto spelopbrengst 40 miljoen euro. In het andere opsporingsonderzoek werden honderden Nederlandse spelers bediend. Vermoedelijk vergaarde het crimineel samenwerkingsverband in de periode 2011 tot en met 2014 jaarlijks een bruto spelopbrengst van ongeveer 800.000 euro.
De KSA schat de bruto spelopbrengst van de online kansspelen in Nederland voor 2015 op ruim 258 miljoen euro. Als het wetsvoorstel Kansspelen op afstand wordt aangenomen, dan wordt een groot deel van deze opbrengst legaal omdat de online kansspelmarkt dan is gereguleerd. De online kansspelmarkt groeit. Voor 2021 wordt de opbrengst uit online kansspelen geschat op ruim 388 miljoen euro.

1.14.3 Huidige gevolgen

Op de illegale kansspelmarkt ligt kansspelverslaving bij spelers op de loer. Illegale aanbieders voeren de in de Wet op de kansspelen opgenomen maatregelen en voorzieningen die 'onmatige deelneming' moeten tegengaan niet uit.
Onderzoek uit 2016 naar het aantal risico- en probleemspelers van kansspelen stelt dat Nederland 95.700 risicospelers ('mogelijk kansspelverslaafden') en 79.000 probleemspelers ('waarschijnlijk kansspelverslaafden') kent.[25] Afgaand op onderzoek uit 2011 kunnen we vaststellen dat ten minste 18.000 van dit soort spelers meedoen aan illegale kansspelen. Onderzoek uit 2015 wijst uit dat in 2014 ruim 2200 mensen hulp zochten voor gokverslaving. De vraag naar hulp vanwege gokproblemen is de afgelopen jaren licht gedaald. Het is onbekend hoe kansspelverslaving over de verschillende kansspelen is verdeeld.

Kansspelverslaving doet zich verhoudingsgewijs vaker voor bij niet-westerse allochtonen dan bij autochtonen. Het gaat daarbij vooral om Nederlanders met een Marokkaanse of Turkse achtergrond.

Illegale kansspelen gaan soms ook gepaard met geweldgebruik of dreiging daarmee. Dat blijkt uit incidenten waarbij gokkers uit de Chinese gemeenschap in Nederland geld lenen van groepen *loan sharks*, Chinese criminele groeperingen. Tegen hoge rentes lenen deze woekeraars geld aan gokkers met schulden. Als spelers achterblijven met het afbetalen van hun schulden, schuwen ze het gebruik van geweld niet. Ze houden zich ook bezig met andere vormen van criminaliteit.
Overlast door illegale kansspelen beperkt zich tot incidenten, bijvoorbeeld wanneer exploitanten of spelers van illegale bingo's, illegale lotto's en toto's of gokzuilen zich te nadrukkelijk manifesteren op locaties waar kansspelen plaatsvinden. Er zijn enkele tientallen politieregistraties waaruit blijkt dat omwonenden daar last van ondervinden. Daartegenover staat informatie waaruit blijkt dat illegale kansspelen als bingo, poker en lotto gemeengoed zijn geworden in veel wijken in Nederland. Veel exploitanten en spelers die zich in die wijken met

25 A. Kruize, M. Boendermaker, M. Sijtstra & B. Bieleman (2016). *Modernisering kansspelbeleid. Nulmeting 2016*. Groningen: Intraval.

deze spelen bezighouden, zien het als een vorm van vrijetijdsbesteding. De vraag of de kansspelen illegaal zijn of niet, doet niet ter zake. Iets vergelijkbaars geldt voor de gokzuilen, in de Turkse gemeenschap lijken die geaccepteerd.

De gevolgen van illegale kansspelen zijn vooral financieel van aard. Het Centraal Bureau voor de Statistiek (CBS) schat de opbrengst van illegale kansspelen in Nederland op 171 miljoen euro per jaar (peiljaar 2010). Door de groei van online kansspelen ligt die opbrengst nu waarschijnlijk hoger. De schade voor de overheid bestaat in het fiscale nadeel over dit bedrag – een bedrag dat, gebaseerd op de schatting van het CBS, vermoedelijk enkele tientallen miljoenen euro's bedraagt.

1.14.4 Verwachtingen

Hoe de illegale bingo's, lotto's en toto's zich in de nabije toekomst gaan ontwikkelen, valt op grond van de meldingen bij de KSA of de registratiecijfers bij de politie moeilijk te voorspellen. Enerzijds komt dat doordat het aantal registraties vrij beperkt is, anderzijds doordat het merendeel van de data geen duidelijke dalingen of stijgingen laat zien.
De illegale markt voor gokzuilen zal naar verwachting groeien. Meldingen van gokzuilen zijn de afgelopen jaren sterk gestegen. Ondanks een afvlakking in de afgelopen twee jaar wordt verwacht dat de populariteit voor gokzuilen aanhoudt. Mogelijk neemt die toe indien het wetsvoorstel Kansspelen op afstand wordt aangenomen. Dit wetsvoorstel wil gokkers verplichten hun identiteit prijs te geven als zij op gelegaliseerde websites gokken. Zij die dat willen vermijden en nog niet eerder op gokzuilen gokten, zouden daarop kunnen overstappen omdat op gokzuilen nog wel anoniem en met contant geld kan worden gegokt.

De nieuwe wet Kansspelen op afstand heeft ook andersoortige consequenties als het wetsvoorstel wordt aangenomen. Met de aanpassing van de wet krijgen buitenlandse kansspelaanbieders toegang tot de Nederlandse gokmarkt. Screening van buitenlandse aanbieders is moeilijker dan screening van binnenlandse aanbieders. Als dat ertoe leidt dat screening ook minder of minder adequaat wordt uitgevoerd, bestaat er een kans dat buitenlandse criminelen of criminele organisaties vergunningen krijgen en goksites zullen exploiteren.
De behoefte aan illegale online kansspelen blijft bestaan, ook na vergunning voor online kansspelen in Nederland. Dat komt vooral doordat er in het geval van illegale online kansspelen hoger kan worden ingezet, de anonimiteit van spelers gewaarborgd is en er geen belasting over speelwinst hoeft te worden betaald. Verder wordt verwacht dat illegale online kansspelaanbieders verschillen in wetgeving, en bestuurlijke en juridische verschillen tussen landen blijven misbruiken om hun criminele activiteiten voort te zetten. Ook hanteren ze een breed scala aan digitale technieken om geldstromen te verdoezelen. Het gaat dan bijvoorbeeld om het toestaan van betaling in virtuele valuta en het gebruik van *cross booking*. Hierbij wordt met spelers overeengekomen dat elke ingezette euro feitelijk een bedrag vertegenwoordigt van vijftig, honderd of duizend keer zo veel. Zo wordt de schijn gewekt dat er slechts met lage inzetten wordt gewed.

De verwachting is dat online kansspelen de fysieke kansspelen op termijn in omvang zullen overtreffen. Dat komt onder andere door de opkomst van nieuwe populaire online games als *e-sports* en *fantasy sports.* E-sports zijn videogame-competities waarbij individuele spelers of teams tegen elkaar strijden. In 2013 keken wereldwijd ruim 71 miljoen mensen naar e-sports. Op de uitslagen van e-sports kan worden gewed, en dat is erg populair.
Fantasy sports zijn games waarbij virtuele wedstrijden worden georganiseerd op basis van bestaande, echte sporten. Op de games wordt gegokt en ze ontwikkelen zich steeds meer in de richting van gokspelen. Vooralsnog is onbekend of fantasy sports in de toekomst zullen worden aangemerkt als behendigheidsspel (geen vergunning vereist) of als gokspel (wel een vergunning vereist).
Mogelijk ontstaat uit de markt van e-sports en fantasy sports een (illegale) gokmarkt waar ook de georganiseerde criminaliteit van wil profiteren. In Nederland lijkt daarvan vooralsnog geen sprake.

1.14.5 Kwalificatie van dreiging

Uit de gerapporteerde meldingen, registraties en opsporingsonderzoeken blijkt dat een aantal illegale kansspelen vanuit de overheid en de samenleving weinig last heeft van 'pottenkijkers'. Traditionele illegale kansspelen als illegale bingo's, lotto's en toto's kunnen zo jaren blijven voortbestaan. De markt voor gokzuilen lijkt enigszins te groeien. Verwacht wordt dat de kansspelmarkt op termijn steeds verder opschuift naar de online kansspelmarkt door een groeiende vraag. De toekomstige invoering van het wetsvoorstel Kansspelen op afstand faciliteert daarin. Hierdoor komen er mogelijkheden voor legaal aanbod van online kansspelen in Nederland en van aanbieders uit binnen- en buitenland. Dit laat onverlet dat illegaal aanbod van online kansspelen mogelijk blijft. Op welke manier en in welke mate de georganiseerde criminaliteit zich daar in de toekomst mee bezig zal houden, is vooralsnog onbekend.

De gevolgen die voortvloeien uit de illegale kansspelen zijn overwegend financieel van aard. Het CBS raamt de opbrengst uit illegale kansspelen op 171 miljoen euro per jaar (peiljaar 2010). Door de groei van online kansspelen – die op dit moment nog illegaal zijn – wordt die opbrengst nu waarschijnlijk hoger. De schade voor de overheid door derving van belastinginkomsten bedraagt, gebaseerd op de schatting van het CBS, enkele tientallen miljoenen euro's per jaar. Schade voor de deelnemers bestaat, ongeacht de vraag of het om legaal of illegaal gokken gaat, uit het verlies dat geleden wordt. Hier wordt het standpunt ingenomen dat het verlies inherent is aan het gokken, en gokkers nemen zelf het risico dat met gokken gepaard gaat. Het verlies van gokkers valt dus niet onder het begrip schade. Vergeleken met de totale opbrengst van kansspelen in Nederland is de financiële schade door illegale kansspelen beperkt. Indien het wetsvoorstel Kansspelen op afstand wordt aangenomen, zullen online kansspelen in Nederland grotendeels legaal worden. Illegale kansspelen worden derhalve gekwalificeerd als **geen concrete dreiging**.

2 Fraude en witwassen

2.1 Inleiding

In dit hoofdstuk zullen witwassen en diverse vormen van fraude behandeld worden, zowel van horizontale fraude, waarvan bedrijven en burgers slachtoffer zijn, als van verticale fraude, waarvan de overheid slachtoffer is. Behalve vele verschillen tussen deze verschijnselen, zijn er ook overeenkomsten. Het gaat vooral om het gebruik van katvangers[26] en het plegen van identiteitsfraude als hulpmiddel bij het uitvoeren van allerlei andere vormen van fraude. In vrijwel elk rapport dat ten grondslag ligt aan dit hoofdstuk komen ze aan de orde. Om te voorkomen dat deze werkwijzen bij elke fraudevorm en witwassen steeds opnieuw behandeld worden, bespreken we ze hier in de inleiding.

Het behandelen van de katvanger en identiteitsfraude onder de kop Fraude en witwassen wil niet zeggen dat beide fenomenen uitsluitend in deze categorieën georganiseerde criminaliteit voorkomen. Wel lijken ze echter bij uitstek op te duiken bij vormen van financieel-economische criminaliteit. De vraag dringt zich dan ook op waarom dat zo is. Een van de kenmerken van financieel-economische criminaliteit is dat deze zich afspeelt in het schemergebied tussen legaal en illegaal, tussen boven- en onderwereld. Voor het plegen van bijvoorbeeld hypotheek- of telecomfraude is het vrijwel een noodzakelijke voorwaarde onder een gefingeerde identiteit gebruik te maken van respectabele legale bedrijven of financiële instellingen. Voor het witwassen van crimineel geld worden bedrijven opgericht die op het oog een legale bedrijfsvoering hebben en zich in de openbaarheid begeven, maar ondertussen een katvanger als zogenaamde eigenaar hebben. Katvangers en identiteitsfraude zijn in dit opzicht in feite de beide kanten van dezelfde euro.

Katvangers

Katvangers, ook wel stromannen genoemd, worden op talloze manieren ingezet bij financieel-economische criminaliteit. Katvangers hebben geen unieke vaardigheden, maar worden door de crimineel simpelweg naar voren geschoven om de werkelijke zeggenschap of eigendomsverhouding te verhullen. De katvanger handelt voor de buitenwereld op eigen titel, maar fungeert in werkelijkheid als instrument van de crimineel. De crimineel weet daardoor officiële registratiesystemen te ontlopen. De inzet van katvangers leidt er in voorkomende gevallen toe dat de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur (Wet Bibob) omzeild wordt.

Van katvangers gaan er dertien in een dozijn. Het zijn vaak jongeren, scholieren, uitkeringsgerechtigden, verslaafden, veelal in geldnood, die tegen een geringe vergoeding hun bankrekeningnummer beschikbaar stellen, bankrekeningen of telefoonabonnementen op naam openen en bedrijven of rechtspersonen op naam zetten.

26 De betekenis van het woord *katvanger* is te herleiden tot het oud-Amsterdamse woord *kat*, dat bargoens is voor 'buit', vergelijk 'kat in 't bakkie'.

Door gebruik van zo'n 'tussenstation' is de identiteit van de criminelen moeilijker te achterhalen en vangen de katvangers de risico's op schulden of aanhoudingen op.
In het geval van *fraude met online handel* worden katvangers (moneymules) ertoe bewogen hun bankrekeningen ter beschikking te stellen of er een te openen. De inzet van katvangers bij fraude met online handel en fraude met betaalmiddelen laat zien dat niet meer alleen individuen met problemen voor een geringe vergoeding misbruikt worden. De katvangers worden geregeld ook via vacatures (online advertenties) gerekruteerd, soms zelfs met een sollicitatiegesprek. Zij worden niet geïnformeerd over hun aandeel in de fraude en krijgen goede vergoedingen voor hun werkzaamheden. Om een indruk te geven: in 2012 zijn bankrekeningen onderzocht, en daaruit bleek dat 6500 bankrekeningen gebruikt werden voor het wegsluizen van geld uit fraude met internetbankieren. Daarbij waren 3600 katvangers betrokken.
In het geval van *acquisitiefraude* worden ze ertoe bewogen om bedrijven (eenmanszaken) op naam te zetten en bankrekeningen te openen. Soms blijft de handeling beperkt tot het openen van bankrekeningen waar het criminele geld op gestort wordt. De katvangers nemen het geld op, sluizen dat door naar andere rechtspersonen, naar het buitenland of naar de criminele leiding. Ze werken op deze manier mee aan belastingfraude en aan het witwassen van de criminele inkomsten.
Bij *hypotheekfraude* en ABC-constructies gebruiken criminelen katvangers om panden niet op eigen naam te hoeven zetten. De katvangers worden doorgaans onder druk gezet om mee te werken en/of ontvangen een geringe vergoeding.
Ook bij *telecomfraude* en *huur-, zorg-* en *toeslagfraude* wordt gebruikgemaakt van katvangers. Vaak zijn dat Bulgaren en Roemenen die met bussen naar Nederland worden gebracht en zich hier laten inschrijven in het bevolkingsregister van allerlei plaatsen in het land. Vervolgens vragen zij om hun Bulgaars of Roemeens rijbewijs om te wisselen naar een Nederlands rijbewijs en openen zij daarmee online een bankrekening. Daarna wordt 'onder toezicht' massaal fraude gepleegd op bovenstaande terreinen.
Ook bij *verzekeringsfraude, accijnsfraude, btw-fraude* en *faillissementsfraude* wordt ruimhartig gebruikgemaakt van katvangers.

Identiteitsfraude
Identiteitsfraude wordt bij vrijwel alle hoofdvormen van horizontale fraude toegepast om de eigen identiteit af te schermen en/of andermans identiteit te misbruiken. Het stelt fraudeurs in staat om korte of lange tijd onzichtbaar te blijven en het kost meer moeite ze op te sporen, omdat bij de opsporing vaak anderen, namelijk katvangers, in beeld komen. Katvangers en het afschermen van de eigen identiteit gaan zo hand in hand. Identiteitsfraude is vaak een logische stap in het criminele proces en het is bijna een noodzakelijke voorwaarde voor het succesvol bedrijven van criminaliteit.
Internet heeft het misbruik van identiteiten talloze mogelijkheden gegeven. We zien allerlei vormen van cybercrime, waarbij ICT (internet of e-mail) wordt gebruikt om onder een valse identiteit personen en bedrijven te benaderen en/of op te lichten.

Het Centraal Meldpunt Identiteitsfraude en -fouten (CMI) van het Ministerie van Binnenlandse Zaken heeft een enquête gehouden onder de volwassen bevolking waarin werd gevraagd of iemand zich wel eens zonder toestemming had voorgedaan als de ondervraagde (bijvoorbeeld om iets te kopen). In 2014 en 2015 gaf respectievelijk 2,1 en 3,4 procent aan hiervan slachtoffer te zijn geweest. Omgerekend naar aantallen, gaat het om enkele honderdduizenden slachtoffers die met verschillende vormen van identiteitsfraude geconfronteerd werden. Ruim 80 procent van de slachtoffers gaf aan geen financiële schade te hebben opgelopen. De slachtoffers die wel schade hebben opgelopen, melden zeer uiteenlopende bedragen. Het gemiddelde is ongeveer 650 euro. Lang niet alle slachtoffers doen aangifte of maken melding van identiteitsfraude. In 2015 hebben zich 800 Nederlanders bij het CMI gemeld die slachtoffer waren van identiteitsfraude. In 2014 ging het om 844 meldingen. Vergeleken met de percentages uit de slachtofferenquête zijn dit bescheiden aantallen, aangenomen moet worden dat het hier om de ernstige gevallen gaat. Identiteitsfraude is weliswaar wijdverbreid, maar in lang niet alle gevallen gaat het om fraude ter facilitering van het criminele bedrijf. Er zijn verschillende gedaanten waarin identiteitsfraude zich voordoet:

- overname van identiteitsgegevens: het overnemen en misbruiken van iemands identiteitsgegevens, zonder toestemming van de persoon. De fraudeur weet andermans identiteitsgegevens frauduleus te bemachtigen en lift vervolgens onrechtmatig op deze identiteit mee;
- identiteitsdelegatie: medegebruikmaken van iemands identiteit, met toestemming van die persoon. Wie een andere persoon inschakelt voor het afleggen van zijn examen of voor het wederrechtelijk verkrijgen van een dienst, maakt zich schuldig aan identiteitsdelegatie;
- identiteitsruil: gebruikmaken van de identiteit van een ander met toestemming van die persoon. Er is sprake van identiteitsruil als persoon A zich geheel kan uitgeven voor persoon B, omdat A alle identificerende persoonsgegevens van B gebruikt. Persoon A gaat hierbij als persoon B door het leven;
- identiteitscreatie: het creëren van een fictieve identiteit, al dan niet met gedeeltelijke identiteitsgegevens van bestaande personen.

Bovengenoemde opzettelijke identiteitsveranderingen gebeuren veelal door middel van valse of vervalste documenten.

2.2 Acquisitiefraude

2.2.1 Inleiding

De basis voor deze paragraaf over acquisitiefraude vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar negen vormen van horizontale fraude, acquisitiefraude is er daar een van. Dat onderzoek is voor dit dreigingsbeeld uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, allen werkzaam

bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Bij acquisitiefraude is sprake van misleidende handelspraktijken tussen organisaties. Ondernemers worden met aanbiedingen overgehaald om een contract te tekenen waaruit dan een aanzienlijke betalingsverplichting ontstaat, terwijl er geen of slechts een geringe prestatie tegenover staat. Een klassiek voorbeeld van acquisitiefraude betreft het aanbod om een advertentie of naamsvermelding in een bedrijvengids of op internet te plaatsen. Het draait bij acquisitiefraude niet alleen om het verwerven van opdrachten, maar ook om het uitlokken van onverschuldigde betalingen door middel van spooknota's.

2.2.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

Recent doen zich ontwikkelingen voor bij drie vormen van acquisitiefraude: spooknota's, factuurfraude en CEO-fraude. Nieuw is verder de opleving van het telefonisch benaderen van slachtoffers.

Spooknota's nemen tegenwoordig een grotere plaats in dan klassieke acquisitiefraude. In het geval van een spooknota stuurt de fraudeur ongevraagd en zonder juridische basis facturen aan potentiële slachtoffers. Tegenwoordig ontvangen niet alleen bedrijven dergelijke spooknota's, maar ook particulieren zijn steeds vaker doelwit. Fraudeurs versturen facturen van voorgewende geleverde prestaties van bedrijven of organisaties die feitelijk niet bestaan, maar ook voor zogenaamd uitgevoerde diensten van daadwerkelijk bestaande bedrijven of organisaties. Vaak bevatten deze facturen tekst in kleine lettertjes onder aan de factuur waarin vermeld wordt dat het om een aanbieding gaat. Slachtoffers zien dit over het hoofd en betalen klakkeloos; vanwege de tekst in de kleine lettertjes is deze vorm van misleiding juridisch moeilijk aan te pakken. De facturen worden tegenwoordig meestal digitaal verzonden en zijn op naam gesteld (naam, adres, woonplaats). Particulieren krijgen bijvoorbeeld namens het Centraal Justitieel Incassobureau (CJIB) bekeuringen op naam gestuurd.

Factuurfraude (ook wel overboekingsfraude genoemd) is een variant van acquisitiefraude waarbij een bestaande factuur ergens in het traject van versturen van bedrijf naar klant wordt onderschept en waarbij vervolgens het rekeningnummer waarop het verschuldigde bedrag moet worden geboekt, wordt gewijzigd in dat van de fraudeur. In het verleden werden facturen uit de brievenbus gehengeld, waarna de fraudeur het rekeningnummer veranderde zodat het geld rechtstreeks naar hemzelf werd overgemaakt. Tegenwoordig worden facturen ook binnen bedrijven onderschept en gewijzigd door een frauderende medewerker.

Bij CEO-fraude ontvangt een medewerker van een groot bedrijf een e-mail of telefoontje van de hoogste baas, de Chief Executive Officer (CEO), waarin deze hem of haar opdraagt om een urgente vertrouwelijke betaling uit te voeren en het bedrag over te maken naar een buitenlandse rekening. De medewerker kan bijvoorbeeld een manager zijn of een medewerker van de boekhouding. Ter verificatie van de gegevens kan deze desgewenst een advocatenkantoor bellen dat in het complot zit. Het e-mailadres van de zogenaamde CEO lijkt veel op dat van de echte CEO. Fraudeurs maken gebruik van onzekerheid bij medewerkers en wenden bijvoorbeeld voor dat het om een grote aankoop of een strategische acquisitie gaat waarbij vertrouwelijkheid, strikte geheimhouding en snelheid van handelen vereist zijn. De kans op het slagen van CEO-fraude neemt toe met de omvang van het bedrijf, omdat in grote bedrijven de medewerkers elkaar niet allemaal kennen en vaak geen persoonlijk contact hebben met de hoogste baas.

Het contact tussen fraudeur en slachtoffer verloopt tegenwoordig doorgaans langs digitale wegen. Het is dan ook opmerkelijk dat de laatste tijd sommige fraudeurs de voorkeur geven aan het telefonisch benaderen van slachtoffers. Dit heeft wellicht te maken met preventieve maatregelen die worden getroffen om digitale oplichting te voorkomen en met voorlichting die wordt gegeven waardoor mensen zich steeds beter bewust zijn van digitale gevaren. Een voorbeeld van deze werkwijze is de nepdeurwaarder die bedrijven telefonisch benadert met een dringend betalingsverzoek van duizenden euro's voor een (niet-bestaande) bedrijvengids. Te kennen gegeven wordt dat bij gebrek aan betaling de volgende dag alle bankrekeningen van de benaderde bedrijven geblokkeerd zullen worden. Nadat het televisieprogramma *Opgelicht?!* aandacht besteedde aan deze werkwijze, zijn vijf verdachten aangehouden. Het is onduidelijk of deze werkwijze, waarbij intimidatie een stevige rol speelt, bredere toepassing gaat krijgen.

Omvang

De Fraudehelpdesk krijgt al jaren tussen de 3000 en 4000 meldingen per jaar voor klassieke acquisitiefraude (zie tabel 6). Voor spooknota's kwamen in 2014 en 2015 meer meldingen binnen dan voor klassieke acquisitiefraude: respectievelijk 9500 en 8300. In 2015 is voor het eerst onderscheid gemaakt tussen spooknota's aan bedrijven en spooknota's aan particulieren. Bij ruim een op de vijf meldingen in dat jaar is het beoogde slachtoffer een particulier.

Het aantal betalende slachtoffers is veel kleiner dan het aantal meldingen. Op grond van de cijfers over 2014, betaalt bij klassieke acquisitiefraude nog geen 4 procent van de slachtoffers, bij spooknota's ligt dat percentage iets hoger (ruim 4 procent). Het bedrag dat betalende slachtoffers afhandig gemaakt wordt, is in geval van spooknota's gemiddeld lager dan bij klassieke acquisitiefraude. Over de omvang van CEO-fraude en factuurfraude is weinig bekend.

Tabel 6. Acquisitiefraude: aantal melders en betalingen voor klassieke acquisitie en spooknota's

		Aantal melders	Aantal betalers	Gemiddelde betaling (€)	Totaalbedrag betalingen (€)
Klassiek	2014	3.700	143	364	52.000
	2015	3.100	200	**	**
Spooknota's	2014	9.500	190	147	28.000
	2015	*8.300	600	118	71.000

* van wie 1800 particulieren
** online opgaven van betaalde bedragen waren in 2015 onbetrouwbaar

2.2.3 Huidige gevolgen

De melders van acquisitiefraude zijn vooral kleinere bedrijven. Voor zulke bedrijven is de impact relatief groot. Wel neemt volgens experts het aantal particulieren dat zich meldt toe; daarover zijn pas sinds 2015 cijfers bekend, waardoor nog niets over ontwikkelingen gezegd kan worden.

Slachtoffers van acquisitiefraude voelen zich bedrogen en opgelicht. De gevolgen liggen niettemin hoofdzakelijk op het financiële vlak. De bedragen uit tabel 6 tonen de schade van de gemelde gevallen van acquisitiefraude. Er is sprake van een omvangrijk dark number. Onderzoek laat zien dat wanneer een delict op internet plaatsvindt de kans op het doen van melding of aangifte klein is. De schatting van een expert van de Fraudehelpdesk is dat 90 tot 95 procent van de slachtoffers geen aangifte doet. Uitgaande van een meldingspercentage van 10 procent, resulteert dit in een gemiddelde jaarlijkse financiële schade van ongeveer 2 miljoen euro.

De schade van bedrijven als gevolg van CEO-fraude is hier buiten beschouwing gelaten. Hoewel er in individuele gevallen grote bedragen mee gemoeid kunnen zijn, is er over dit nieuwe fenomeen nog te veel onbekend om de omvang van de schade te kunnen schatten. Er is ook geen zicht op de schade door factuurfraude.

2.2.4 Verwachtingen

De beschikbare cijfers over acquisitiefraude vormen een wankele basis om er toekomstverwachtingen op te baseren. Het gebrek aan consistente registratie ontneemt niet alleen het zicht op de ontwikkelingen van de meldingen in het afgelopen decennium, maar ook valt hierdoor de mogelijkheid weg om door extrapolatie van historische gegevens de toekomstige omvang in te schatten.

Bij de aanpak van acquisitiefraude staat publiek-private samenwerking centraal. Er wordt gewerkt aan voorlichting, preventie en het verbeteren van de inzet van het strafrecht. Om met dat laatste te beginnen, in januari 2016 is het initiatiefwetsvoorstel Strafbaarstelling Acquisitiefraude aangenomen door de Eerste Kamer. Dit voorstel behelst onder meer dat

ondernemers onder een overeenkomst uit kunnen komen als die via een 'misleidende omissie' tot stand is gekomen. Een misleidende omissie is het weglaten of verborgen houden van belangrijke informatie bij het aangaan van een transactie waardoor het als onrechtmatig handelen kan worden aangemerkt. Acquisitiefraude tegen ondernemers is strafbaar gesteld met een gevangenisstraf van maximaal twee jaar. De wetswijziging is per 1 juli 2016 van kracht. Daarnaast wordt al jaren ingezet op preventie. Instanties zoals de Fraudehelpdesk, het Ondernemersplein en VNO-NCW/MKB waarschuwen burgers en bedrijven voor (acquisitie) fraude. In de media is aandacht voor slachtoffers, bijvoorbeeld in het televisieprogramma *Opgelicht?!*.
Tegenwoordig kunnen bedrijven software aanschaffen om de uitgaande geldstroom te controleren. Door verbanden te leggen tussen gegevens uit bijvoorbeeld het betaalbestand, het personeelsbestand en het crediteurenbestand kunnen onregelmatigheden worden geconstateerd en kan acquisitiefraude worden voorkomen.

Door de combinatie van voorlichting, preventie, wetgeving en eigen maatregelen van bedrijven zal het aantal gevallen van acquisitiefraude binnen de perken blijven. Het aantal betaalde spooknota's zal naar verwachting eerder dalen dan toenemen. Wel zou tijdelijk het aantal spooknota's richting particulieren nog verder kunnen toenemen. De voorlichting die erop gericht is te waarschuwen voor deze oplichtingspraktijk, zal meer bewustzijn kweken waardoor minder burgers erin zullen trappen. De traditionele acquisitiefraude zal vermoedelijk op hetzelfde niveau blijven: ongeveer vierduizend meldingen per jaar, met een beperkt aantal betalende slachtoffers. De te verwachten ontwikkelingen omtrent factuurfraude en het telefonisch benaderen van slachtoffers zijn ongewis.

CEO-fraude komt vooral voor in landen waar in bedrijven strakke hiërarchische verhoudingen bestaan en de CEO ook echt de baas is. In Nederland bestaat wellicht een meer egalitaire cultuur, waardoor werknemers minder geneigd zijn klakkeloos uit te voeren wat de baas verordonneert. Grote bedrijven doen aan *compliance management* waarmee onder meer aandacht wordt besteed aan intern beleid en procedures en het voorkomen van fraude.
Bedrijven zijn erbij gebaat hier serieus werk van te maken vanwege de afbreuk die fraude doet aan het imago van het bedrijf. Al met al bestaat de verwachting dat CEO-fraude in Nederland zich niet tot een omvangrijk probleem gaat ontwikkelen.

2.2.5 Kwalificatie van dreiging

De schade van acquisitiefraude is hoofdzakelijk financieel van aard en wordt geschat op 2 miljoen euro per jaar.
De Fraudehelpdesk verwacht de komende periode geen grote verschuivingen. Deze verwachting is vooral gebaseerd op het tamelijk stabiele beeld dat deze vorm van fraude al jarenlang te zien geeft. Voorlichting, preventie, wetgeving en eigen maatregelen van bedrijven dragen ertoe bij dat het aantal gevallen van acquisitiefraude ook de komende jaren binnen de perken zal blijven. Gegeven de relatief geringe huidige en verwachte omvang van de schade vormt acquisitiefraude **geen concrete dreiging** voor de komende jaren.

2.3 Hypotheekfraude

2.3.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017.* Dat rapport is een verslag van onderzoek naar negen vormen van horizontale fraude, hypotheekfraude is er daar een van. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, alle drie werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf wordt de kwalificatie van dreiging beschreven. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is beargumenteerd en vastgesteld in een andere context door een groep van beoordelaars (de consensusgroep).

Hypotheekfraude bestaat uit het op oneigenlijke en/of valse gronden verkrijgen van een hypothecaire lening om onroerend goed aan te schaffen. Hypotheekfraude is facilitair aan allerlei andere criminele activiteiten, zoals witwassen, hennepteelt, illegale verhuur, uitbuiting en het *stashen* van drugs.

Een bijzondere vorm van hypotheekfraude is depotfraude. Bij deze fraude wordt een bouwdepot leeggehaald met behulp van valse facturen. Een bouwdepot is een lening waarmee de bouw of verbouw van een onroerend goed wordt bekostigd.

2.3.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

In 2014 is in totaal 238 keer aangifte gedaan van hypotheek- of depotfraude. In de drie daaraan voorafgaande jaren (2011-2013) lag het aantal aangiften op hetzelfde niveau. Er zijn veel meer aangiften van hypotheekfraude dan van depotfraude, die daarmee regelmatig samengaat. Bij de Stichting Fraude Hypotheken zijn in 2013 bijna 700 gevallen gemeld, zo'n 300 geslaagde en bijna 400 pogingen tot hypotheekfraude. Deze fraudegevallen betreffen een fractie van de honderdduizenden hypotheken die jaarlijks verstrekt worden. In 2015 waren dat er 253.000 met een totale waarde van 62 miljard euro. Bij een vergelijkbaar aantal aangiften van fraude als in eerdere jaren is dat nog geen promille van het totale aantal verstrekte hypotheken.

Aard

In de aard van hypotheekfraude en depotfraude is de afgelopen jaren weinig veranderd. De kern blijft het falsificeren van gegevens (documenten) op basis waarvan hypotheken worden verstrekt of betalingen uit bouwdepots worden gedaan. Het gaat dan om het vervalsen of valselijk opmaken van loon- en inkomensgegevens, identiteitsbewijzen, offertes en facturen voor bouw en verbouwing. De belangrijkste ontwikkeling daarbij is dat de geldverstrekker de informatie steeds vaker digitaal aangeleverd krijgt. Met behulp van verschillende software is het voor criminelen mogelijk om de benodigde falsificaten te maken. Fraudeurs

maken gebruik van steeds betere vervalsingen en betrekken schijnconstructies met werkgevers bij de fraude. Controle op de geleverde digitale documenten is niet eenvoudig, doordat de gefalsificeerde documenten zeer professioneel zijn vervaardigd en moeilijk van echt zijn te onderscheiden. Via internet is het eenvoudig om aan vervalsingen van de benodigde documenten te komen.

Andere verschuivingen in modus operandi doen zich voor als reactie op veranderingen die banken doorvoeren bij het al dan niet toekennen van een hypotheekaanvraag. Fraudeurs trekken lering uit mislukte aanvragen en passen zich daarop aan.

2.3.3 Huidige gevolgen

De huidige schade is vooral financieel en bedraagt volgens schatting van de Stichting Fraude Hypotheken 20 tot 30 miljoen euro per jaar. Dit schadebedrag is ongeveer 0,004 procent van de totale hypotheekschuld in Nederland. Deze schade treft vooral de geldverstrekkers als fraudeurs niet meer aan de hypotheekverplichtingen voldoen en treft de overheid als er gebruik wordt gemaakt van hypotheekrenteaftrek bij onterecht verstrekte hypotheken. De hypotheekverstrekkers lopen daarnaast het risico dat het onderpand een te lage waarde heeft omdat er gesjoemeld is met de taxatie of als gevolg van criminele exploitatie, bijvoorbeeld een hennepplantage in de woning, met alle schade van dien.

De personen die op papier als eigenaar van de huizen fungeren, kunnen als gevolg van betrokkenheid bij de hypotheekfraude met een restschuld blijven zitten. Daarnaast zijn deze stromannen of katvangers betrokken bij criminele activiteiten waarvoor zij medeverantwoordelijk kunnen worden gehouden. Naast persoonlijke misère worden eventuele kosten van schuldsanering op de samenleving afgewenteld omdat niet alle schulden hoeven te worden afgelost.

De maatschappelijke schade wordt vooral veroorzaakt door de criminele exploitatie die gefaciliteerd wordt door hypotheekfraude. Bij deze criminele exploitatie gaat het vooral om hennepteelt, mensenhandel en verhuur aan illegalen. Omwonenden ondervinden hier overlast van en huurders worden uitgebuit met te hoge huren, te veel huurders in één ruimte en slecht onderhouden woningen. Het gevolg is dat in buurten waar dit veel voorkomt de leefbaarheid wordt aangetast.

2.3.4 Verwachtingen

De aanvraag van hypotheken zal de komende jaren steeds meer online gebeuren. Dit gebeurt vooral vanuit het oogpunt van klantvriendelijkheid (snelle afhandeling) en efficiency bij de verwerking (kostenbesparing). Vanwege een toenemende concurrentie op de hypotheekmarkt zijn kostenbesparingen wenselijk. Waarschijnlijk zullen aanvragen steeds vaker zonder tussenpersoon gaan plaatsvinden en kunnen klanten via apps op basis van hun persoonlijke situatie een online advies krijgen. In eerste instantie zullen hier nog voorwaarden aan gesteld worden, zoals een bepaald kennisniveau van financiële producten dat online

getest wordt. Het is moeilijk te voorspellen, maar het is niet uitgesloten dat het verlies van direct contact met de klant de frauderisico's eerder zal versterken dan afzwakken. Toch zal dat de komende jaren waarschijnlijk niet tot grote veranderingen leiden. Deze ontwikkelingen hebben zich deels al wat eerder ingezet, terwijl het aantal aangiften de afgelopen jaren redelijk stabiel is gebleven evenals het aantal rechtspersonen dat hypotheekfraude pleegt. Dat zal de komende jaren naar verwachting zo blijven en leiden tot gevolgen voor de Nederlandse samenleving die vergelijkbaar zijn met de huidige.

2.3.5 Kwalificatie van dreiging

Evenmin als in het Nationaal dreigingsbeeld van 2012 worden er de komende jaren grote veranderingen verwacht in aard en omvang van hypotheekfraude. De totale gevolgen voor de Nederlandse samenleving zijn relatief beperkt. Hypotheekfraude (inclusief depotfraude) is daarom gekwalificeerd als **geen concrete dreiging** voor de Nederlandse samenleving in de komende vier jaar.

2.4 Beleggingsfraude

2.4.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van een onderzoek naar negen vormen van horizontale fraude in Nederland, beleggingsfraude is er daar een van. Dat onderzoek is voor dit dreigingsbeeld in de eerste helft van 2016 uitgevoerd. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, die alle drie werkzaam zijn bij de politie. De bronnen die bij dit onderzoek zijn gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Er is sprake van beleggingsfraude wanneer burgers en bedrijven verleid worden te beleggen in producten die niet bestaan, waardeloos zijn of rendementen beloven die opgebracht moeten worden door nieuwe deelnemers, zogenoemde piramidespelen.

2.4.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

Bij beleggingsfraude worden drie hoofdvormen onderscheiden: boilerroomfraude, Ponzizwendel en piramidespelen.
Boilerroomfraude ontleent zijn naam aan de boilerroom, meestal een (relatief) klein kantoor in het buitenland, van waaruit mensen telefonisch benaderd worden om geld te investeren. Doordat de potentiële klanten de telefoongesprekken van de andere medewerkers op de achtergrond kunnen horen, wordt de indruk gewekt dat er een succesvol en betrouwbaar bedrijf actief is. Om potentiële klanten over te halen geld in te leggen, worden hun hoge

rendementen in het vooruitzicht gesteld. In werkelijkheid blijkt het vaak om waardeloze aandelen te gaan. Soms worden ook niet-bestaande aandelen verkocht of worden andere financiële producten aangesmeerd, zoals financiële derivaten. In alle gevallen worden er grote sommen geld verloren.
Ponzi-zwendel is vernoemd naar de oplichter Charles Ponzi. Het is een vorm van klassieke beleggingsfraude waarbij investeerders wordt voorgehouden dat hun geld lucratief wordt belegd. In werkelijkheid wordt niets of slechts een (klein) deel van de ingelegde gelden belegd. De vooraf afgesproken (hoge) rendementen worden betaald met de inleggelden van latere investeerders.
Piramidespelen verschillen weinig van de hierboven genoemde Ponzi-zwendel. Het voornaamste verschil is dat de deelnemers geacht worden zelf nieuwe deelnemers aan te brengen. De 'voet' van de piramide betaalt het rendement van de top.

Sinds het NDB2012 zien we een tweetal nieuwe fenomenen die allebei mogelijkheden voor beleggingsfraude bieden: *foreign exchange* handel (*forex trade*) en binaire opties. Bij *forex trade* gaat het om de (dag)handel in vreemde valuta, speculerend op koersschommelingen, waarbij beleggers veel meer geld kunnen verliezen dan ze ingelegd hadden (hefboomwerking). De afgelopen jaren is het aantal investeringen in de forex trade gestegen, mede omdat het laagdrempelig is om via online platforms virtuele valutaderivaten aan te schaffen. Hoewel we de omvang van fraude met forex trade niet kennen, zijn er voorbeelden bekend van het toepassen van de boilerroomconstructie om slachtoffers over te halen deel te nemen.

Binaire opties zijn een riskant beleggingsproduct met een lage financiële en technische instapdrempel. Deelnemers doen een voorspelling van de koers van een onderliggende waarde (aandelen, een wisselkoers of een index). Bij een goede voorspelling wordt een vast bedrag uitbetaald; als de voorspelling niet uitkomt, is de hele inleg verloren. De kans op het maken van winst op lange termijn is nihil. In de voorwaarden staat dat de aanbieders de koersen moeten volgen, maar dat gebeurt lang niet altijd en voor consumenten is vrijwel niet te controleren welke koers gevolgd is bij het vaststellen van winst of verlies. De Autoriteit Financiële Markten (AFM) waarschuwt consumenten tegen binaire opties en ook de Kansspelautoriteit (de toezichthouder op het gebied van kansspelen) heeft hier aandacht voor omdat het kenmerken van een kansspel heeft.

Omvang

In 2012 werd de omvang van beleggingsfraude op 500 miljoen euro geschat. Deze schade kwam vooral voor rekening van particuliere beleggers. Als gevolg van de financiële crisis is het aantal particuliere beleggers in de jaren na 2012 sterk afgenomen. In 2014 belegden ongeveer 770.000 huishoudens op de beurs. Enkele jaren daarvoor bedroeg dit aantal anderhalf miljoen. Inmiddels stappen weer meer particulieren in de markt. Onder andere door de vergrijzing neemt het aantal oudere beleggers toe. Zij gebruiken beleggingen als pensioenvoorziening.

Door het internationale karakter van beleggingsfraude ontbreekt een precies beeld van de schade. De AFM schat de schade op enkele honderden miljoenen euro's.

In vijf opsporingsonderzoeken is de omvang van de schade berekend op zo'n 100 miljoen euro.
In de eerste zaak zouden inleggelden grotendeels in Duits vastgoed belegd worden. Met de huuropbrengsten van de aangekochte panden zou het rendement van de beleggers worden betaald. In totaal werden 700 beleggers gedupeerd. De fraudeurs zouden in totaal 43 miljoen euro hebben opgehaald.
In een tweede zaak werden ook hoge rendementen voorgeschoteld rondom de aankoop van vastgoed. De fraudeurs zouden ongeveer 12 miljoen euro hebben verduisterd. Ze hadden in totaal ongeveer 27,5 miljoen aan ingelegde gelden van particulieren ontvangen. De rendementen die aan de beleggers werden uitgekeerd, waren vooral afkomstig uit inleggelden van nieuwe beleggers. Bij deze beleggingsfraude waren 580 gedupeerden betrokken, die gemiddeld ruim 47.000 euro hadden ingelegd.
Het derde voorbeeld betreft een boilerroomfraude. Beleggers werden gedurende een periode van zes maanden benaderd via internet en telefoon voor de aankoop van aandelen. Na de transactie bleken de aandelen waardeloos te zijn of helemaal niet te bestaan. De AFM sprak van een substantieel aantal gedupeerden die bedragen hadden ingelegd van 6000 tot 700.000 euro. De totale omvang van de schade is naar schatting minimaal enkele tientallen miljoenen euro's.
In een vierde zaak zijn beleggers misleid met een investering in zonne-energie. De investeringen zouden gegarandeerd zijn via een garantiefonds dat niet bleek te bestaan. Het Nederlandse bedrijf dat de beleggingen beheerde, is failliet gegaan en de beleggers hebben hun inleg plus rendementen niet teruggekregen. In totaal is bij deze fraude ongeveer 8,5 miljoen euro ingelegd door 314 beleggers. Het gemiddelde ingelegde bedrag komt daarmee op ruim 27.000 euro.
De laatste zaak heeft betrekking op verschillende fondsen in onroerend goed in Duitsland. Het leek een aantrekkelijk investeringsdoel dat weinig argwaan wekte, omdat ook verschillende media de afgelopen jaren berichtten over de Duitse huizenmarkt die (flink) in de lift zou zitten. Gedupeerden legden in totaal 24 miljoen euro in, waarvan een (groot) deel werd overgemaakt naar rekeningen van fraudeurs.

De veronderstelling is dat de schade door beleggingsfraude de afgelopen jaren zo'n 300 miljoen euro per jaar bedroeg.

2.4.3 Huidige gevolgen

De gevolgen van beleggingsfraude zijn ten opzichte van het vorige Nationaal dreigingsbeeld nagenoeg gelijk gebleven. De slachtoffers zijn in de meeste gevallen particuliere beleggers. Zij verliezen vaak grote sommen geld, soms oplopend tot tienduizenden of in enkele gevallen honderdduizenden euro's. De impact die dat heeft verschilt van persoon tot persoon en kan zich zowel fysiek als psychisch manifesteren. Bij de een is de schade als gevolg van

beleggingsfraude te overzien, maar in veel gevallen overstijgen de verliezen de draagkracht van het slachtoffer. Tevens wordt het vertrouwen van veel mensen geschaad, en ook breder kan het vertrouwen in maatschappelijke en financiële instanties geschaad worden.

2.4.4 Verwachtingen

Er zijn geen aanwijzingen dat de omvang van beleggingsfraude in de komende vier jaar veel zal dalen ten opzichte van het huidige niveau. De verwachting is dat – vanwege de lage rentestand – het aantal particuliere beleggers zal toenemen in de komende jaren, evenals het aantal producten waarin zij vooral via internet kunnen beleggen. Zelfs als deze ontwikkeling niet leidt tot een (flink) groter aantal slachtoffers, blijft het probleem hoogstwaarschijnlijk onverminderd omvangrijk. Bovendien is de aanpak van beleggingsfraude lastig gebleken als gevolg van het grensoverschrijdende karakter.
De AFM zal de inzet op preventie, waaronder voorlichtingscampagnes, continueren. Het effect is dat mensen minder vaak in mooie aanbiedingen trappen en dat zij hoge rendementen wantrouwen. Fraudeurs spelen hierop in door rentepercentages (rendementen) zodanig aan te passen dat ze wel aanlokkelijk zijn, maar geen argwaan wekken. Voor de economische crisis heerste een ander beeld van een hoog rendement, nu zijn voorgespiegelde rendementen van 4 procent al zeer risicovol te noemen door de lage rentestand. Dit wordt door sommige beleggers niet zo ervaren, waardoor het de fraudeurs toch lukt om slachtoffers over de streep te trekken.

2.4.5 Kwalificatie van dreiging

Voor de komende jaren blijft de schade van beleggingsfraude onverminderd hoog. In de eerste plaats is de kredietcrisis (vrijwel) achter de rug en lijkt het economische tij op groei te wijzen. Hierdoor neemt het vertrouwen in de markt toe en zullen particulieren meer gaan beleggen. Door de lage rente levert een spaarrekening vrijwel geen rendement op, en een deel van het spaargeld zal belegd gaan worden in al dan niet malafide fondsen en ondernemingen. Tevens zullen zich nieuwe vormen van beleggen voordoen die door het gebruik van internet een lage instapdrempel hebben. Gegeven de omvang van de huidige financiële schade en de verwachtingen voor de komende jaren wordt beleggingsfraude gekwalificeerd als **dreiging.**

2.5 Faillissementsfraude

2.5.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017*. Dat rapport is een verslag van onderzoek naar negen vormen van horizontale fraude, faillissementsfraude is er daar een van. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, die alle drie werkzaam zijn bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*

Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Van faillissementsfraude is sprake als een faillissement opzettelijk wordt misbruikt om financieel gewin te behalen. Er worden twee vormen onderscheiden:

1. Een onderneming wordt gestart en gefailleerd met het oogmerk schuldeisers door een faillissement te benadelen.
2. Een bestaande onderneming gaat niet vooropgezet failliet en voor of tijdens het faillissement worden illegaal activa aan de boedel onttrokken.

De georganiseerde vormen van faillissementsfraude worden uitgevoerd door beroepsfraudeurs en die worden vooral geassocieerd met de eerste vorm.

2.5.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

De krediet- en landencrises hebben de afgelopen jaren een zwaar stempel gedrukt op het economisch tij. Volgens cijfers van het Centraal Bureau voor de Statistiek (CBS) liep in de periode 2008-2013 het aantal faillissementen op van ongeveer 7000 in 2008 tot ruim 12.000 in 2013. Het aantal uitgesproken faillissementen bereikte zijn hoogtepunt in 2013. Daarna is er sprake van een dalende trend, in 2015 waren er 7338 faillissementen.
Faillissementsfraude is in Nederland een veelvoorkomende vorm van fraude. Het percentage van faillissementen waarbij schuldeisers zeker of waarschijnlijk strafrechtelijk of onrechtmatig benadeeld zijn, is gestegen van 24 procent in 2010 tot 30 procent in 2015.[27] Dit komt voor 2015 neer op zo'n 2200 faillissementen waarbij gefraudeerd is. Bij 25 procent van die faillissementen, zo'n 540, gaat het om hoge bedragen en hierbij zijn meestal, zo blijkt uit onderzoeken, beroepsfraudeurs betrokken.

Aard

Er hebben zich de afgelopen jaren verschillende ontwikkelingen voorgedaan die mogelijkheden bieden voor beroepsfraudeurs. Deze ontwikkelingen spelen ook de komende jaren een rol: turboliquidaties en prepackfaillissementen.

Bij een turboliquidatie wordt een rechtspersoon ontbonden door de Kamer van Koophandel zonder dat er een officieel faillissement plaatsvindt. En omdat het geen faillissement is, komt er geen curator aan te pas waardoor er ook geen melding wordt gedaan van mogelijke faillissementsfraude en volgt er ook geen nader onderzoek. De advieswereld heeft hier handig op ingespeeld; diverse juridische advieskantoren hebben zich gespecialiseerd in turboliquidaties. De scheidslijn tussen wettelijk en niet-wettelijk is dun, waardoor opzet

27 D.A. van Elswijk, J.P. Jansen, R.P.R. Duijkers & M.P. Moerman (2016). *Faillissementen: oorzaken en schulden 2015*. Den Haag: Centraal Bureau voor de Statistiek.

moeilijk te bewijzen is. Fraudeurs maken daar bewust gebruik van. Op basis van valse informatie over de verhouding tussen bezittingen en schulden wordt de Kamer van Koophandel verzocht de rechtspersoon te ontbinden. De Kamer van Koophandel heeft echter niet de beschikking over de administratie van de rechtspersoon om dit te verifiëren en zal dus aan het verzoek voldoen.

Prepackfaillissementen of flitsfaillissementen zijn uit de Verenigde Staten en Groot-Brittannië overgewaaid en worden toegepast bij bedrijven met financiële problemen waarbij na faillissement de mogelijkheid van een doorstart bestaat. Een prepackfaillissement werkt als volgt: de ondernemer die zijn onderneming ziet afstevenen op een faillissement, kan aan de rechtbank verzoeken een stille bewindvoerder aan te stellen. Deze stille bewindvoerder is vaak ook de beoogde curator in het faillissement. In tegenstelling tot de curator in een 'gewoon' faillissement heeft deze stille bewindvoerder de mogelijkheid om in een vroeg stadium de financiële situatie van de onderneming in kaart te brengen en te beoordelen op een mogelijke doorstart na faillissement. Dat dient het belang van werknemers en schuldenaren, omdat de gevolgen minder verstrekkend zullen zijn dan bij een faillissement zonder doorstart. De keerzijde is dat prepackfaillissementen het voor fraudeurs mogelijk maken om op oneigenlijke wijze van schulden en werknemers af te komen. Het prepackfaillissement krijgt weliswaar een wettelijke basis, maar zal naar verwachting in de samenleving op steeds meer weerstand stuiten omdat het niet transparant is en het als oneerlijk(e concurrentie) wordt ervaren.

We zien ook dat fraudeurs een bv oprichten met een postadres net over de grens. Deze handelswijze maakt een (administratieve) controle en opsporing moeilijker. Cijfers hierover zijn niet bekend.

2.5.3 Huidige gevolgen

Schattingen van de financiële schade liggen over het algemeen tussen de 1 en 2 miljard euro per jaar. De schade is volgens het CBS opgelopen van 1,28 miljard euro in 2010 tot 1,56 miljard euro in 2015. Voor dit dreigingsbeeld is de vraag van belang welk deel daarvan veroorzaakt wordt door georganiseerde criminaliteit. Op basis van de jaarlijkse verdeling van zaken tussen de politie en de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) wordt het aandeel van beroepsfraudeurs geschat. Deze verdeling is vastgelegd in de instructie 'toedeling zaken faillissementsfraude' en een van de indicatoren is een schadebedrag van 100.000 euro per zaak. Het gaat hierbij om onrechtmatige onttrekkingen die voorafgaand aan het faillissement zijn gedaan, zoals het wegsluizen van geld om schuldeisers te benadelen. Zaken met een bedrag lager dan 100.000 euro gaan naar de politie en zaken met een hoger bedrag gaan naar de FIOD. In 25 procent van de zaken gaat het om hogere bedragen. Hierbij zijn over het algemeen beroepsfraudeurs betrokken. De schade die door hen wordt aangericht, komt dan in 2015 uit op 390 miljoen euro.

Slachtoffers zijn werknemers, schuldeisers en de overheid. Jaarlijks worden naar schatting 7500 werknemers benadeeld doordat achterstallig salaris niet wordt uitbetaald. Bedrijven worden benadeeld doordat de vorderingen van schuldeisers open blijven staan, waardoor zij mogelijk in financiële problemen geraken en ook failliet kunnen gaan. De Belastingdienst en het UWV zijn bij faillissementen preferente schuldeiser en krijgen als eerste uitbetaald. Zij hebben financiële schade wanneer de boedel niet toereikend is.

2.5.4 Verwachtingen

De recente conjunctuurverbetering van de Nederlandse economie heeft al geleid tot minder faillissementen en minder meldingen van fraude door curatoren. De verwachting bestaat dat de conjunctuur de komende jaren verder zal verbeteren en dat het aantal faillissementen en het aantal meldingen van fraude verder zullen dalen. De gelegenheid van een faillissement zal zich minder voordoen, waardoor de afname vooral te zien zal zijn bij gelegenheidsfraudeurs.

De afname van het aantal meldingen kan echter ook een aanwijzing zijn dat de faillissementsfraudeurs zich steeds meer gaan bedienen van het fenomeen turboliquidatie. Dit wordt nog niet als faillissementsfraude gekwalificeerd, maar het door de dader gewenste effect blijft hetzelfde. Verwacht mag worden dat beroepsfraudeurs de komende jaren gebruik zullen blijven maken van de fraudemogelijkheden die turboliquidaties en prepackfaillissementen bieden.

Ook de komende jaren zijn de belangrijkste slachtoffers de werknemers, bedrijven en de overheid. De maatschappelijke schade is waarschijnlijk veel groter dan blijkt uit openbare verslagen. Als het beeld bestaat dat fraudeurs ‘ermee wegkomen’ en telkens opnieuw schulden maken en een spoor van oude schulden achter zich laten, dan tast dat het vertrouwen van burgers in de overheid aan.

In de bestrijding van faillissementsfraude zijn verschillende initiatieven ontplooid die de verwachting van een dalende trend rechtvaardigen. Zo is er nieuwe wetgeving om de positie van de curator te versterken, om een bestuursverbod op te leggen aan malafide bestuurders en om de strafbaarstelling van laakbaar handelen bij faillissementen uit te breiden. Daarnaast wordt er de komende jaren ingezet op verbetering van de publiek-private samenwerking, waaronder die met banken, en op intensivering van de opsporing.

2.5.5 Kwalificatie van dreiging

De komende jaren wordt een daling verwacht van het aantal faillissementen. De economische vooruitzichten voor de komende jaren zijn matig positief en nieuwe wetgeving maakt het minder eenvoudig om te frauderen. Verwacht wordt dat beroepsmatige fraudeurs minder beïnvloed zullen worden door de geschetste ontwikkelingen dan de aanvragers van een regulier faillissement. Conjuncturele omstandigheden zijn voor beroepsfraudeurs niet de primaire motivatie om te frauderen met faillissementen. Bovendien zijn met faillissementen

van beroepsfraudeurs in het algemeen grotere bedragen gemoeid dan met reguliere faillissementen. Ook de komende jaren zal de schade jaarlijks honderden miljoenen euro's bedragen en duizenden werknemers zullen geen achterstallig salaris ontvangen en hun baan kwijtraken. Kortom, het afnemend aantal faillissementen zal er niet toe leiden dat de schade van in georganiseerd verband gepleegde faillissementsfraudes (veel) zal dalen. Om die reden wordt deze vorm van fraude ook de komende vier jaar tot **dreiging** voor de Nederlandse samenleving gerekend.

2.6 Fraude met betaalmiddelen

2.6.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017.* Dat rapport is een verslag van onderzoek naar negen vormen van horizontale fraude, fraude met betaalmiddelen is er daar een van. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, alle drie werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf wordt de kwalificatie van dreiging beschreven. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is beargumenteerd en vastgesteld in een andere context door een groep van beoordelaars (de consensusgroep).

Er is sprake van fraude met betaalmiddelen als er financiële transacties worden gedaan met het betaalmiddel van een ander zonder dat die ander daarvan op de hoogte is. De meest in het oog springende vormen van fraude met betaalmiddelen zijn fraude met internetbankieren (phishing, malware) en fraude met betaalkaarten (skimmen, creditcards).

2.6.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

Fraude met betaalmiddelen is sinds het vorige dreigingsbeeld flink afgenomen. In 2014 is 538 keer aangifte gedaan, terwijl dit in 2011 nog 2236 keer was.

Vooral fraude met betaalkaarten waarbij de magneetstrip wordt gekopieerd (skimming) is in Nederland flink afgenomen en vrijwel tot nul gereduceerd. Dat is te danken aan de invoering van de EMV-chip en *geoblocking*. De chip beveiligt de betaalkaart veel beter dan de magneetstrip en bij geoblocking is de magneetstrip op de betaalkaart alleen buiten Europa te gebruiken als de gebruiker dat aanvraagt.

De Fraudehelpdesk registreert meldingen van fraude, waaronder die met betaalmiddelen. Het gaat om kleine aantallen en onbekend is welk deel fraude met betaalmiddelen betreft.

Aard

Bij fraude met betaalmiddelen heeft de afgelopen jaren geen grote verschuiving plaatsgevonden in de wijze waarop deze wordt gepleegd. *Phishing* en *social engineering* blijven de belangrijkste modi operandi. Daarbij haken fraudeurs aan bij actuele thema's in de media om contact te leggen met potentiële slachtoffers. Een belangrijke ontwikkeling is dat fraudeurs vaker phishing en social engineering combineren om de fysieke kaart te bemachtigen. Deze verschuiving lijkt het gevolg te zijn van de betere beveiliging bij banken.

Phishing is de belangrijkste werkwijze bij fraude met internetbankieren. Phishing is een verzamelnaam van technieken die criminelen gebruiken om vertrouwelijke gegevens (beveiligingscodes) te ontfutselen, zoals inlogcodes, wachtwoorden en pincodes. Dit gebeurt op verschillende manieren. Bijvoorbeeld via e-mail, telefoon, tekstberichten en nepwebsites. Een nieuwe ontwikkeling is dat, naast het massaal versturen van misleidende e-mails, de criminelen steeds meer gebruikmaken van social engineering. Zij benaderen de slachtoffers steeds persoonlijker en via meerdere kanalen, waarbij zij hun slachtoffers manipuleren om hun persoonlijke gegevens over te dragen. Zo zijn er voorbeelden in de geanalyseerde aangiften waarbij de fraudeur zich voordoet als een medewerker van de bank of als iemand die bij Microsoft werkt. In het geval van de bankmedewerker gaven de fraudeurs als reden voor hun bellen aan dat er een update van internetbankieren zou plaatsvinden of dat de bank bezig was met het controleren van persoonsgegevens, en wel om internetfraude te voorkomen. Vervolgens vroegen zij naar de inlog- en signeercodes waarmee zij geld van de rekening afboekten. In sommige gevallen werd de slachtoffers verteld dat ze de eerste 24 uur geen gebruik mochten maken van internetbankieren. Vaak hadden slachtoffers vóór het telefonisch contact geklikt op een phishingmail of is op een andere manier malware op hun computer geïnstalleerd.

De combinatie van phishing en social engineering wordt ook gebruikt bij fraude met betaalkaarten. Zo is het recent gebruikt bij de pas-opstuurfraude. Bij deze vorm van fraude proberen fraudeurs de fysieke kaarten in handen te krijgen door deze te laten opsturen. Slachtoffers werden zowel via de mail als per telefoon door een zogenaamde medewerker van hun bank benaderd met de mededeling dat hun pas niet meer veilig was. Vervolgens werden ze doorgelinkt naar een valse (phishing)website waar naar hun pincode en eventuele andere inlogcodes werd gevraagd. Daarna werd de slachtoffers verzocht hun pas op te sturen zodat banken deze zouden kunnen recyclen. Afhankelijk van de bank konden de fraudeurs vervolgens met de inlogcodes, pincodes en bankpas (online) betalingen verrichten en internetbankieren.

De handel in gestolen creditcardgegevens verschuift van grootschalige handel op ondergrondse fora naar kleinschalige handel via sociale media. De handel op ondergrondse fora verloopt vaak niet snel genoeg. Dit levert voor de koper het risico op dat veel creditcards al zijn geblokkeerd en daardoor onbruikbaar zijn geworden. Om dat voor te zijn worden de kaartgegevens in kleine aantallen aangeboden bijvoorbeeld via besloten Facebookgroepen

en Whatsapp-groepschats. Op die manier worden creditcardgegevens gedeeld die nog geen half uur eerder zijn gestolen. Fraudeurs voelen zich veilig genoeg om deze gegevens op deze manier uit te wisselen. Een voordeel van het gebruik van Facebook is dat als mensen lid worden van een Facebookgroep van creditcardhandelaars, ze automatisch van Facebook suggesties krijgen voor soortgelijke groepen. Fraudeurs krijgen zo hun eigen groepen.

2.6.3 Huidige gevolgen

Door verbeteringen in de monitoringsystemen van banken en voorlichtingscampagnes voor veilig online bankieren is de totale schade van fraude met betaalmiddelen flink afgenomen, van 82 miljoen euro in 2012 tot 17 miljoen euro in 2015. Deze schade komt hoofdzakelijk voor rekening van banken en online winkels. Alleen bij grove nalatigheid van de klant, zoals in het geval van katvangers, draaien de rekeninghouders op voor de schade.

Sinds 2005 is internetbankieren steeds populairder geworden. Ouderen hebben de laatste jaren een inhaalslag gemaakt in het gebruik van internet en internetbankieren. In 2014 maakte 86 procent van de Nederlanders gebruik van internetbankieren. Per jaar vinden 1,5 miljard transacties plaats met een totale waarde van 4800 miljard euro. Ondanks de groei van het internetbankieren daalde de schade van fraude met internetbankieren van 9,6 miljoen euro in 2013 naar 3,7 miljoen in 2015. Banken detecteren het gebruik van malware steeds beter, waardoor de schade als gevolg daarvan met 90 procent is gedaald tot minder dan 500.000 euro per jaar. Op de totale waarde van de transacties is de geleden schade bij fraude met internetbankieren een erg klein bedrag.

In 2012 was skimmen nog de grootste schadepost voor de banken. Na invoering van de EMV-chip en geoblocking zijn de gevolgen van het skimmen van betaalpassen enorm teruggedrongen. Als gevolg van deze maatregelen is de schade door skimmen sterk gedaald, namelijk van 6,8 miljoen euro in 2013 naar 1,7 miljoen euro in 2015.

De fraude met gestolen en verloren betaalpassen is daarentegen de laatste jaren gestegen tot bijna 5 miljoen euro in 2015. Deze stijging was vooral te wijten aan de pas-opstuurfraude. In 2015 heeft deze fraude een schade veroorzaakt van in totaal bijna 2 miljoen euro.

2.6.4 Verwachtingen

E-commerce maakt als sector een enorme groei door. In 2013 werd de waarde van de online consumentenbestedingen in Nederland geschat op bijna 11 miljard euro. In 2015 is de omzet de 16 miljard gepasseerd. Driekwart van de Nederlanders heeft in dat jaar online aankopen gedaan. Nederlanders zijn daarmee koploper in Europa. De verwachting is dat dit de komende jaren verder zal toenemen en dat schept mogelijkheden voor fraudeurs.

Bij de invoering van *instant payment* zal iedere betaling in Nederland binnen vijf seconden op de betreffende rekeningen zijn af- dan wel bijgeboekt. Nu duurt dat bij pinbetalingen nog een dag. Een snellere betalingsverwerking kan de fraudedetectie onder druk zetten.

Dit leidt mogelijk tot meer fraude en schade. De verwachting is dat instant payment op zijn vroegst in 2019 ingevoerd zal worden.

De komende jaren zal mobiel bankieren verder gaan toenemen waaronder de mogelijkheid van contactloos betalen met de smartphone. Banken en andere aanbieders investeren flink in de ontwikkeling van *apps* om dit mogelijk te maken. Tot nu toe heeft er geen fraude met mobiel betalen plaatsgevonden. Het zou net zo veilig zijn als betalen met een betaalpas en zelfs veiliger dan internetbankieren. Ook zal er de komende jaren een toename zijn van contactloos betalen met een bankpas; banken verstrekken steeds meer betaalpassen met die mogelijkheid en op steeds meer plekken kan contactloos worden betaald.

Blockchain is de technologie achter cryptocurrency's als bitcoin. In de toekomst wordt deze techniek van belang bij zaken waar een vorm van toezicht nodig is, zoals overdrachten van bezit en betalingen. Dit gaat vooral gevolgen hebben voor banken, accountants, notarissen en overheden. Toezicht dat nu bij deze partijen belegd is, zal in de toekomst met blockchain niet meer nodig zijn. In de kern is blockchain een administratie waarbij informatie versleuteld wordt gedistribueerd. Partijen kunnen op deze manier rechtstreeks zakendoen zonder tussenkomst van een derde toezichthoudende partij, omdat het grootboek openbaar is en wereldwijd gedistribueerd wordt. Daarnaast heeft blockchain de mogelijkheden om online bankieren veiliger te maken en kan het de transactiekosten tussen banken naar beneden brengen. Op dit moment zijn in Nederland diverse organisaties bezig om de toepassingen van blockchain uit te werken. Zo heeft ING zich aangesloten bij R3 CEV, een collectief van internationale banken dat sleutelt aan toepassingen die gebruikmaken van blockchaintechnologie. Ook andere Nederlandse banken zoals de Rabobank en ABN Amro zijn ermee bezig. De toepassingen waarnaar gekeken wordt, zijn heel divers: van publieke databases, zoals die van de Kamer van Koophandel, tot eenvoudige notariële aktes. De potentie van deze technologie is groot, maar wat daarvan gerealiseerd gaat worden is nog ongewis.

In de komende jaren zal het toenemend gebruik van biometrische eigenschappen bijdragen aan het verminderen van identiteitsfraude. Vermoedelijk worden biometrische gegevens opgeslagen en gebruikt om het identificatieproces betrouwbaarder te maken. Voorbeelden daarvan zijn de vingerafdruk die nu al wordt gebruikt voor internetbankieren via de smartphone en stemherkenning tegen identiteitsfraude.

Vanwege de grote toename in e-commerce en mobiele betalingen lanceerde de Europese Commissie in 2013 een pakket van aanvullende wetgevende maatregelen om de betalingsdiensten in Europa te reguleren, de zogenoemde Payment Service Directive 2 (PSD2). Deze wordt in 2018 van kracht. Een van de maatregelen is dat banken dan aan derde partijen toegang moeten geven tot rekeninginformatie van hun klanten en dat particulieren daartoe hun persoonlijke inlogcodes moeten verstrekken. Zowel banken als de Betaalvereniging, De Nederlandsche Bank en de Europese Centrale Bank hebben hierover hun zorgen geuit. Dit staat namelijk haaks op de boodschap dat rekeninghouders hun persoonlijke toegangsco-

des geheim dienen te houden en nooit aan derden dienen te verstrekken. Het ten uitvoer brengen van de Payment Service Directive 2 zou de mogelijkheden voor fraude kunnen doen toenemen. Op basis van de huidige (verminderde) omvang en de beschreven verwachtingen aan de hand van zowel remmende als stimulerende factoren, is de verwachting dat deze elkaar in evenwicht houden en dat de gevolgen van fraude met betaalmiddelen de komende jaren grotendeels dezelfde blijven.

2.6.5 Kwalificatie van dreiging

De gevolgen van fraude met betaalmiddelen zijn vooral financieel van aard. De huidige omvang van de financiële schade is ongeveer een kwart van die van vier jaar geleden. Er zijn weinig aangiften en fraude met betaalmiddelen wordt nauwelijks gemeld bij de Fraudehelpdesk. Onder invloed van de geschetste ontwikkelingen wordt verwacht dat de schade voorlopig op het huidige, relatief lage, niveau blijft. Fraude met betaalmiddelen is daarmee **geen concrete dreiging** voor de periode 2017-2021.

2.7 Fraude met online handel

2.7.1 Inleiding

De basis voor deze paragraaf over fraude met online handel vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar negen vormen van horizontale fraude, fraude met online handel is er daar een van. Dat onderzoek is voor dit dreigingsbeeld uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, alle drie werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Fraude met online handel is het niet nakomen van leverings- of betalingsverplichtingen die voortkomen uit transacties die online tot stand zijn gekomen. Fraudeurs bieden producten aan op een online handelsplaats, vragen een koper vooruit te betalen en leveren vervolgens niet. De fraude kan er ook in bestaan dat fraudeurs een product bestellen, aan de leverancier vragen om vooruit te leveren, maar vervolgens niet betalen.

2.7.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

In het vorige dreigingsbeeld werd gesignaleerd dat fraudeurs niet meer alleen gebruikmaken van bestaande online handelsplaatsen voor verkoop van goederen, maar steeds vaker ook zelf websites (laten) maken. Inmiddels heeft deze trend doorgezet en vormen malafide webwinkels volgens de Fraudehelpdesk de meest voorkomende vorm van oplichting via internet.

Fraudeurs lokken kopers naar de site van hun malafide webwinkel via advertenties met een link. Zo worden de bekende online handelsplaatsen nu steeds vaker gebruikt als advertentieplatform in plaats van als handelsplaats voor het kopen of aanbieden van artikelen. Deze verschuiving is waarschijnlijk het gevolg van de maatregelen die Marktplaats heeft ingevoerd om frauduleuze aan- en verkoop te weren. Marktplaats weert fraudeurs van de website op basis van politie-informatie. En als aangevers melden naar welk rekeningnummer ze hun geld hebben overgemaakt, gaat die informatie naar de betreffende bank en die kan bij meerdere meldingen de rekening blokkeren.
Voor het adverteren gebruiken fraudeurs niet alleen online handelsplaatsen, maar steeds vaker ook sociale media. Slachtoffers komen bijvoorbeeld via een link op Instagram of Facebook op de site van een malafide webwinkel terecht.

Tot enkele jaren geleden waren malafide webwinkels meestal nog wel te herkennen aan het amateuristische knip-en-plakuiterlijk. Tegenwoordig zijn valse websites voor consumenten steeds lastiger te herkennen. Het internetadres bevat vaak de naam van een bonafide webwinkel en de bijbehorende valse website, inclusief logo's en het Webshop Keurmerk is daarvan niet te onderscheiden. De makers van de valse website zorgen voor een inschrijving bij de Kamer van Koophandel op naam van katvangers, een kantoorpand, een telefoonnummer (met telefoniste) en een bestaand adres. Voor de betalingen door de slachtoffers wordt een iDEAL-contract afgesloten. Vaak openen deze webwinkels hun virtuele deuren op vrijdagavond en gaan na het weekend offline, nadat veel bestellingen zijn geplaatst en factuurbedragen zijn ontvangen. Het geld wordt gestort op de bankrekening van personen die als katvanger fungeren. Het geld gaat vervolgens door naar andere rekeningen om uiteindelijk in de zakken van de fraudeurs te verdwijnen.

Een recent verschijnsel vormt het massaal opkopen door malafide aanbieders van adressen van websites die niet meer bestaan. Het gebruik van deze websites krijgt de voorkeur boven het oprichten van nieuwe websites. Nieuwe websites scoren laag op de ranking van zoekmachines, terwijl websites met een zoekhistorie een hogere positie hebben en dus eerder in beeld komen bij potentiële kopers. Op die websites bieden malafide aanbieders goederen aan die geen enkel verband houden met de 'gekozen' domeinnaam, bijvoorbeeld schoenen die worden aangeboden in een webwinkel met de domeinnaam Vriendenvandeheemtuin.nl. Als na betaling de levering van de goederen achterwege blijft, levert het opnemen van contact met de webwinkel geen gehoor op.

Een relatief nieuwe fraudemethodiek is de zogenaamde ABC-constructie. Deze methodiek bestaat uit drie stappen:

1. De fraudeur koopt online een product bij persoon A,
2. de fraudeur zet tegelijkertijd dat product online te koop en verkoopt het aan persoon B, en
3. de fraudeur laat persoon B aan persoon A betalen en laat persoon A het product aan hemzelf versturen.

Om vroegtijdige ontdekking te voorkomen opereert de fraudeur daarbij vanuit verschillende online plekken: de ene keer op Marktplaats, de andere keer op eBay en een volgende keer op een van de vele andere verkoopsites.

De goederen die online frauduleus worden verhandeld, zijn grotendeels dezelfde als ten tijde van het vorige dreigingsbeeld: elektronische apparaten en gadgets zijn nog steeds populair. Wel bevat het aanbod nu meer oudere modellen dan toen. Die modellen voldoen blijkbaar prima, zijn gunstiger geprijsd en daarmee aantrekkelijk voor potentiële slachtoffers. Naast elektronica zijn ook toegangskaarten voor amusement (concert, sportwedstrijd, musical) regelmatig onderwerp van fraude.

Fraudeurs met online handel opereren hoofdzakelijk vanuit Nederland. Over de mate van georganiseerdheid is weinig bekend. Het Landelijk Meldpunt Internetoplichting levert zaken aan de politie op grond van meldingen die voldoende verdenkingen opleveren. In 2015 gebeurde dat 83 maal. In vrijwel elke zaak ging het daarbij om meerdere fraudeurs die verdacht werden van tientallen gevallen van oplichting.

Omvang

In oktober 2010 is het Landelijk Meldpunt Internetoplichting (LMIO) opgericht. Gedupeerden kunnen op deze politiesite online een melding en aangifte van internetfraude doen. Het LMIO registreert en analyseert de meldingen en aangiften van aan- en verkoopfraude via handelsplaatsen, malafide webwinkels en sociale media. Het aantal aangiften fluctueert in de periode 2012-2016 (zie tabel 7).

Tabel 7. Fraude met online handel: registraties bij het LMIO en geschatte totale aantal fraudes[28]

	2012	2013	2014	2015	2016
Aantal aangiften (netto)	41.500	45.000	37.000	35.500	39.000
Aantal fraudes als de helft aangifte doet	83.000	90.000	74.000	71.000	78.000

Bron: Landelijk Meldpunt Internetoplichting

Sommige slachtoffers laten aangifte achterwege, bijvoorbeeld uit schaamte of omdat ze menen dat het niets voor hen oplevert. Onderzoek van het LMIO naar geldstromen van fraudeurs wijst uit dat bij fraude met online handel de helft van de slachtoffers geen aangifte doet. Met een aangiftepercentage van 50 procent komt het geschatte aantal gevallen van fraude met online handel jaarlijks op ongeveer 80.000 per jaar (zie tabel 7).

De Veiligheidsmonitor is een jaarlijks terugkerend bevolkingsonderzoek naar veiligheid, leefbaarheid en slachtofferschap. Burgers wordt gevraagd naar de delicten die zij ondervonden hebben in de twaalf maanden voorafgaand aan de enquête. Het aantal gerapporteerde

28 Het netto aantal aangiftes is het aantal aanvankelijke aangiftes minus het aantal intrekkingen waarbij de bestelling alsnog wordt geleverd of het geld wordt terugbetaald. Bron: LMIO.

fraudegevallen met online handel per 100 inwoners steeg vanaf 2012 en neemt in 2016 weer enigszins af (zie tabel 8).[29] Met een bevolkingsomvang van 17 miljoen inwoners zou het aantal fraudegevallen in 2016 daarmee rond de 700.000 liggen (met ruim een half miljoen slachtoffers). Nader onderzoek van het CBS[30] met behulp van de gegevens uit beide bronnen (het LMIO en de Veiligheidsmonitor) toont aan dat er sprake is van een overschatting van slachtofferschap van fraude met online handel in de Veiligheidsmonitor met een factor 1,6 tot 2 voor de periode 2012-2015. Vastgesteld is ook dat de overschatting per jaar is toegenomen. Een en ander betekent dat het geschatte aantal fraudegevallen op grond van de slachtofferenquête geen stijgende tendens laat zien, maar langzaam afneemt van ongeveer 390.000 in 2012 naar 350.000 in 2015 (zie tabel 8).

Tabel 8. Fraude met online handel: slachtofferschap volgens de Veiligheidsmonitor, geschatte totale aantal fraudes voor en na correctie

	2012	2013	2014	2015	2016
Aantal fraudes per 100 inwoners	3,4	3,9	4,1	4,2	4,1
Aantal fraudes voor correctie	578.000	663.000	697.000	714.000	697.000
Aantal fraudes na correctie	393.000	375.000	367.000	352.000	

Bron: Veiligheidsmonitor en CBS

De conclusies op grond van de gegevens van het LMIO en de Veiligheidsmonitor lopen uiteen. Het jaarlijkse aantal fraudegevallen met online handel ligt volgens de slachtofferenquête veel hoger dan volgens het politieregister (370.000 versus 80.000). Verder is het aantal fraudegevallen in de periode 2012-2016 volgens de politiecijfers tamelijk stabiel, terwijl de tendens volgens de slachtofferenquête licht dalend is.

Het overgrote deel van de fraudes is afkomstig van online shoppers die hebben betaald voor goederen of diensten die vervolgens niet worden geleverd. Een klein deel betreft goederen of diensten die zijn geleverd en vervolgens niet worden betaald.

De vergelijking tussen de omvang van fraude met online handel in de afgelopen jaren (2012-2016) met de omvang ten tijde van het vorige dreigingsbeeld gaat mank en wordt hier daarom verder achterwege gelaten: het LMIO was destijds nog niet operationeel en de Veiligheidsmonitor in zijn huidige vorm was nog niet van start gegaan.

2.7.3 Huidige gevolgen

Online winkeliers hebben last van fraudeurs, omdat de betrouwbaarheid van online verkoop vermindert als hun bonafide webwinkels door fraudeurs vakkundig worden nagemaakt. Maar de gevolgen van fraude met online handel zijn toch hoofdzakelijk financieel van aard.

29 https://www.cbs.nl/nl-nl/publicatie/2017/09/veiligheidsmonitor-2016
http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=83095ned&D1=114-123&D2=0-6&D3=0&D4=2&VW=T

30 C. Reep (2017). *Fraude met online handel. Antwoorden uit de Veiligheidsmonitor vergeleken met het politieregister.* Den Haag: Centraal Bureau voor de Statistiek.

De hoogte van de financiële schade is niet precies vast te stellen, wel kunnen we een onder- en een bovengrens aangeven. De ondergrens baseren we op de politieregistraties door het LMIO. Met rond de 40.000 aangiften per jaar en een gemiddeld schadebedrag van 185 euro bedraagt de ondergrens voor het jaarlijkse totale schadebedrag bijna 8 miljoen euro.
Voor het berekenen van de bovengrens nemen we het geschatte aantal fraudegevallen op grond van de Veiligheidsmonitor als uitgangspunt en hanteren we voor al die gevallen hetzelfde gemiddelde schadebedrag. Dit resulteert in een schadebedrag van ongeveer 70 miljoen euro.
Ten slotte merken we op dat het onbekend is welk deel van de schade het werk is van georganiseerde groepen.

2.7.4 Verwachtingen

Naar verwachting zal oplichting via malafide webwinkels (vooral gehost in het buitenland) verder toenemen. De bekende online handelsplaatsen zullen door oplichters steeds vaker worden gebruikt als advertentieplatform, waar een koper vervolgens wordt weggelokt naar de site van een malafide webwinkel. Websites als Marktplaats weten oplichters steeds sneller in beeld te krijgen en hun advertenties te verwijderen. Oplichters zullen hun werkterrein daarom verder verschuiven naar sociale media zoals Facebook. Politie, Openbaar Ministerie en diverse marktpartijen zoals Marktplaats proberen door middel van gezamenlijke preventieve maatregelen fraude met online handel te bestrijden. Vooralsnog is onduidelijk in hoeverre deze partijen daarin de komende vier jaar zullen slagen.

2.7.5 Kwalificatie van dreiging

De afgelopen jaren zijn steeds meer mensen online gaan shoppen. Het aantal fraudegevallen met online handel is daarbij tamelijk stabiel gebleven. De jaarlijkse financiële schade bedraagt minimaal 8 miljoen euro en maximaal 70 miljoen euro. Welk aandeel georganiseerde groepen hierin hebben is niet bekend.
Gelet op de ontwikkeling van het aantal gevallen en de schade in de afgelopen periode, is de verwachting dat de financiële schade in de komende jaren op een vergelijkbaar niveau zal liggen. Daarmee is de financiële schade niet dusdanig omvangrijk dat kan worden gesproken van ernstige gevolgen voor de Nederlandse samenleving, zelfs niet als alle schade wordt toegerekend aan de activiteiten van georganiseerde groepen. Hiermee vormt fraude met online handel voor de komende jaren **geen concrete dreiging** voor ons land.

2.8 Telecomfraude

2.8.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017*. Dit rapport bevat het verslag van een onderzoek dat voor dit dreigingsbeeld is uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, die alle drie werkzaam zijn bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*

Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Telecomfraude betreft elke vorm van misbruik van een telecommunicatievoorziening, waardoor de integriteit van de telecommunicatie-infrastructuur wordt of kan worden aangetast. Ook frauduleuze handelingen om een telecommunicatiedienst te verkrijgen zonder daarvoor te betalen, vormen een overtreding van het Wetboek van Strafrecht.
Om enkele voorbeelden te noemen: het kan gaan om het afsluiten van een telefoonabonnement met valse identiteitspapieren, het doorgeleiden van telefoongesprekken naar dure, buitenlandse nummers (Wangirifraude), maar ook om het illegaal gebruik van streamingdiensten zoals Netflix en sportkanalen.

2.8.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

Naast de meer traditionele vormen van telecomfraude, zoals abonnementsfraude en PABX-fraude[31] die in het vorige dreigingsbeeld aan de orde zijn gekomen, treffen we ook twee relatief nieuwe vormen aan.
De eerste is een mengvorm van telecomfraude en schending van het intellectueeleigendomsrecht. Het wordt *cardsharing, controlwordsharing* of *keysharing* genoemd. Telecomproviders bieden in toenemende mate *content* aan in de vorm van speelfilms, televisieseries en muziek. Dit aanbod wordt versleuteld verzonden. Abonnees op deze diensten hebben de beschikking over de sleutel om hier gebruik van te kunnen maken. De fraude bestaat erin dat die sleutel aan vele anderen verkocht wordt (vaak via internet), zodat illegaal van de *content* gebruik kan worden gemaakt. Hierbij wordt ook inbreuk gemaakt op het intellectueeleigendomsrecht.
De tweede is de terugbel- of Wangirifraude en is afkomstig uit Japan. Vele duizenden mensen worden, met tussenkomst van een computer, vanuit verre landen opgebeld waarbij de verbinding direct wordt verbroken. Als de gebelde in reactie op de gemiste oproep terugbelt, krijgt hij een kiestoon te horen. De kiestoon is echter nagebootst op een bandje en wanneer de terugbeller ophangt omdat er niet lijkt te zijn opgenomen, heeft hij al geruime tijd verbinding gehad met een duur servicenummer in een ver land als Togo, Tsjaad of Madagaskar.

Omvang

Er is weinig zicht op de omvang van telecomfraude. Er zijn gefragmenteerd cijfers beschikbaar maar over het totaal is weinig bekend. Zo worden per jaar zo'n 2000 meldingen van abonnementsfraude gedaan en tussen de 150 en 200 meldingen van PABX-fraude. Uit de

31 *Private Automation Branche Exchange*. Dit is een bedrijfstelefooncentrale. De fraude bestaat erin dat op de centrale wordt ingebroken zodat gesprekken worden doorgeleid naar bijvoorbeeld dure *premium-rate-service*-nummers, zoals de 0900-nummers.

media werd bekend dat bij één provider binnen enkele maanden 3,6 miljoen pogingen tot Wangirifraude waren gedaan. De kosten werden geschat op 9,5 miljoen euro. Hoewel onbekend is hoeveel mensen illegaal gebruikmaken van content van providers (*cardsharing*), blijkt uit onderzoek dat wanneer het plaatsvindt, er gemiddeld twee extra zenders bekeken worden. Per illegale kijker leidt dit tot een (virtuele) omzetderving van 360 euro per jaar.
De afgelopen jaren werd gemiddeld 147 keer aangifte gedaan van telecomfraude bij de politie.

2.8.3 Huidige gevolgen

De gevolgen van telecomfraude zijn vooral financieel van aard. Sinds 2006 zijn er geen nieuwe cijfers over de omvang van deze financiële schade. Toen werd deze geschat op 40 miljoen euro. Een groot deel van de schade komt voor rekening van de providers, die dit verdisconteren in de tarieven. Bezien tegen de totale omzet van ongeveer 5,4 miljard (in 2013) is de schade zeer beperkt en in dat opzicht niet ernstig. Wanneer echter bedrijven of consumenten het slachtoffer worden van PABX- of Wangirifraude, kunnen de gevolgen aanzienlijk ernstiger zijn. Overigens zijn sommige providers begonnen met het vergoeden van de (opgelopen) schade.

2.8.4 Verwachtingen

De telecomsector is een sector die bij uitstek gevoelig is voor ontwikkelingen in de toepassingen van digitale technologie. Deze ontwikkelingen gaan zeer snel, bijna dagelijks worden nieuwe producten en diensten in de markt gezet die mogelijkheden bieden voor nieuwe vormen van fraude. Welke dat zijn en wat de ernst ervan zal zijn, is buitengewoon ongewis, daarom wordt daarover hier geen uitspraak gedaan.

2.8.5 Kwalificatie van dreiging

De schade is vooral financieel en komt voor het overgrote deel voor rekening van de telecomproviders. De laatste schatting van de omvang van de schade stamt uit 2006 en bedroeg 40 miljoen euro. Sindsdien zijn geen nieuwe cijfers bekend geworden.
Vanwege de onbekendheid van de omvang van het fenomeen en de onmogelijkheid om verwachtingen te formuleren, wordt telecomfraude als **witte vlek** betiteld.

2.9 Verzekeringsfraude

2.9.1 Inleiding

De basis voor deze paragraaf over verzekeringsfraude vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar negen vormen van horizontale fraude, verzekeringsfraude is er daar een van. Dat onderzoek is voor dit dreigingsbeeld uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, alle drie werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*

Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Verzekeringsfraude is het met opzet misleiden van de verzekeraar bij het aanvragen van een verzekering of bij het beroep doen op een verzekering. Fraude komt voor bij alle soorten verzekeringen, zoals schadeverzekeringen, inkomensverzekeringen, levensverzekeringen en zorgverzekeringen.

2.9.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

Op hoofdlijnen bezien, blijven de mogelijkheden voor het frauderen met verzekeringen telkens dezelfde: majoreren, fingeren, ensceneren en het onjuist informeren bij het aanvragen van een verzekering. Bij sommige specifieke werkwijzen zijn enkele ontwikkelingen te melden.

Een relatief nieuw fenomeen vormen de fraudes met ziekteverzuimverzekeringen. Er worden bedrijven opgezet om te declareren voor ziekteverzuim. Het personeel dat zich ziek meldt, bestaat alleen op papier. De bedrijven zijn feitelijk 'lege' bv's zonder personeel of met niet-bestaande werknemers en met valse jaarrekeningen. Regelingen voor ziekteverzuimverzekeringen kennen vaak zowel een publieke als een private component. Fraude manifesteert zich dan ook vaak gelijktijdig bij overheidsinstanties en inkomensverzekeraars.

De afgelopen jaren gebeurt de aanvraag van steeds meer verzekeringen geautomatiseerd. Dit maakt het gemakkelijker voor mensen om fraude te plegen, omdat ze bij het afsluiten van verzekeringen niet meer in persoon hoeven te verschijnen en daarmee gemakkelijker een andere identiteit kunnen aannemen.

Volgens het Verbond van Verzekeraars zijn fraudeurs steeds beter op de hoogte van de criteria en de methoden die verzekeraars hanteren om fraude te detecteren. Fraudeurs zijn daardoor ook steeds beter in staat geautomatiseerde fraudedetectiesystemen te omzeilen en grote schades te claimen. Ze gebruiken daarbij valse identiteiten en schakelen katvangers in.

Verzekeringsfraude gaat regelmatig samen met andere vormen van fraude zoals belastingfraude en faillissementsfraude. Verder ondervinden verzekeraars hinder van fraudeurs die bestanden hacken om verzekeringsclaims te laten uitbetalen aan zichzelf.

Ten tijde van dit schrijven wordt onderzoek uitgevoerd naar een groot aantal opzetaanrijdingen. Er zijn groeperingen betrokken bij het in scene zetten van aanrijdingen waarbij de schade die ontstaat door de vooraf geplande botsing bij de verzekering wordt geclaimd. Omdat het onderzoek nog niet is afgerond, ontbreekt momenteel nadere informatie over schade en slachtoffers.

Omvang

Registratiecijfers van het Verbond van Verzekeraars die ten tijde van het vorige dreigingsbeeld nog niet beschikbaar waren, maken een betere schatting van de omvang mogelijk. De schade-, levens- en inkomensverzekeraars in Nederland voerden in 2014 in totaal ruim 20.000 onderzoeken uit. In meer dan 7700 gevallen werd fraude vastgesteld.

Uit eerder onderzoek naar schadeverzekeringen komt naar voren dat de aantoonbaarheid ongeveer 12 procent bedraagt. Van de hiervoor vermelde 7700 fraudezaken ging het in 7500 zaken over fraude met *schade*verzekeringen. De meeste fraudezaken met schadeverzekeringen worden uiteindelijk civielrechtelijk afgehandeld. Een kleiner deel gaat naar de politie en het Openbaar Ministerie, waar prioriteit en capaciteit ontbreken om dit op te pakken. De laatste jaren zijn nagenoeg geen opsporingsonderzoeken naar verzekeringsfraude uitgevoerd, waardoor de kans op strafrechtelijke afdoening veel lager ligt dan de kans op een civielrechtelijke afdoening.
Uitgaande van de aantoonbaarheid van 12 procent komt het totale aantal gevallen van fraude met schadeverzekeringen voor 2014 naar schatting op 62.500. Deze 62.500 gevallen bevatten zowel fraudes veroorzaakt door individuele daders als fraudes die voor rekening komen van daders in georganiseerd verband. De mate waarin sprake is van georganiseerde criminaliteit is vastgesteld op basis van een aselecte steekproef van honderd fraudedossiers uit het register van het Verbond van Verzekeraars met ongeveer 3500 zaken. Er is onderscheid gemaakt tussen professionele fraudeurs, samenwerking met interne medewerkers binnen bedrijven en georganiseerde criminaliteit. Van georganiseerde criminaliteit was sprake in 18 procent van de dossiers. Bij toepassing van dit percentage op het totale aantal geregistreerde fraudes met schadeverzekeringen in 2014 resulteert dit in 11.250 fraudes in georganiseerd verband. Ervaring leert dat de fraudes van individuen naar verhouding amateuristischer van opzet zijn en daardoor sneller ontdekt worden. Fraudes door individuen zijn dan ook oververtegenwoordigd in de registraties, terwijl fraudes in georganiseerd verband ondervertegenwoordigd zijn. Het percentage van 18 procent ligt in werkelijkheid dus hoogstwaarschijnlijk hoger en het geschatte aantal van 11.250 georganiseerde fraudes vormt dan een ondergrens.

Onbekend is de omvang van georganiseerde fraudes met inkomensverzekeringen, levensverzekeringen en zorgverzekeringen.

De ontwikkeling van de omvang sinds het vorige dreigingsbeeld blijft ongewis, aangezien er destijds geen gedetailleerde cijfers beschikbaar waren. Daardoor kan er geen vergelijking worden gemaakt met de voorgaande periode.

2.9.3 Huidige gevolgen

De schade door fraude met levens-, inkomens- en zorgverzekeringen is onbekend omdat betrouwbare gegevens ontbreken. De financiële schade door fraude met schadeverzekeringen veroorzaakt door criminele samenwerkingsverbanden bedraagt jaarlijks minstens 108 miljoen euro. Een toelichting bij de berekening van deze ondergrens voor de schade volgt hieronder.

Er zijn 7500 gevallen van fraude met schadeverzekeringen vastgesteld voor 2014, met een aantoonbaar vastgestelde schade van 82 miljoen euro die is teruggevorderd of voorkomen door niet uit te keren. Als 12 procent aantoonbaar is, dan is de totale schade 600 miljoen euro (683 minus de 82 teruggevorderd of voorkomen). Als 18 procent van deze gevallen georganiseerde fraudes zijn, dan is de financiële schade daarvan minstens 108 miljoen euro. Minstens, om twee redenen. Allereerst omdat, zoals eerder is betoogd, het werkelijke percentage georganiseerde fraudes zeer waarschijnlijk hoger ligt dan 18 procent en ten tweede omdat het in de rede ligt dat de gemiddelde bedragen die gemoeid zijn met fraudes in georganiseerd verband hoger zullen zijn dan die bij fraudes met individuele daders.

De financiële schade is bij deze fraudes in eerste aanleg voor rekening van de verzekeringsmaatschappijen. Doorgaans wordt aangenomen dat deze verzekeringsmaatschappijen over het algemeen een goede financiële weerbaarheid kennen. In 2014 ontvingen de verzekeraars 74 miljard euro aan premies, keerden ze 75 miljard euro uit en belegden ze in totaal 460 miljard euro. Dergelijke bedragen zetten het bedrag aan geleden schade door fraude in 2014 in perspectief. Inmiddels zou de situatie voor verzekeringsmaatschappijen wel verslechterd zijn: zij geven aan te maken te hebben met een verzadigde en teruglopende markt, lage rente, veel concurrentie en strenger toezicht. Hoe dit ook zij, uiteindelijk zijn het niet de verzekeringsmaatschappijen die voor de schade opdraaien. Verzekeringsmaatschappijen berekenen de schade door in de verzekeringspremie en daardoor zijn het de consumenten die opdraaien voor de schade.

Naast financiële schade kennen bepaalde vormen van verzekeringsfraude nog andere negatieve gevolgen. Gevallen van brandstichting met frauduleus oogmerk en opzetaanrijdingen leveren in voorkomende gevallen aanmerkelijk gevaar op voor mensen. Verder kan de identiteitsfraude waarmee sommige gevallen van verzekeringsfraude gepaard gaan, anderen opzadelen met onterechte claims.

2.9.4 Verwachtingen

Voor de komende jaren wordt op het terrein van de verzekeringsfraude weinig verandering verwacht. De omvang van de verzekeringsfraude zal waarschijnlijk stabiel blijven. Door verzekeraars zal blijvend ingezet worden op preventie en detectie van verzekeringsfraude en de aanpak ervan. Door samenwerking binnen het Convenant Aanpak Verzekeringsfraude zal de informatiepositie worden versterkt. Daar staat tegenover dat steeds meer verzekeringen en claims via internet zullen worden afgehandeld en dit werkt fraude in de hand.

Door gebrek aan prioriteit en capaciteit bij de politie om zaken op te pakken, zijn de laatste jaren weinig opsporingsonderzoeken naar verzekeringsfraude uitgevoerd. De pakkans is zodoende laag. Zoals al gesteld, het overgrote deel van de zaken wordt niet strafrechtelijk maar civielrechtelijk afgedaan. De verwachting is dat deze werkwijze en de pakkans de komende jaren niet zullen veranderen.

2.9.5 Kwalificatie van dreiging

Verzekeringsfraude doet zich voor bij schadeverzekeringen, inkomensverzekeringen, levensverzekeringen en zorgverzekeringen. Over de omvang van fraude met de drie laatstgenoemde verzekeringen is betrekkelijk weinig bekend. Over fraude met schadeverzekeringen weten we meer. Op jaarbasis zijn er ongeveer 7500 geregistreerde gevallen van fraude met schadeverzekeringen met aantoonbare kosten. De totale financiële schade voor fraude met schadeverzekeringen bedraagt naar schatting jaarlijks 600 miljoen euro. Het aandeel daarvan voor rekening van criminele organisaties komt met een conservatieve schatting ruim uit boven de 100 miljoen euro op jaarbasis.

De financiële kosten van verzekeringsfraude komen via verhoging van de verzekeringspremie voor rekening van de burgers. En die kosten zijn alleen al bij schadeverzekeringen hoog. De kosten als gevolg van fraude met andere verzekeringsvormen, zoals georganiseerde fraudes met ziekteverzuimverzekeringen, komen daar nog bij. Voor de komende vier jaar verwachten de verzekeraars weinig verbeteringen op dit vlak. Het gebruik van internet bij het afsluiten van verzekeringen zal verder toenemen. Dit vergemakkelijkt volgens experts het plegen van fraude. Verder is er gevaar voor lijf en leden verbonden aan verzekeringsfraudes waarbij fraudeurs met opzet brand stichten of met voorbedachten rade aanrijdingen begaan. Gegeven de verwachte omvang van de financiële schade en het gevaar dat aan bepaalde vormen van verzekeringsfraude verbonden is, vormt deze fraudevorm voor de komende jaren een **dreiging.**

2.10 Voorschotfraude

2.10.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Horizontale fraude. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar negen vormen van horizontale fraude, voorschotfraude is er daar een van. Dat onderzoek is voor dit dreigingsbeeld uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Brigitte Bloem, Albert Harteveld en Micha de Heus, alle drie werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*

Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Voorschotfraude omvat allerlei vormen van oplichting waarbij het slachtoffer onder valse voorwendselen wordt verzocht voorschotten te betalen, met een veel grotere beloning in het vooruitzicht. De voorschotten kunnen onkosten zijn (zoals belasting, smeergeld, notariskosten en bemiddelingskosten) die nodig zijn om de beloofde deal te voltooien. Slachtoffers komen er na een of meer betalingen achter dat de beloofde geldsommen, goederen, of diensten niet worden geleverd. Op dat moment hebben zij vaak al grote bedragen overgemaakt – soms wel tienduizenden tot honderdduizenden euro's, dollars of andere valuta.
Vooral door het gebruik van het digitale verkeer is de fraude grenzeloos geworden en is het bereik van potentiële slachtoffers groot. Voorbeelden van voorschotfraude zijn: erfenis-, dating-, loterij- en werkaanbodfraude.

2.10.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

We zullen hier een drietal vormen van voorschotfraude behandelen: datingfraude, loterijfraude en voorschotfraude met *crowdfunding*. Van datingfraude en loterijfraude was de verwachting in het vorige dreigingsbeeld dat het zou toenemen en crowdfunding was sterk in opkomst.

Bij *datingfraude* scannen fraudeurs (vaak georganiseerde groepen West-Afrikaanse daders) allerlei datingwebsites en sociale media op zoek naar potentiële slachtoffers over de hele wereld, met wie ze vervolgens contact proberen te leggen. De werkwijze en oogmerken bij deze vorm van fraude zijn de laatste paar jaar niet veranderd.

Bij *loterijfraude* krijgen potentiële slachtoffers voorgespiegeld dat zij een grote prijs hebben gewonnen in een loterij. Voordat de prijs in ontvangst genomen kan worden, moeten echter eerst allerlei kosten betaald worden. Volgens cijfers van de Fraudehelpdesk is loterijfraude geen probleem meer. Mensen melden weliswaar (pogingen tot) loterijfraude, maar vrijwel niemand betaalt meer.

Crowdfunding is geen nieuw fenomeen, maar de populariteit ervan is de laatste jaren enorm toegenomen. Banken verstrekken als gevolg van de financiële (economische) crisis minder leningen waardoor bijvoorbeeld *start-ups* moeilijk aan startkapitaal kunnen komen; zij nemen dan hun toevlucht tot crowdfunding. Ook fraudeurs hebben de mogelijkheden ervan ontdekt. De afgelopen jaren bleek een aantal crowdfundingprojecten frauduleus te zijn en waren investeerders hun geld kwijt. Crowdfunding vindt digitaal plaats en het aantal platforms waar crowdfundingprojecten worden aangeboden, neemt sterk toe. De risico's zijn vergelijkbaar met het kopen in een webshop en toezicht en regulering zijn nog niet gangbaar.

Omvang

Cijfers van de Fraudehelpdesk en de politie lijken erop te wijzen dat voorschotfraude in Nederland een afnemend probleem is. Het totale aantal meldingen bij de Fraudehelpdesk daalt van 1480 in 2014 naar 865 in 2015. Weliswaar stijgt daarbinnen het aantal meldingen van datingfraude licht, maar het aantal betalende slachtoffers blijft gelijk. Er werden de afgelopen jaren gemiddeld 400 meldingen per jaar van loterijfraude gedaan; negen melders betaalden gemiddeld 2500 euro.

Ook het aantal aangiften bij de politie daalt. Tussen 2011 en 2014 werd gemiddeld 396 keer per jaar aangifte gedaan. In de periode voorafgaand aan het vorige dreigingsbeeld was dat gemiddeld 604 keer. Er is sprake van een omvangrijk dark number. Onderzoek laat zien dat wanneer een delict op internet plaatsvindt, de kans op het doen van melding of aangifte klein is. De schatting van een expert van de Fraudehelpdesk is dat 90 tot 95 procent van de slachtoffers geen aangifte doet.

Ook het aantal actieve dadergroepen op dit terrein is een indicatie voor de omvang. Het aantal actieve dadergroeperingen in Nederland is gezakt van 32 in 2009 naar 17 in 2013 (recentere cijfers zijn nog niet beschikbaar). Dit zijn groeperingen die vanuit Nederland slachtoffers maken in andere landen. Onderzoeksbureau Ultrascan maakt een *ranking* van landen die aantrekkelijk zijn voor dadergroeperingen om te verblijven. Nederland stond destijds op een achtste plaats in de top 25, maar is in 2013 gezakt naar een achttiende plaats.

2.10.3 Huidige gevolgen

Slachtoffers zijn overwegend burger. De hoogte van de betaalde bedragen en de emotionele schade is afhankelijk van de soort fraude. Loterijfraude is een vorm van fraude waarbij relatief lage bedragen worden betaald. Meestal wordt over een korte periode betaald (een paar maanden tot een half jaar). Bedragen variëren volgens de Fraudehelpdesk tussen de 400 en 4000 euro per persoon. Bij datingfraude worden grotere bedragen betaald. Hierbij wordt over een langere periode (een half jaar tot enkele jaren) betaald en de bedragen variëren tussen de 10.000 en 20.000 euro. Het gaat hier om gemiddelden, maar uitschieters van enkele tonnen zijn ook bekend. Bij datingfraude kan de emotionele schade groot zijn.

Wanneer de 90 procent van de slachtoffers dat geen aangifte doet, wordt geëxtrapoleerd naar het totaalbedrag dat is betaald voor voorschotfraude, bedraagt de totale financiële schade zo'n 60 miljoen euro per jaar.

2.10.4 Verwachtingen

In navolging van de voorspellingen uit het vorige dreigingsbeeld wordt voor de komende jaren weinig verandering verwacht. Het aantal meldingen en aangiften zal waarschijnlijk stabiel laag blijven, de gemiddeld betaalde bedragen hoog en de emotionele gevolgen voor sommige slachtoffers groot. De inzet op preventie door de Fraudehelpdesk, verschillende televisieprogramma's en waarschuwingen op allerhande websites en in kranten en tijd-

schriften is de afgelopen jaren succesvol gebleken. Dit blijkt uit het beperkte aantal betalende slachtoffers, en de verwachting is dat dit de komende jaren zo zal blijven.
Een van de grotere datingsites houdt zich actief bezig met het weren van fraudeurs door alle nieuwe profielen handmatig te beoordelen op IP-adressen, de gebruikte bankrekeningnummers, het soort berichten dat verstuurd wordt, gebruik van e-mailadressen en taalgebruik. Sinds kort hebben zeven datingsites een Keurmerk Veilig Daten in het leven geroepen. Om voor het keurmerk in aanmerking te komen moet aan een aantal voorwaarden zijn voldaan op het gebied van veiligheid en klantvriendelijkheid. Dit soort initiatieven moet het aantal fraudegevallen in de toekomst verder doen dalen.

2.10.5 Kwalificatie van dreiging

De gevolgen van voorschotfraude bevinden zich op het individuele financiële en emotionele vlak. Allerlei vormen van ondermijning of kosten voor de overheid en het bedrijfsleven zijn afwezig. De laatste jaren is een daling te zien van zowel meldingen bij de Fraudehelpdesk als aangiften bij de politie. Ook het aantal actieve dadergroepen neemt af.
Gezien het kleine aantal betalende slachtoffers werpt de inzet op preventie zijn vruchten af. De verwachting is dat het aantal meldingen en aangiften op een stabiel, laag niveau zal blijven. Daarom vormt voorschotfraude de komende jaren **geen concrete dreiging** voor de Nederlandse samenleving.

2.11 Accijnsfraude

2.11.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Thema rapportage Douanefraude t.b.v. NDB 2017*. Dat rapport doet verslag van onderzoek dat in de eerste helft van 2016 is uitgevoerd voor dit dreigingsbeeld. De auteurs van het onderzoeksrapport zijn Silvie Jansen en Simone Stevelmans, werkzaam bij de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) van de Belastingdienst. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017*.
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Bij accijnsfraude is sprake van het doelbewust ontlopen van verplichte nationale heffingen op grondstoffen en producten uit het buitenland. Accijnsfraude is een vorm van verticale fraude. Dit houdt in dat de overheid het voornaamste slachtoffer is van de fraude.

2.11.2 Ontwikkelingen in aard en omvang sinds het NDB2012

In het vorige dreigingsbeeld is het onderwerp accijnsfraude niet aan de orde gesteld. Daardoor wijkt de behandeling van dit onderwerp enigszins af van die van de andere onderwerpen in dit dreigingsbeeld. Zo wordt er eerst nader uitleg gegeven bij deze fraudevorm voordat er ontwikkelingen worden belicht. Verder ontbreken referentiepunten uit het vorige

dreigingsbeeld. De nadruk ligt dan ook op ontwikkelingen die zich meer recent hebben voorgedaan.

Bij accijnsfraude wordt fraude gepleegd met accijnsgoederen. Conform Richtlijn 2008/118/EG zijn dit alcoholhoudende producten, tabaksproducten en minerale oliën. Er bestaan vier vormen van accijnsfraude:

1. Smokkel van buiten de Europese Unie. Accijnsgoederen worden op illegale wijze de EU binnengebracht. De douaneformaliteiten worden omzeild en de goederen worden aan de accijnsheffing onttrokken.
2. Smokkel binnen de Europese Unie. Dit betreft goederen waarover in EU-lidstaat A voor vertrek accijns is betaald en waarover na aankomst in EU-lidstaat B ook accijns dient te worden afgedragen, waarna de accijns in EU-lidstaat A kan worden teruggevraagd. De eenvoudigste vorm van fraude met deze goederen is om te kopen in land A met een lage accijns en te verkopen in land B met een hoge accijns, nadat de goederen het land in gesmokkeld zijn en er dus geen aangifte is gedaan. Omdat de accijns in de prijs wordt doorberekend, kan in land B flink winst worden gemaakt op de gesmokkelde goederen.
3. Illegale productie. Illegale bedrijven produceren binnen de EU tabak of alcohol en omzeilen zodoende de accijnsheffing volledig.
4. Fraude met goederen onder schorsing van accijns. Zolang accijnsgoederen zijn opgeslagen in een accijnsgoederenplaats (AGP) hoeft geen accijns te worden betaald. Een AGP is een plaats in Nederland waarvoor vergunning is verleend om er accijnsgoederen te produceren, te verwerken of op te slaan. Pas als de goederen de AGP verlaten moet men accijns betalen. Bij zowel productie, opslag als vervoer kunnen goederen aan het zicht van de douaneautoriteiten worden onttrokken. Zo kan bij fabricage of opslag van de accijnsgoederen een deel van de voorraad illegaal worden verkocht. En als verzender en ontvanger samenspannen, is het mogelijk de indruk te wekken dat goederen van land A naar land B gaan, terwijl dat feitelijk niet gebeurt. De verzender wordt dan ten onrechte ontslagen van zijn accijnsplicht, terwijl hij de goederen nog steeds in bezit heeft. Door de accijns wel door te berekenen aan de afnemer en deze vervolgens niet af te dragen, wordt extra winst gemaakt. Hierbij ontstaat ook de mogelijkheid om de goederen relatief goedkoop af te zetten.

Alcohol

In het geval van alcoholhoudende producten gaat het meestal om de vierde vorm van accijnsfraude. Partijen drank worden vanuit AGP's in Nederland *onder schorsing van accijns* verzonden aan belastingentrepots (zo heten AGP's in het buitenland) of geregistreerd geadresseerden in andere lidstaten en hier afgemeld, terwijl deze daar feitelijk nooit zijn aangekomen. Een geregistreerd geadresseerde is een bedrijf met een vergunning voor het ontvangen van accijnsgoederen uit andere landen van de EU, onder schorsing van accijns. Een geregistreerd geadresseerde behoort na ontvangst binnen vijf dagen aangifte te doen en accijns te betalen. Bij fraude gebruikt men als geregistreerd geadresseerde een plof-bv.

Daarbij wordt een katvanger ingezet om de vergunning te krijgen en de bv op naam te zetten. Vervolgens gaan op papier in een kort tijdsbestek grote hoeveelheden drank naar deze bv waarover de accijns nooit betaald wordt. Tegen de tijd dat deze fraude ontdekt wordt, is de bv al verlaten. In het geval van de belastingentrepots betreft het zogenoemde *ghost warehouses* in het buitenland. Dit zijn belastingentrepots die puur zijn opgericht om voor afmelding van dergelijke praktijken zorg te dragen, maar waar feitelijk nooit goederen aankomen. Zo zijn de loodsen waar deze entrepots zich bevinden in sommige gevallen niet eens bereikbaar voor vrachtverkeer. Vanuit de belastingentrepots worden de goederen op papier doorgezonden naar volgende entrepots om uiteindelijk ergens, in ieder geval zonder accijns en mogelijk ook zwart, op de markt te komen.
De fraude met de zogeheten ghost warehouses is inmiddels alweer afgenomen. Door de invoering van het *Excise Movement Control System* (EMCS) voor de elektronische douaneaangifte voor het verzenden en ontvangen van goederen onder schorsing van accijns, is men in Europa beter in staat verdachte patronen in de vervoersbeweging te ontdekken. Hierdoor kunnen deze warehouses in een vroeg stadium ontdekt en bestreden worden. Daarnaast heeft Nederland actie ondernomen om de geregistreerd geadresseerden in Nederland nauwgezetter te controleren, zowel bij afgifte van de vergunning als bij aangifte van goederen. Hierdoor zou fraude met geregistreerd geadresseerden in Nederland momenteel niet meer voorkomen. In reactie hierop hebben fraudeurs hun werkwijze aangepast. Criminele organisaties zijn gebruik gaan maken van logistieke dienstverleners voor hun digitale administratie en aangifte bij de Belastingdienst. Deze dienstverleners registreren in Nederland maar weinig informatie in het EMCS en dit bemoeilijkt het ontdekken van verdachte patronen. Verder kunnen criminele organisaties genoegen nemen met minder winst door wel accijns te betalen maar met een lager tarief. Zo wenden fraudeurs voor dat hun bier wordt vervoerd naar een geregistreerd geadresseerde in Duitsland om daar vervolgens ook aangifte en betaling van accijns te doen. De accijns op bier in Duitsland is relatief laag en als het bier feitelijk naar het Verenigd Koninkrijk wordt gesmokkeld en afgezet, zijn de omzetten nog steeds aanzienlijk. Bij een fraudegeval met bier dat was afgemeld in Duitsland en gesmokkeld naar Engeland, leverde een succesvol gesmokkelde vrachtwagen met bier zo'n 16.000 euro op aan ontdoken accijns.
Met de oprichting van het Fraude Team Accijns in 2012 is voor het eerst uitgebreid aandacht besteed aan alcoholzaken. In de periode van 2012 tot en met 2015 zijn zeventien onderzoeken gedraaid die zich richtten op fraude met alcoholhoudende drank met een totaal financieel nadeel van bijna 6 miljoen euro. Het fraudeteam is in 2015-2016 overgegaan naar het *Anti Fraud Coordination Service*-team (AFCOS-team).

Sigaretten
De accijnsfraude met sigaretten betreft allereerst smokkel, zowel van buiten de EU als daarbinnen. De sigaretten zijn hoofdzakelijk bestemd voor de buitenlandse markt en in die gevallen komt het financiële nadeel van de gesmokkelde waar voor rekening van een buitenlandse overheid en niet van de Nederlandse staat.

Criminele groepen die zich met sigarettensmokkel bezighouden zijn incidenteel gewelddadig. Een voorbeeld vormt het geval waarin de eigenaar van een eenmanszaak onder bedreiging akkoord ging met de ontvangst van een container op naam van zijn zaak. De container werd verzonden van Piraeus in Griekenland naar Rotterdam. Volgens de *Bill of Lading* zou de container watermeloenen bevatten, maar er zaten ook 6 miljoen sigaretten in zonder de vereiste accijnszegels.

Naast smokkel vindt er ook illegale productie plaats. Waar voorheen de illegale productie van sigaretten binnen de EU zich vooral concentreerde in Oost-Europa, vinden we deze productie de laatste jaren ook in toenemende mate in ons land. De FIOD heeft in de periode van 2013 tot en met 2015 zes illegale productiestraten ontmanteld. Een doorsnee illegale sigarettenfabriek produceert per minuut 5000 sigaretten (263 pakjes). Gaan we er vanuit dat er acht uur per dag productie plaatsvindt – al draaien dergelijke machines vermoedelijk non-stop –, dan zijn dat 5000 x 60 x 8 = 2.400.000 sigaretten per dag.
Om een illegale productiestraat te laten draaien, zijn diverse machines nodig. Een complete fabriek bestaat in elk geval uit een sigarettenmachine en een verpakkingsmachine en in sommige gevallen ook nog uit een snijmachine voor ruwe tabak en een scheidingsmachine voor productiefouten. De prijzen voor een complete productielijn variëren van 60.000 tot 150.000 euro. Meestal worden er diverse locaties gebruikt (voor productie, voor opslag en voor het ompakken/voorzien van deklading) voordat de sigaretten klaar zijn om vervoerd te worden naar de afzetbestemming. Deze locaties worden gehuurd en de huur wordt contant betaald. Afgezien van de benodigde tabak is er bijkomend materiaal nodig om de sigaretten te produceren, zoals filters, sigarettenpapier en verpakkingsmateriaal. Ook is er personeel nodig:

- om de loods voor te bereiden (onder meer voor het aanbrengen van geluidsisolatie en het afdichten van ramen);
- om de productielijn op te zetten en te laten draaien (technici);
- om de daadwerkelijke productie te draaien.

Personeel wordt soms vanuit het buitenland ingevlogen (Bulgaren, Roemenen, Polen). Vervolgens moet zorg gedragen worden voor het vervoer van personeel en materialen, en voor de beveiliging van locaties.
Al met al vergt de illegale productie veel investering en organisatie. Ons land is aantrekkelijk vanwege de grote leegstand, weinig controle, goede uitvalsbasis naar omringende landen en de gebrekkige communicatie met de autoriteiten in die landen. Het vermoeden bestaat dat Nederlandse ondernemers zich hebben toegelegd op het leveren van machines, locaties en dekmantels voor illegale productie.

Tabak
Experts zien een stijging van de illegale handel in tabak en shagverpakkingen en er zijn zelfgebouwde machines aangetroffen om de verpakkingen met tabak te vullen. Volgens experts stijgt de vraag naar waterpijptabak en neemt ook de smokkel ervan toe.

Minerale oliën

Uit politieonderzoek komt naar voren dat criminelen gebruikmaken van de verliesnorm van 0,3 procent voor gasolie. Deze verliesnorm is door het bedrijfsleven opgesteld, omdat er tijdens vervoer van gasolie soms verlies kan optreden als gevolg van bepaalde omstandigheden (verdamping, temperatuurschommelingen, krimping). Over het verloren gegane goed is geen accijns verschuldigd. Een criminele organisatie speelde hierop in door te zorgen dat altijd het maximale verlies werd aangegeven. Men gebruikte bedreiging en afpersing om de medewerking van scheepseigenaren af te dwingen en ongestoord te kunnen blijven opereren. De winst die de organisatie door grootschalige diefstal en verduistering van brandstof in de binnenvaart heeft gemaakt, wordt geschat op 6,8 miljoen euro.

2.11.3 Huidige gevolgen

In het rapport *Bestrijding van accijnsfraude bij alcohol en tabak* uit 2012 heeft de Algemene Rekenkamer veel kritiek op de aanpak van accijnsfraude in Nederland. De Algemene Rekenkamer verwijt de Belastingdienst, de Douane en de FIOD dat er geen concrete doelen voor accijnsfraudebestrijding bestaan en dat dit probleem geen hoge prioriteit krijgt. Volgens de Algemene Rekenkamer lopen EU-lidstaten jaarlijks miljarden euro's aan accijns mis. De uiteenlopende accijnstarieven tussen de lidstaten maken het illegaal produceren en verhandelen van tabaksproducten en alcoholhoudende drank tot een zeer winstgevende activiteit.

Tabel 9 toont hoeveel accijnsgoederen er in Nederland, in de periode na de publicatie van het rapport van de Algemene Rekenkamer, in beslag zijn genomen. Het bedrag aan niet-afgedragen accijns dat hierdoor is misgelopen, bedraagt in de periode jaarlijks gemiddeld 23,5 miljoen euro, indien deze goederen in Nederland op de markt zouden zijn gebracht. De grootste hoeveelheden in beslag genomen accijnsgoederen blijken, gelet op soort en merk, bestemd voor andere EU-lidstaten (met name het Verenigd Koninkrijk).

Tabel 9. In beslag genomen sigaretten, tabak en alcohol in Nederland in de periode 2012 t/m juli 2016: hoeveelheid en financieel nadeel vanwege niet-afgedragen accijns

Jaar	Sigaretten (miljoenen)	Nadeel sigaretten (mln €)	Tabak (kg x 1000)	Nadeel tabak (mln €)	Alcohol (liters x 1000)	Nadeel alcohol (mln €)	Totaal nadeel (mln €)
2012	64,8	11,7	0,6	0,05	-	-	**11,7**
2013	101,3	20,5	23,3	2,6	10,6	0,07	**23,2**
2014	82,9	18,7	62,5	6,7	32,7	0,6	**26,0**
2015	123,5	28,6	4,6	0,5	27,0	0,2	**29,3**
2016 (t/m juli)	74,1	17,2	254,9	0,03	-	-	**17,2**
Totaal	**446,7**	**96,8**	**345,9**	**9,9**	**70,4**	**0,8**	**107,5**
Gemiddeld jaar	**97,5**	**21,1**	**75,5**	**2,2**	**15,4**	**0,2**	**23,5**

In de periode van 2012 tot en met 2015 zijn er door de FIOD 106 strafrechtelijke onderzoeken gedraaid op accijnsfraude (zie tabel 10). Daarvan waren 75 onderzoeken gericht op fraude met sigaretten (71%) en 17 op fraude met alcoholhoudende drank (16%). De resterende zaken waren gewijd aan onderzoek naar fraude met tabak, waterpijptabak of minerale oliën.

Tabel 10. Strafrechtelijke onderzoeken van de FIOD naar accijnsfraude afgerond in de periode 2012-2015

Jaar afronding	Zaken (aantal)	Nadeel (miljoen €)
2012	22	14,1
2013	36	20,7
2014	31	16,6
2015	17	13,2
Totaal	**106**	**64,6**

Het nadeel verbonden aan de afgeronde zaken van de FIOD bedraagt in de periode 2012-2015 jaarlijks gemiddeld ruim 16 miljoen euro. Daarnaast is er nog het nadeel verbonden aan inbeslagnames waarvoor geen strafrechtelijk onderzoek is gestart; dit bedraagt jaarlijks gemiddeld 8,2 miljoen euro. Dit brengt het totale financiële nadeel van accijnsfraude jaarlijks gemiddeld op ongeveer 24,5 miljoen euro. De bedragen die in de zaken zijn teruggevorderd en hiervan nog moeten worden afgetrokken, zijn niet omvangrijk: voor 2015 is 8000 euro geïncasseerd. Het hier berekende financiële nadeel komt voor rekening van de Nederlandse staatskas voor zover de accijnsgoederen bestemd waren voor de Nederlandse markt.

Het deel van de schade waarvoor criminele groeperingen verantwoordelijk zijn, is niet precies vast te stellen. Zo worden er bij in beslag genomen zendingen soms geen verdachten aangetroffen, zodat niet kan worden vastgesteld of er een groepering achter schuilt dan wel een individu. Daardoor kon slechts in ruim een kwart van de zaken de fraude met zekerheid worden toegeschreven aan een criminele groepering; deze zaken vertegenwoordigden 35 procent van de schade. Daar staat tegenover dat bij de strafrechtelijke onderzoeken die door de FIOD in de periode zijn uitgevoerd, het slechts in enkele gevallen ging om een alleen handelende particulier. Dit ligt voor de hand omdat de aard van het criminele bedrijf verlangt dat er meer mensen aan meewerken. Al met al is het daarom aannemelijk dat het overgrote deel van de schade door accijnsfraude voor rekening komt van georganiseerde criminaliteit.

De hoogte van het hiervoor berekende financiële nadeel is afhankelijk van de intensiteit van controle en opsporing. De berekende jaarlijkse bedragen vormen een ondergrens die gebaseerd is op de aangetroffen en in beslag genomen goederen alsmede de uitgevoerde strafrechtelijke onderzoeken. Dat de werkelijke kosten hoger liggen, is evident.

Overige gevolgen van fraude met accijns

Experts wijzen op nog diverse andere dan financiële gevolgen. Fraude met accijns leidt tot verlies aan draagvlak voor belastingheffing en heeft een negatief effect op de belastingmoraal van bedrijven. De gederfde overheidsinkomsten kunnen bovendien het vertrouwen van de Nederlandse burger in het fiscale systeem aantasten. Door accijnsfraude ontstaat oneerlijke concurrentie tussen ondernemingen, omdat een frauderend bedrijf producten goedkoper kan aanbieden dan een bedrijf dat op reguliere wijze accijns afdraagt. Als de bedrijfskosten door accijnsfraude worden gedrukt, wordt de winst groter en dat biedt ook meer mogelijkheden voor investeringen. Dit heeft er volgens experts toe geleid dat er bepaalde wijken zijn waar uitsluitend illegale sigaretten te koop zijn, wat ten koste gaat van de omzet van legale verkopers. Ook slijterijen ondervinden oneerlijke concurrentie en klagen over bodemprijzen voor alcoholhoudende drank van winkeliers die geen accijns afdragen.
Binnen het bulktransport van olie per binnenschip is het volgens sommige experts tegenwoordig moeilijk om het hoofd boven water te houden: de verleiding tot het ontduiken van accijns in de oliebranche is behoorlijk toegenomen. In deze branche maar ook in andere branches dreigen bonafide bedrijven door frauderende concurrenten uit de markt te worden gedrukt. Het gevaar bestaat dat steeds meer bedrijven heffingen (accijns, btw) gaan ontduiken. De transportsector heeft het meest te lijden onder de fraudes, omdat deze sector de goederen vervoert of opslaat. In veel gevallen zijn medewerkers zich er niet van bewust dat ze meewerken aan fraude, maar worden zij bij ontdekking wel ter verantwoording geroepen door de toezichthoudende instanties. De Nederlandse accijnswetgeving bepaalt dat degene die de beschikking heeft over de accijnsgoederen, aansprakelijk kan worden gehouden voor de niet-afgedragen accijns.

2.11.4 Verwachtingen

Experts verwachten een toename van accijnsfraude en de betrokkenheid daarbij van criminele organisaties. Internationalisering, automatisering en een hiermee gepaard gaand afnemend fysiek toezicht zouden hier debet aan zijn. Criminele organisaties maken steeds meer gebruik van digitale en verhullende technieken. Geautomatiseerde systemen zijn door fraudeurs gemakkelijk te manipuleren.
Experts geven aan dat in de meeste gevallen van accijnsfraude sprake is van georganiseerde criminaliteit. Ze verwachten dat deze betrokkenheid nog verder zal toenemen vanwege de lage pakkans, hoge winsten en de lage straffen bij veroordeling in vergelijking met andere criminele activiteiten.

Experts verwachten een stijging van accijnsfraude, om diverse redenen. Er wordt een stijging van de accijns in Nederland verwacht, waardoor het verschil met de overige EU-lidstaten groter zal worden. Nederland wordt dan aantrekkelijker als afzetgebied voor accijnsgoederen waarvan de accijns in een goedkopere lidstaat of in het geheel niet wordt voldaan. Als accijnsfraude weinig prioriteit heeft en de accijnsverschillen tussen Nederland en de andere lidstaten groter worden, dan wordt het aantrekkelijker voor criminele organisaties om accijnsfraude te gaan plegen. Verder zou accijnsfraude gaan toenemen vanwege de stij-

gende verkoop van tabak en sigaretten via internet. Ten slotte vrezen experts dat instanties te veel vertrouwen op automatisering en te weinig doen aan toezicht en controle.
De verwachtingen ten aanzien van de ontwikkeling van accijnsfraude met sigaretten lopen uiteen. De FIOD heeft geïnvesteerd in een nieuw team (SMOKE) dat zich zal gaan richten op accijnsfraude met sigaretten, waarbij ze ook de organisatie en de financiële stromen die met deze fraude gepaard gaan, in kaart proberen te brengen. Dit kan op termijn wellicht leiden tot een daling van deze fraude en een verminderde interesse van de georganiseerde criminaliteit. Daar staat tegenover dat de stijgende trend in illegale productie binnen Europa waarschijnlijk zal doorzetten. Ondanks internationale initiatieven lukt het niet om de illegale fabrieken snel te ontdekken. Ten slotte blijkt uit onderzoek dat er een omvangrijke online markt bestaat waar de Wet op de accijns geschonden wordt. Internet biedt nieuwe mogelijkheden voor malafide sigarettenaanbieders om structureel de wet te ontduiken en de grote accijnsverschillen tussen landen te exploiteren.

De smokkel van shag en nagemaakte shagverpakkingen naar het Verenigd Koninkrijk via Nederland neemt volgens experts toe. De afzetmarkt voor waterpijptabak groeit en daarmee ook de mogelijkheden voor fraude.
Recent is Nederlandse betrokkenheid bij fraude met minerale oliën vastgesteld. Het gaat om *designerfuels.* Over deze oliën hoeft geen, of in sommige lidstaten minder, accijns te worden afgedragen. Deze designerfuels worden veelal geproduceerd in België, en in Nederland gebruikt als brandstof voor het wegverkeer, zonder dat daar accijns of omzetbelasting over is betaald. Ook vindt er doorvoer plaats via de weg naar Duitsland en via de haven naar het Verenigd Koninkrijk. Volgens experts is sprake van een toename van zowel productie als import van deze designerfuels.

Illegaal geproduceerde sigaretten zijn op de zwarte markt verkrijgbaar voor een lagere prijs. Ook zijn ze daar verkrijgbaar voor jongeren, zonder dat er leeftijdscontrole plaatsvindt. In een enkel geval zijn ondernemers mishandeld om medewerking af te dwingen.
De huidige vastgestelde financiële schade van accijnsfraude bedraagt 25 miljoen euro, die deels voor rekening komt van de Nederlandse overheid en deels voor rekening van het buitenland. Dit bedrag betreft uitsluitend de minimale schade van gederfde belastinginkomsten. De schade ligt in werkelijkheid hoger en gaat naar verwachting nog toenemen. De algemene verwachting is dat de stijgende trend in illegale productie van sigaretten binnen Europa zal doorzetten, aangezien het onvoldoende lukt om illegale fabrieken bijtijds te ontdekken. Op grond van de bevindingen uit voorgaande jaren en de verwachte doorzettende trend, verwacht men dat er in Nederland de komende jaren meerdere illegale fabrieken actief zijn. Voor zover bekend gaat het merendeel van de geproduceerde sigaretten naar het buitenland en daar ligt dan het grootste deel van de schade door gemiste afdracht van accijns. De verdiensten van de criminele organisatie in Nederland zijn zwart en moeten worden witgewassen.

Het Nederlandse bedrijfsleven ondervindt door controles gericht op het ontdekken van accijnsfraude vertragingen en hinder tijdens het logistieke proces. Hieraan zijn kosten verbonden die worden geschat op enkele miljoenen euro's. Voorts leidt accijnsfraude tot oneerlijke concurrentie waardoor bonafide bedrijven failliet gaan of besluiten zelf te gaan frauderen om het hoofd boven water te houden. Zo geven slijterijen aan dat ze niet kunnen concurreren tegen de bodemprijzen die bepaalde winkeliers kunnen hanteren doordat zij geen accijns afdragen. Iets soortgelijks is aan de hand op de markt van het bulktransport van minerale oliën per binnenschip. Dit zorgt voor verstoring van de sociaal-economische verhoudingen en leidt tot normvervaging.
Met de verwachte stijging van accijns in Nederland zullen de verschillen in accijns met andere lidstaten groeien. Dit maakt het aantrekkelijker om goederen naar Nederland te smokkelen waarvoor de accijns niet, of in een ander land tegen een lager tarief, is voldaan.
Naar de mening van diverse experts gaat accijnsfraude in veel gevallen gepaard met ambtelijke corruptie, hoofdzakelijk in het buitenland.
Bij afzet van goederen in Nederland kan sprake zijn van vervagend normbesef. Zo zijn er complete wijken waarbinnen uitsluitend illegale sigaretten worden verkocht, terwijl de aanpak ervan achterwege blijft. Dit kan ertoe leiden dat burgers dit niet meer zien als criminaliteit maar als een normale gang van zaken.

2.11.5 Kwalificatie van dreiging

De gevolgen van accijnsfraude zijn divers. Het vastgestelde financiële nadeel dat uit inbeslagnames en onderzoek naar accijnsfraude naar voren komt, bedraagt gemiddeld jaarlijks ongeveer 24,5 miljoen euro. Dit is slechts het deel dat door opsporing en handhaving zichtbaar wordt. Het werkelijke financiële nadeel door misgelopen accijns ligt hoger. Voor zover de accijnsgoederen voor de Nederlandse markt bestemd zijn, is dit nadeel voor de Nederlandse overheid.
Naast financiële schade manifesteren zich diverse ondermijnende effecten: oneerlijke concurrentie, verstoring van sociaal-economische verhoudingen, normvervaging. Bonafide bedrijven dreigen door frauderende concurrenten uit de markt te worden gedrukt.

Er wordt voor de komende jaren een toename van fraude met accijns verwacht. Daarmee nemen niet alleen de financiële kosten toe, maar verergeren ook de ondermijnende effecten. Gelet op de huidige gevolgen van accijnsfraude en de verwachte ontwikkelingen in de toekomst vormt deze fraude voor ons land in de komende jaren een **dreiging**.

2.12 Fiscale fraude

2.12.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Thema rapportage Fiscale fraude t.b.v. NDB 2017.* Dat rapport doet verslag van een onderzoek dat in het najaar van 2016 is uitgevoerd voor dit dreigingsbeeld. De auteurs van het onderzoeksrapport zijn René Zoetekouw, Kees den Hollander en Ed van Lil, allen werkzaam bij de Fiscale Inlichtingen- en Opsporingsdienst van de Belastingdienst (FIOD). De bronnen die bij dit onderzoek zijn gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Fiscale fraude is een vorm van verticale fraude, dat wil zeggen dat de overheid slachtoffer is. Er zijn vier grote belastingbronnen:
- inkomstenbelasting: belasting op inkomsten uit loon/pensioen, winst uit onderneming, eigen woning en spaartegoeden;
- loonbelasting: inhouding van belasting en premies op uitbetaald loon/pensioen;
- vennootschapsbelasting: belasting op de winst genoten door rechtspersonen (bijvoorbeeld de nv, bv of coöperatie);
- omzetbelasting: belasting op levering van goederen en diensten (waaronder de btw).

We zullen eerst de omvang en schade van de fraude die deze vier bronnen betreffen, behandelen om vervolgens meer in detail aandacht te besteden aan btw-carrouselfraude.

2.12.2 Omvang en schade van fiscale fraude

Niet alle fiscalefraudezaken die ter kennis komen van de Belastingdienst worden aangemeld bij de FIOD ter verdere opsporing. Zaken die wel bij de FIOD worden aangemeld, voldoen aan de zogeheten meldingsrichtlijnen. Kort gezegd wordt aan de hand van die richtlijnen de ernst van de ter kennis gekomen fraudezaken bepaald. De ernstige zaken worden bij de FIOD gemeld, de kleinere zaken worden door de Belastingdienst zelf afgedaan met een bestuurs- of een administratiefrechtelijke sanctie. Van belang voor dit dreigingsbeeld is dat er bij de zaken die door de Belastingdienst zelf afgedaan worden over het algemeen geen sprake is van georganiseerde fraude. De FIOD op zijn beurt onderwerpt de aangemelde zaken in twee stappen[32] aan een volgende weging. Dit resulteert in een tweedeling: zaken die daadwerkelijk in onderzoek worden genomen en zaken die terugverwezen worden naar de Belastingdienst. De terugverwijzingen zijn in meerderheid het gevolg van schaarste aan opsporingscapaciteit en prioritering van onderwerpen. In tabel 11 staan de aantallen bij de FIOD aangemelde fraudezaken per jaar en per belastingbron.

32 Inmiddels zijn deze twee stappen (het Selectieoverleg en Tripartitieoverleg) omgezet in een zogenoemd Stuur- en weegoverleg, waardoor de besluitvorming nu in één overleg plaatsvindt.

Tabel 11. Fiscale fraude: aantal zaken aangemeld bij de FIOD naar soort belasting in de periode 2012-2015

Jaar aanmelding	Inkomsten-belasting	Loon-belasting	Vennootschaps-belasting	Omzet-belasting	Overig	Totaal
2012	282	71	38	304	31	**635**
2013	306	58	57	345	40	**670**
2014	272	51	70	443	89	**755**
2015	261	43	64	367	42	**644**
Totaal	**1121**	**223**	**229**	**1459**	**202**	**2704**

Bron: FIOD, GEFIS (Geïntegreerd fraude-informatiesysteem)[33]

In de periode 2012-2015 zijn in totaal 2704 zaken bij de FIOD aangemeld. Fraude met omzetbelasting komt het vaakst voor.

In tabel 12 staan de fraudebedragen vermeld die per jaar en per belastingbron gevonden zijn.

Tabel 12. Fiscale fraude: fraudebedragen van bij FIOD aangemelde zaken naar soort belasting (x miljoen euro)

Jaar aanmelding	Aantal zaken	Inkomsten-belasting	Loon-belasting	Vennootschaps-belasting	Omzet-belasting	Overig	Totaal bedrag
2012	635	56	19	13	65	41	€ 195
2013	670	172	37	30	50	23	€ 311
2014	755	68	19	26	59	112	€ 283
2015	644	66	9	113	55	47	€ 291
Totaal	**2704**	**€ 362**	**€ 84**	**€ 183**	**€ 229**	**€ 223**	**€ 1.081**

De 2704 zaken kenden een totaal fraudebedrag van 1081 miljoen euro. Per jaar is dat gemiddeld 270 miljoen. Hierbij moet opgemerkt worden dat het om *aangemelde* bedragen gaat, bedragen die op het eerste gezicht geschat worden. Het daadwerkelijke bedrag kan pas vastgesteld worden na diepgaand opsporingsonderzoek. Zoals we verderop nog zullen zien, komen de bedragen dan hoger uit.
Om uiteenlopende redenen (schaarste aan opsporingscapaciteit, prioritering van onderwerpen, nog niet afgerond, gevoegd met andere zaak) werden van de 2704 aangemelde zaken er 416 in de onderzoeksperiode afgerond.

In tabel 13 zien we de fraudebedragen van de afgeronde opsporingsonderzoeken en is onderscheid gemaakt naar zaken waarbij een crimineel samenwerkingsverband (csv) betrokken was en zaken waarbij dat niet het geval was.

33 Per 1 juni 2016 is dit systeem vervangen door PSF, proces systeem fraudesignalen.

Tabel 13. Fiscale fraude: opgespoord bedrag (x miljoen euro), aantal afgeronde zaken en csv-betrokkenheid

Jaar	Geen csv-zaak	Wel csv-zaak	Totaal
2012	€ 16 (60)	€ 23 (37)	**€ 39 (97)**
2013	€ 74 (59)	€ 42 (33)	**€ 117 (92)**
2014	€ 16 (77)	€ 84 (35)	**€ 101 (112)**
2015	€ 19 (66)	€ 87 (49)	**€ 106 (115)**
Totaal	**€ 125 (262)**	**€ 237 (154)**	**€ 362 (416)**
Gemiddeld per jaar	**€ 31 (65)**	**€ 59 (39)**	**€ 90 (104)**
Gemiddeld per zaak	**€ 0,48**	**€ 1,5**	**€ 0,87**

Bron: FIOD, GEFIS (Geïntegreerd fraude-informatiesysteem)

Tussen 2012 en 2015 zijn 416 strafrechtelijke onderzoeken afgerond. Deze afgeronde zaken hebben een gezamenlijk fraudebedrag van 362 miljoen euro. Het gemiddelde fraudebedrag per zaak is 870.000 euro. In 37 procent van de zaken was sprake van een crimineel samenwerkingsverband. Deze csv-zaken kennen een totaal fraudebedrag van 237 miljoen euro en een gemiddelde per zaak van 1,5 miljoen euro. Samengevat neemt 37 procent van de zaken waarbij een csv betrokken was, 65 procent van het opgespoorde fraudebedrag voor zijn rekening.

Als we de resultaten van de afgeronde opsporingszaken extrapoleren naar het totale aantal bij de FIOD aangemelde fiscalefraudezaken, kunnen we een schatting maken van het totale schadebedrag dat veroorzaakt wordt door criminele samenwerkingsverbanden. Er werden in de onderzoeksperiode 2704 fraudezaken aangemeld. We nemen aan dat 37 procent daarvan in georganiseerd verband werd gepleegd, dat zijn 1000 zaken. Uit de afgeronde opsporingsonderzoeken blijkt dat deze zaken elk een schadebedrag van 1,5 miljoen euro kennen. Dat maakt samen 1,5 miljard euro, per jaar is dat een fraudebedrag van 375 miljoen.

Voor deze berekening geldt dat het uitsluitend om ter kennis gekomen fraudezaken gaat. Het per definitie onbekende dark number is hierbij vanzelfsprekend niet inbegrepen. We moeten dus aannemen dat de feitelijke bedragen hoger liggen.

Tot zover de fiscale fraude in het algemeen, we zullen nu aandacht besteden aan een variant ervan, de btw-carrouselfraude.

2.12.3 Inleiding btw-carrouselfraude

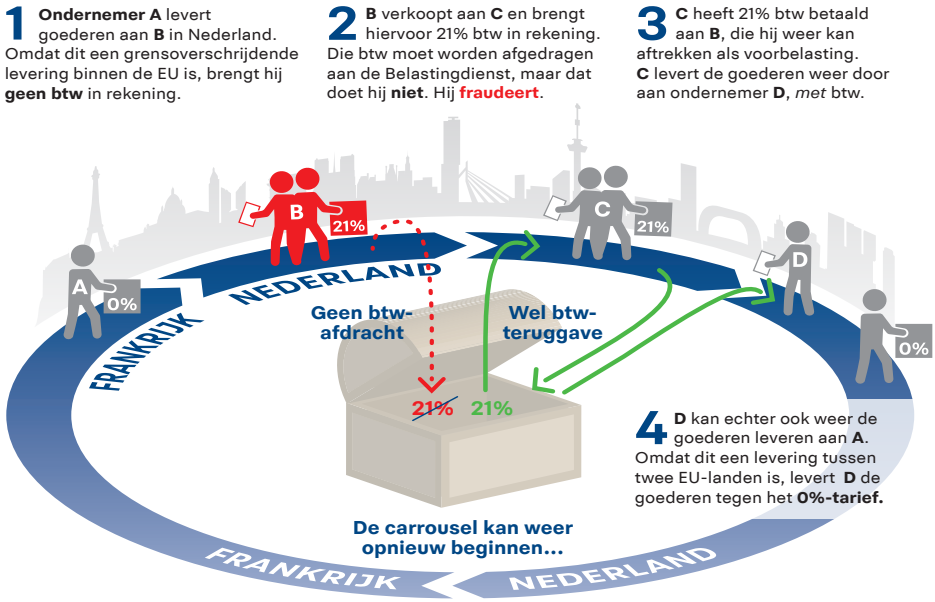
Er is een drietal redenen waarom btw-fraude hier speciale aandacht krijgt. In de eerste plaats blijkt uit een inventarisatie van de Algemene Rekenkamer uit 2008 dat btw-carrouselfraude qua fiscaal nadeel de meest omvangrijke vorm van fraude is. Ten tweede wordt btw-carrouselfraude nagenoeg altijd in georganiseerd verband gepleegd. Ten derde is de gelegenheid tot het plegen van btw-carrouselfraude groot.

Deze drie aspecten, de grote financiële schade, het georganiseerde karakter en de gelegenheden, maken dat btw-carrouselfraude binnen het geheel van fiscale fraude een bijzondere plaats inneemt.

Btw (belasting toegevoegde waarde) wordt gerekend tot de omzetbelastingen. De toegevoegde waarde is het verschil tussen inkoop- en verkoopprijs. Bij btw-carrouselfraude draagt een ondernemer geen btw af aan de Belastingdienst, terwijl hij zijn afnemers die btw wel in rekening brengt. Er zijn altijd meerdere bedrijven betrokken waarbij minimaal één bedrijf de ontvangen btw niet afdraagt aan de Belastingdienst. Dit bedrag komt dus niet in de schatkist terecht, terwijl een ander bedrijf in de keten wel de btw-vooraftrek terugontvangt. Er vloeit dus feitelijk geld uit de schatkist weg. Kenmerkend voor een btw-carrouselfraude is dat de papieren factuurstroom een andere is dan de feitelijke goederenstroom. Producten van hoge waarde, zoals smartphones, auto's, computerchips, worden bij een ondernemer in een ander EU-land ingekocht. Vervolgens vindt er levering plaats aan een Nederlandse onderneming. De ontvangende partij in Nederland factureert de goederen – inclusief btw die niet wordt afgedragen – door aan een tweede schakel in Nederland. Deze schakel/ondernemer kan de in rekening gebrachte btw in Nederland in aftrek brengen. Eventueel kan er dan vervolgens nog een levering aan een derde ondernemer plaatsvinden. Dit is de facturenstroom.

De goederenstroom loopt vaak via zogenoemde *warehouses* waar ze worden opgeslagen. Van daaruit gaan ze naar een bedrijf of ze gaan naar een warehouse of bedrijf in een ander land. De handel via warehouses is kenmerkend voor btw-carrouselfraude. Het bedrijf dat de omzetbelasting niet afdraagt, wordt ploffer of *missing trader* genoemd (B in figuur 5). Door het niet afdragen van de btw creëert men een potentiële bruto winstverhoging van 21 procent. Een ander kenmerk van de btw-carrousel is dat er een enorme prijsverlaging plaatsvindt, in de regel bij de ploffer die tegen zeer concurrerende prijzen kan leveren. De directe schade valt in het land waar de ploffer gevestigd is. Soms worden de goederen niet eens verplaatst of bestaan ze enkel op papier. Om het voor de belastingautoriteiten moeilijker te maken de frauduleuze constructie te traceren, verkoopt de ploffer de goederen soms door aan bufferhandelaars, van wie sommige bonafide zijn. Daar waar goederen of diensten die frauduleus worden geleverd, terug worden verkocht aan dezelfde leverancier om dezelfde commerciële keten opnieuw te volgen, is sprake van een gesloten cirkel, cyclus of carrousel en spreken we van 'carrouselfraude'. In figuur 5 is de carrousel schematisch in beeld gebracht.

Figuur 5. Carrouselfraude schematisch in beeld[34]



2.12.4 Recente ontwikkelingen in aard en omvang van btw-carrouselfraude

In het Nationaal dreigingsbeeld 2012 is fiscale fraude niet onderzocht. Een vergelijking met het vorige dreigingsbeeld is daarom niet mogelijk. We richten de aandacht op een aantal recente ontwikkelingen zonder die te vergelijken met een peiljaar, zoals dat in de andere paragrafen gebruikelijk is.

Aard

Er is een viertal ontwikkelingen van belang.

1. De btw-carrousels worden complexer.
   De traditionele carrouselfraude werd gepleegd door drie of vier bedrijven en er waren twee EU-lidstaten bij betrokken. Tegenwoordig zijn er meer bedrijven en meer landen bij betrokken, waardoor het lastiger wordt te bewijzen dat deze bedrijven fraude plegen.
2. Er is een grotere variëteit aan verschijningsvormen.
   De verschijningsvorm *crossed invoicing* kennen we al langer. Hierbij importeert de ploffer goederen uit een andere lidstaat en verkoopt deze binnenlands door. Deze transactie zet hij op de btw-aangifte. Daarnaast geeft hij echter een tweede fictieve transactie aan waarbij hij van een binnenlandse ondernemer gekocht zou hebben en door zou hebben verkocht aan het buitenland.
   Bij *contra trading* wordt een reguliere handelsketen gekoppeld aan een fraudeketen door de afnemer van de ploffer. Deze afnemer is een medefraudeur die gebruikmaakt

34 Figuur 5 is een bewerking van een figuur afkomstig van de Belastingdienst.

van de methode van *crossed invoicing*. De afnemer van de ploffer zit zowel in de fraudeketen als in de reguliere keten.
De *remote missing trader* is een relatief nieuwe vorm en komt de laatste tijd veel voor. Bij deze vorm zijn minimaal drie landen betrokken en vier ondernemingen. Het doel is om het bestaan van de ploffer en de relaties tussen de ondernemingen onderling te verbergen. Onderneming A in land 1 levert op papier aan onderneming B in land 2. B is de *remote missing trader*. Hij betaalt niets en geeft niets aan. Onderneming A levert de goederen aan onderneming C, de ploffer, in land 3. C verkoopt de goederen binnenlands door aan D en geeft alleen deze transacties aan. Verder wordt ervoor gezorgd dat er geen facturen zijn tussen A en C, tussen B en C et cetera. Land 3 kan geen onregelmatigheden constateren.

3. Nieuwe fraudeterreinen, verschuivingen in goederen en diensten. Binnen korte tijd kan btw-carrouselfraude in een nieuwe sector opduiken. Zo worden aantrekkelijke goederen of landen met inadequaat toezicht bewust opgezocht.
   Enkele voorbeelden:
   - Elektronische Communicatie Services (ECS). ECS betreft de handel in telefoonnummers via internet. De manier waarop de internationale telecommarkt werkt, maakt deze tot een aantrekkelijk doelwit voor btw-fraudeurs. De handelswaar heeft een bestaan gelijk aan de lengte van een telefoongesprek en er bestaat daarom geen mogelijkheid tot het onderscheppen of herleiden van goederen.
   - De energiemarkt (CO_2-rechten). De laatste jaren is er een snelle toename van de (internationale) handel in emissierechten. Er wordt in meerdere EU-landen btw-fraude met betrekking tot CO_2-rechten gepleegd.
   - Elektriciteit en gas. Btw-fraudeurs zijn zich actief gaan bewegen op de elektriciteits- en gasmarkt. Hoewel btw-fraude in deze sector moeilijker op te zetten is, zijn fraudeurs hierin al sinds 2011 actief. De grensoverschrijdende handel in gas en elektriciteit is vergelijkbaar met de grensoverschrijdende handel in CO_2-rechten.
4. Beter verhullen van financiële sporen.
   De wijdverspreide e-commerce en nieuwe elektronische wijzen van geld overmaken (bijvoorbeeld cloudbankieren) helpen de criminele spelers bij het sneller witwassen van geld, terwijl het tegelijk voor de opsporende autoriteiten moeilijker wordt om deze witwaspraktijken te signaleren. Zaten de fraudeurs vroeger allemaal nog bij hun eigen bank, daarna allemaal bij dezelfde offshore-bank, tegenwoordig maken zij gebruik van zogenoemde *payment platforms*, via *payment service providers*. Dit zijn betaalmogelijkheden die buiten een reguliere banktransactie omgaan en het naspoeren van de geldstroom bemoeilijken.

Omvang

In subparagraaf 2.12.2 is uit de doeken gedaan hoe bepaald wordt of een ter kennis van de Belastingdienst gekomen fraude ook ter verdere opsporing bij de FIOD wordt aangemeld. Om die reden beperken we ons hier tot het resultaat van die opsporing voor btw-fraudes. In tabel 14 staan die resultaten op een rijtje.

Tabel 14. Btw-carrouselfraude: opgespoord bedrag (x miljoen euro), afgeronde zaken en csv-betrokkenheid

Jaar	Afgeronde zaken	Geen csv-zaak	Wel csv-zaak	Totaal	% csv
2012	16	€ 5,00	€ 2	€ 7	33
2013	10	€ 0,39	€ 11	€ 11	97
2014	3	-	€ 41	€ 41	100
2015	8	-	€ 42	€ 42	100
Totaal	**37**	**€ 5,39**	**€ 96**	**€ 101**	**95**

Bron: FIOD, GEFIS (Geïntegreerd fraude-informatiesysteem)

De tabel laat drie met elkaar samenhangende ontwikkelingen zien. In de eerste plaats een sterke toename van de betrokkenheid van csv's bij btw-carrouselfraude, tegelijkertijd een afname van het aantal afgeronde zaken en een toename van de fraudebedragen. In 2014 en 2015 zijn uitsluitend georganiseerde vormen van btw-fraude onderzocht. Dat zijn waarschijnlijk omvangrijke zaken die veel capaciteit vragen, waardoor er minder gedaan kunnen worden. Het gaat bij de zaken van georganiseerde fraude om aanzienlijke bedragen: in 2015 een gemiddeld bedrag van 5,2 miljoen euro per zaak. Hierbij moet in het achterhoofd gehouden worden dat het om ter kennis gekomen zaken gaat die geselecteerd zijn voor verdere opsporing. Er is verder sprake van een onbekend dark number. Aangenomen moet worden dat het aantal zaken in de tabel een absolute ondergrens vormt van de feitelijk gepleegde btw-fraude.

2.12.5 Huidige gevolgen van fiscale fraude

Fiscale fraude heeft een groot aantal negatieve gevolgen voor de Nederlandse samenleving. De belangrijkste worden hieronder kort behandeld.

Financiële schade bij de overheid

Dat fiscale fraude tot financiële schade bij de overheid leidt is evident. Voor dit onderzoek is uitgegaan van de schadebedragen die aan de FIOD worden aangemeld door de Belastingdienst en voldoen aan specifieke meldingsrichtlijnen. Uitgaande van die cijfers en bedragen kunnen we vaststellen dat er per jaar gemiddeld voor 270 miljoen euro aan fraudebedragen wordt gemeld. Zoals eerder opgemerkt, betreft dit *aangemelde* bedragen die niet noodzakelijk het equivalent zijn van de werkelijke fraudebedragen. Op grond van afgeronde opsporingsonderzoeken is hierboven een schatting gegeven van 375 miljoen euro per jaar. Dat is de schade die blijkt uit de afgeronde opsporingsonderzoeken in de periode 2012-2015. Daar werd opgemerkt dat er waarschijnlijk een hoog dark number bestaat, waardoor de schade hoger uitpakt dan uit de afgeronde onderzoeken blijkt. Een bevestiging daarvan vinden we bij de Europese Commissie, die in 2016 schatte dat het fiscale nadeel van de btw-fraude voor Nederland ongeveer een derde bedraagt van de zogeheten btw-kloof[35].

35 De btw-kloof is het verschil tussen de theoretisch te verwachten opbrengst aan btw en de feitelijke opbrengst.

Dit zou betekenen dat de schade – alleen voor de btw-fraude – uitkomt op ongeveer 1,5 miljard euro per jaar. De Europese Commissie vermeldt niet welk deel hiervan voor rekening van de georganiseerde fraudes komt. Enigszins speculatief kan verdedigd worden dat bij btw-carrouselfraude dermate veel personen betrokken zijn, dat ze eigenlijk per definitie georganiseerd zijn.

Aantasting van het rechtsgevoel en vertrouwen in het fiscale systeem
Een belangrijk maatschappelijk gevolg is het verlies aan draagvlak voor belastingheffing in het algemeen, en het negatieve effect dat frauderende bedrijven uitoefenen op de belastingmoraal van bedrijven die de regels wel naleven in het bijzonder.

Concurrentievervalsing
Waar btw-fraude kan lonen voor malafide bedrijven, is ze nadelig voor bonafide bedrijven. Een btw-fraudeur kan zijn producten goedkoper aanbieden dan de bedrijven die wel btw afdragen. Indien de kosten door fiscale fraude worden gedrukt, wordt de winst groter en biedt dit mogelijkheden voor investeringen en het hanteren van lagere prijzen op de markt.

Corrumperende werking van fraude
Het ondermijnende effect van fraude raakt ook bonafide ondernemingen. Door het geven van fiscale adviezen en diensten raken zij (on)bewust betrokken bij criminele fiscale praktijken. Ook de (deels) frauderende ondernemingen zelf raken steeds verder in de problemen, ze investeren crimineel verkregen geld in de legale activiteiten en corrumperen daarmee hun eigen bedrijfsvoering. Naast beroepsfraudeurs worden ook steeds vaker gerenommeerde fiscale adviseurs betrokken bij de fraude. Dit heeft een negatieve uitstraling op de bonafide werkgever van deze malafide adviseurs.

Financiële schade bij particulieren en ondernemingen
Hoe groot de financiële schade voor particulieren en ondernemingen is, is niet te beoordelen. Voor ondernemingen vormt concurrentievervalsing een schadepost, dit kan leiden tot winstverkleining maar ook tot faillissement. Het aantal faillissementen is wel bekend, maar niet in welke gevallen er een causaal verband is met fiscale fraude. Zowel particulieren als ondernemingen ondervinden financiële schade door ongunstige belastingmaatregelen ten gevolge van derving van belastinginkomsten bij de overheid.

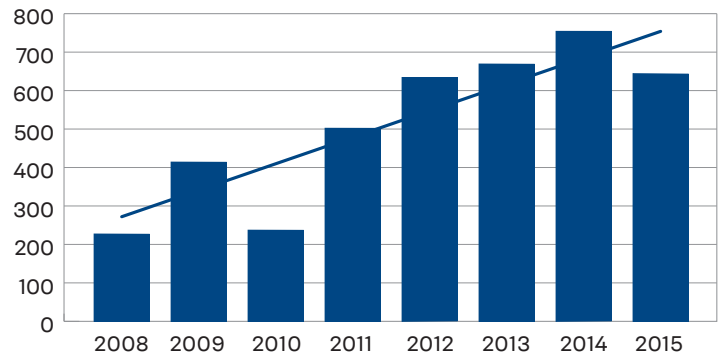
Aantasting van de integriteit van beroepsgroepen die betrokken zijn bij fraude
(Fiscaal) dienstverleners spelen de laatste jaren een steeds grotere rol bij fiscale fraudes. De aanpak van facilitatoren, zoals notarissen, accountants en advocaten, staat dan ook op de prioriteitenlijst van toezichthouders en opsporingsdiensten.

2.12.6 Verwachtingen

Omvang

Figuur 6 laat de ontwikkeling in het aantal aangemelde gevallen van fiscale fraude zien.

Figuur 6. Aantallen fiscalefraudemeldingen 2008-2015 en de lineaire trendlijn



Bron: FIOD, GEFIS (Geïntegreerd fraude-informatiesysteem)

Als we de lineaire trend extrapoleren, zal het aantal aangemelde fiscalefraudegevallen verder toenemen. Deze trend hoeft niet per se samen te gaan met een stijging van het werkelijke aantal fraudegevallen. Maar experts verwachten over het algemeen ook daarin een toename. Zij baseren dat op de volgende ontwikkelingen:

Digitalisering

Ontwikkelingen op het digitale terrein zullen voor problemen gaan zorgen. Vooral het op buitenlandse servers of in de cloud plaatsen van informatie en het gebruiken van uitzonderlijk goed beveiligde communicatie en gegevensdragers maakt het voor de opsporingsinstanties lastig om de informatie te achterhalen. Daarnaast zal steeds meer gebruikgemaakt gaan worden van digitale geldstromen en betalingsvormen. Contant geld zal een minder belangrijke rol gaan spelen. Daar hangt het toenemende gebruik van virtuele valuta als bitcoins mee samen. Het gebruik van bitcoins maakt het voor de opsporingsinstanties lastiger om te achterhalen wie achter de transacties zit, maar ook dat transacties moeilijker te traceren zijn. De anonimiteit van de transacties wordt door het gebruik van bitcoins verhoogd. Het gebruik van de blockchaintechnologie (de technologie achter de virtuele valuta) biedt echter ook kansen aan de opsporingsinstanties, vooral omdat de transacties in principe openbaar zijn.[36] De opsporingsinstanties zullen moeten investeren in kennis en kunde inzake het gebruik en het opsporen van de digitale valuta. Overigens geldt dit niet alleen voor virtuele valuta, ook het gebruik van betaalmethoden zoals de *payment service providers* (zie de paragraaf over witwassen) vraagt relatief nieuwe expertise bij de fiscale opsporing.

36 Zie voor een beknopte toelichting op de blockchaintechnologie de paragraaf over vals geld.

Internationalisering en (internationale) wet- en regelgeving
Fraude wordt internationaler. Niet alleen zijn veel van de fraudeconstructies grensoverschrijdend, ook worden de criminele gelden vaker in het buitenland gestald. Daarmee groeit de overtuiging dat belastingfraude geen nationaal maar een internationaal probleem is, dat ook door internationale samenwerking moet worden aangepakt. Desondanks blijft het erg lastig om de belastingwetgeving van de diverse landen op elkaar af te stemmen. Fraudeurs maken hier gebruik van door die landen te gebruiken waar de wet- en regelgeving het meest achterblijft en waar de fraude derhalve meer lonend is. Fraudeurs zoeken met behulp van financieel dienstverleners de zwakste schakel, en het maakt hun niet uit in welke lidstaat van de EU ze die vinden.

Criminele samenwerkingsverbanden
De organisatiegraad en daarmee de professionaliteit van de fraudeurs neemt toe. Zoals eerder al aan de orde kwam, worden specialisten zoals accountants, advocaten en notarissen ingehuurd. Zij richten rechtspersonen op en maken geldstromen onzichtbaar. Bij boekenonderzoek zal nog maar zelden administratie worden aangetroffen. De *Ultimate Beneficial Owner* (UBO, de uiteindelijk gerechtigde van het geld) is nog wel te ontdekken, maar dit is in feite een stroman. Wie de *Ultimate Criminal Owner* is, valt door de Belastingdienst in regulier toezicht niet te ontdekken.

Gevolgen

De verwachte gevolgen van fiscale fraude liggen in het verlengde van de gevolgen zoals die voor de afgelopen periode zijn beschreven: financiële gevolgen en ondermijnende gevolgen.
Zoals hierboven duidelijk werd, is de verwachting dat fiscale fraude de komende jaren zal toenemen. Hierdoor mag aangenomen worden dat ook het schadebedrag zal stijgen. Dat zal in ieder geval enkele honderden miljoenen per jaar bedragen. EU-schattingen gebaseerd op de zogeheten btw-kloof komen tot bedragen van boven de 1 miljard euro. Deze schade raakt vooral de overheid. De omvang van de financiële schade voor individuen en het bedrijfsleven is onbekend.

De schatting op grond van afgeronde opsporingsonderzoeken bedraagt op dit moment 375 miljoen euro per jaar. Dit betreft zaken die ter kennis gekomen zijn van de Belastingdienst. De verborgen gebleven fraudegevallen (het dark number) zijn hierin niet meegerekend. Gegeven de verwachte toename van fiscale fraude zal het schadebedrag waarschijnlijk toenemen.

Fiscale fraude veroorzaakt niet alleen financiële schade maar heeft ook ondermijnende effecten. Die betreffen vooral de rechtspleging en rechtsorde, het economische stelsel en verweving van boven- en onderwereld. De ondermijning van het economische stelsel en de verwevenheid worden door experts hoog genoemd. De trefwoorden daarbij zijn concurrentievervalsing, verstoring van de markt, verlies van vertrouwen in het fiscale stelsel en besmetting van beroepsgroepen zoals notarissen, accountants en advocaten.

2.12.7 Kwalificatie van dreiging

Fiscale fraude heeft een groot aantal negatieve consequenties, zowel financieel als in termen van ondermijning. De schattingen van de financiële schade lopen uiteen van enkele honderden miljoenen euro's per jaar tot een bedrag van boven de miljard euro. De schattingen houden geen rekening met het dark number en zijn respectievelijk gebaseerd op afgeronde opsporingsonderzoeken en de btw-kloof. Het is daarom plausibel te concluderen dat de financiële schade ten minste enkele honderden miljoenen euro's bedraagt. In aanvulling daarop gaat fiscale fraude gepaard met ondermijning van de rechtsorde en –handhaving en van het economische stelsel en is er een sterke verwevenheid van de boven- met de onderwereld. Deze combinatie van gevolgen leidt ertoe dat fiscale fraude een **dreiging** voor de Nederlandse samenleving vormt.

2.13 Witwassen

2.13.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Deelproject witwassen. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van een onderzoek naar het georganiseerd witwassen van crimineel geld in Nederland. Dit onderzoek is voor dit dreigingsbeeld in de eerste helft van 2016 uitgevoerd. De auteur van het onderzoeksrapport is Melvin Soudijn, werkzaam bij de politie. De bronnen die bij dit onderzoek zijn gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Witwassen wordt, net als in het NDB2012, vanuit een economische invalshoek benaderd. Dat wil zeggen dat er gekeken wordt naar het doel van witwassen, het integreren van misdaadgeld in de legale economie. Witwassen wordt daarom hier gedefinieerd als het (doen) verrichten van handelingen waardoor crimineel geld een schijnbaar wettige oorsprong krijgt. Het voorwenden van een legale herkomst vergemakkelijkt besteding zonder verdenking. De criminele herkomst van het geld kan alle terreinen van het NDB beslaan, variërend van de handel in verdovende middelen tot fraude en vermogenscriminaliteit.

2.13.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

Er bestaat een grote diversiteit aan witwasmethoden. In *Witwassen. Criminaliteitsbeeldanalyse 2012* (hierna: CBA witwassen 2012) werden deze naar negen categorieën teruggebracht. Het ging om (1) constructies met een *loanback*, (2) gefingeerde omzet, (3) gefingeerde speelwinst, (4) ABC-transacties in vastgoed, (5) *trade based money laundering*, (6) *new payment methods*, (7) leaseconstructies, (8) gebruik van stichtingen, en (9) verkoop in

consignatie. Daarnaast speelde het gebruik van contant geld zo'n belangrijke rol dat hier apart aandacht aan werd besteed.
Bijna alle witwasvormen uit de CBA witwassen 2012 zijn de afgelopen vier jaar nog steeds actueel. In sommige gevallen is sprake van nieuwe ontwikkelingen. Hieronder volgt per vorm een korte toelichting. Daarbij worden de eventueel nieuwe ontwikkelingen benoemd voor zover die op Nederland van toepassing zijn.

1. Bij een *loanback*-constructie leent de crimineel zijn eigen, door criminaliteit verkregen vermogen aan zichzelf. Daarmee houdt hij de schijn op dat het geld aan iemand anders toebehoort. Voor de buitenwereld lijkt er sprake van een legale leningsovereenkomst tussen twee partijen. Hij koopt hiermee bijvoorbeeld een huis, laat de overdracht regelen door de notaris en zijn criminele geld heeft een schijnbaar legale herkomst.
Maar loanbacks zijn niet altijd zo simpel. Wanneer het om grote vermogens gaat, nemen loanbacks vaak ingewikkelde vormen aan. Dan wordt niet meer gebruikgemaakt van particuliere leners maar zijn er financiële instellingen, bedrijven, trusts en buitenlandse offshorevennootschappen tussen geschoven.
Een nieuwe ontwikkeling binnen de methode van loanback is het gebruik van een crowdfundingplatform. Crowdfunding is een vorm van publieke financiering. Voor het startkapitaal van een project worden kleine particuliere investeerders direct benaderd, in plaats van dat gebruik wordt gemaakt van een grote financieel intermediair zoals een bank. Een particulier kan vaak al voor een laag bedrag inleggen, en het effect van de *crowd* (veel kleine particulieren) zorgt uiteindelijk voor voldoende kapitaal. Crowdfunding kan ook voor witwassen worden gebruikt. Een voorbeeld: een verdachte richt zich tot de crowd voor de financiering van een vastgoedobject om zijn misdaadgeld een schijnbaar legale herkomst te geven. Op een website tekenen enkele tientallen personen in voor bedragen variërend van enkele honderden tot duizenden euro's. Het vermoeden bestaat dat deze personen gefingeerd zijn en dat de verdachte er zelf achter zit of dat de personen weliswaar bestaan, maar niet zelf betalen.

2. Binnen de categorie gefingeerde omzet, waarbij crimineel geld gemengd wordt met legale omzet uit een regulier bedrijf, hebben zich geen nieuwe ontwikkelingen voorgedaan.

3. Er is sprake van gefingeerde speelwinst wanneer crimineel geld voorgesteld wordt als speelwinst die in een casino is behaald. Binnen dit gebied hebben zich evenmin ontwikkelingen voorgedaan.

4. De ABC-transactie, waarbij onroerend goed in korte tijd diverse keren tegen een hogere prijs wordt verkocht, wordt nog steeds aangetroffen. Dit betreft een min of meer traditionele manier van witwassen die weinig evolueert.

5. In de categorie *trade based money laundering* (TBML) wordt het (inter)nationale handelsverkeer gebruikt. Legale internationale goederenstromen lenen zich uitstekend om crimi-

neel geld te verplaatsen door het enorme volume dat daarin omgaat, de complexiteit rond de financiering ervan en de gebrekkige internationale uitwisseling van douanegegevens. Als variant op TBML bestaat de zogeheten *sham litigation*, die in de CBA witwassen 2012 nog niet voorkwam. Twee partijen wenden daarbij een zakelijk conflict voor dat ze voor de rechter brengen. De ene partij heeft daar een boeteclausule op gezet die de andere partij dan moet betalen.

6. *New Payment Methods* (NPM) zijn nieuwe betaalsystemen waarmee geld wordt weggesluisd, verhuld of geïnvesteerd. Recent wordt gesproken van NPPS (*New Payment Products and Services*). Het betreft hier vooral mobiele betalingen en *internet-based payment services*. Witwassen met mobiele betalingen is in de onderzoeksperiode niet in Nederland gezien, maar internet-based payment services des te meer. Daarbij wordt ook gebruikgemaakt van cryptocurrency's, zoals de bitcoin. In deze digitale portemonnees kunnen accounthouders bedragen aanhouden zonder bancaire tegenrekening in de analoge wereld. Een nieuwe ontwikkeling bij NPPS die in Nederland is gezien, is het gebruik van een *payment service provider* (PSP). Een PSP is een online betaaldienst die de betalingen aan winkeliers afhandelt. Het voert hier te ver om allerlei technische varianten van de PSP te behandelen. Relevant is dat uit opsporingsonderzoeken is gebleken dat het gebruik van een PSP de crimineel niet alleen kan helpen bij het verhullen van de herkomst van zijn omzet, maar ook bij het verhullen van de identiteit van zijn cliënten. De reden hiervoor is dat een PSP vaak verschillende transacties opspaart om deze in een grotere *batch* bij de bank aan te leveren. Omdat de transacties dan niet meer op consumentenniveau zijn uitgesplitst, kan de bank niet controleren of de regels zijn nageleefd (*compliance*). Soms richten verdachten zelf een PSP op. Heeft de crimineel een eigen PSP tot zijn beschikking, dan biedt dat hem een goede mogelijkheid om zijn cliënten of zijn omzet te verhullen.

7. Bij het leasen en huren van auto's en woonruimte wordt het verschuldigde leasebedrag contant met crimineel geld betaald. Het is een nog altijd voorkomende vorm van witwassen, die bestand is tegen veranderingen.

8. Bij witwassen met behulp van stichtingen moet vooral gedacht worden aan een stichting administratiekantoor. Net als in de CBA witwassen 2012 komt de stichting administratiekantoor in de huidige onderzoeksperiode in enkele witwasconstructies naar voren. Zulke stichtingen zijn opgericht ten behoeve van investeringen van vermogen in Nederland. Daar wordt doorgaans onroerend goed in ondergebracht of de aandelen van een vennootschap waarin vastgoed het vermogen vormt. De stichting geeft daarop certificaten uit waarmee recht op dividend kan worden geclaimd. Met andere woorden, de stichting heeft het juridisch eigendom (van de aandelen van de vennootschap) en de certificaathouders hebben het economisch eigendom (van de vennootschap). Een kenmerk van deze certificaten is dat het eigendom of de eigendomsoverdracht niet in openbare registers valt terug te vinden. Het juridische eigendom van onroerend goed kan weliswaar worden opgezocht in het Kadaster, maar het economisch eigendom moet blijken uit het register van certificaathouders dat vaak

op het kantoor van de stichting wordt bijgehouden. Dit register kan derhalve niet zomaar door derden/buitenstaanders worden geraadpleegd. Ook bestuurswisselingen zijn nergens verplicht vastgelegd en daardoor voor derden/buitenstaanders moeilijk te onderzoeken.
In een opsporingsonderzoek bleek dat een stichting derdenrekening werd misbruikt en er is informatie dat dit geen incident is. Een stichting derdenrekening is een legale constructie om derdengelden (geldsommen van derden die door bepaalde beroepsgroepen, zoals advocaten, notarissen of gerechtsdeurwaarders uit hoofde van hun functie worden beheerd) te beschermen in geval van een eventueel faillissement van de dienstverlener. Deze gelden worden dan niet tot het vermogen van de rekeninghouder gerekend, maar staan daar slechts 'geparkeerd'. In enkele gevallen is gebleken dat criminelen een beheerder (notaris, advocaat) van zo'n rekening hadden gecorrumpeerd. Door hun beroepsgeheim was de herkomst van het geld op de derdengeldrekening extra afgeschermd. De manier waarop gebruik wordt gemaakt van stichtingen is aan weinig verandering onderhevig.

9. Bij de consignatieconstructie neemt een bemiddelaar (vaak een handelaar) voor persoon A een of meer objecten onder zijn hoede. Het is dan de taak van de bemiddelaar om een koper (persoon B) voor de betrokken objecten te zoeken. Consignatie als witwasmethode houdt vaak in dat de crimineel een bemiddelingsrol fingeert. De goederen die hij in consignatie heeft, behoren echter in werkelijkheid aan hemzelf toe. Het voordeel hiervan is dat het goed dat zogenaamd in consignatie is gegeven niet aan de crimineel kan worden toegeschreven. Deze vorm van fraude wordt nog maar weinig gezien en lijkt niet langer relevant.

Ten slotte kan crimineel geld ook simpelweg contant worden uitgegeven in het legale economische verkeer zonder dat het een traject van plaatsen en verhullen heeft doorgemaakt. Sommige criminelen laten het geld goed rollen en geven dagelijks duizenden euro's contant uit aan een 'patser'-levensstijl. Net als in de CBA witwassen 2012 wordt in de huidige onderzoeksperiode gezien dat contant geld in een omvangrijke criminele diensteneconomie rondgaat. Opvallend daarin is dat grote bedragen crimineel geld contant naar het buitenland worden verplaatst of gesmokkeld. Het criminele geld komt vervolgens in het buitenland in het financieel stelsel terecht dankzij corrupt bankpersoneel of financieel facilitatoren aldaar. Er is echter weinig zicht verkregen op hoe dit precies in zijn werk gaat, omdat het zich in het buitenland afspeelt.
Nieuw is dat het *bank-to-bank* vervoerssysteem van contant geld incidenteel is gebruikt. Dit systeem betreft internationale contantgeldstromen tussen banken, waarbij via speciale vervoersbedrijven contanten als cargo of in postzakken worden vervoerd. Voor dit vervoer bestaan geen speciale douanevereisten, het volstaat om aan te geven om hoeveel kilo papiergeld het gaat. *De Ultimate Beneficial Owner* (UBO, de uiteindelijk belanghebbende) en de betrokken banken hoeven niet te worden vermeld.

Bij witwassen van crimineel geld zijn vrijwel altijd personen betrokken die hand-en-span-diensten verlenen. Hun rollen verschillen. In het algemeen kan een onderscheid gemaakt worden tussen personen die moeten verhullen wie de verantwoordelijke voor het witwasproces is (de katvangers) en personen die dankzij hun kennis en vaardigheden specialistische diensten verlenen (de facilitatoren). Meerdere van de financieel facilitatoren zijn in het criminele milieu goed bekend. Dat blijkt uit het feit dat diverse criminelen bij hen uitkomen voor dienstverlening.
Uit opsporingsonderzoek blijkt dat er sprake is van een relatief grote groep meldplichtige financieel dienstverleners die het niet zo nauw neemt met de regels van compliance zoals bedoeld in de Wet ter voorkoming van witwassen en financiering van terrorisme (Wwft). Zij verrichten bijvoorbeeld onvoldoende cliëntenonderzoek, waardoor het niet te doorgronden valt wie de UBO is. Deze dienstverleners opereren op de reguliere markt. De schijn van legaliteit wordt daarmee versterkt. Een gevolg is dat de Nederlandse financiële markt via deze dienstverleners toegankelijk is voor crimineel geld.
Nieuw ten opzichte van de CBA witwassen 2012 is een bepaalde vorm van facilitering in het FinTech-domein. Het betreft IT'ers die onderlegd zijn in (nieuwe) financieel-technologische ontwikkelingen en daarvoor producten kunnen aanbieden. Te denken valt aan het bouwen van een PSP, het bouwen van een crowdfundingplatform of het wisselen van bitcoins. Personen die zich met deze laatste activiteit bezighouden, worden de afgelopen vier jaar steeds vaker in Nederlandse opsporingsonderzoeken aangetroffen. Het verschaffen van een bitcoin *exchange service* is op zich legaal. Maar in de opsporingsonderzoeken is gezien dat diverse exchangers bewust hun diensten aanbieden aan criminelen.
Een andere groep facilitatoren houdt zich uitsluitend bezig met (het verplaatsen van) contant geld. In de onderzoeksperiode is zicht verkregen op meer dan honderd ondergrondse bankiers. Het grootste deel van de facilitatoren in het contantgeldcircuit houdt zich bezig met het op een of andere manier over de landsgrenzen brengen van crimineel geld. Omdat Nederland gekenmerkt wordt door transitcriminaliteit, is er veel vraag naar hun diensten.

Omvang

De totale omvang van de Nederlandse witwasmarkt is onbekend. In 2007 werd in een onderzoek van de universiteit van Utrecht becijferd dat het om 18,5 miljard euro zou gaan. Sindsdien is geen uitputtend wetenschappelijk onderzoek gedaan naar de omvang van de witwasmarkt. Het onderzoek uit 2007 werd kritisch ontvangen.[37]
Een complicerende omstandigheid bij het vaststellen van de omvang is dat een schatting uitgesplitst zou moeten worden naar een deel dat in Nederland wordt gegenereerd en in Nederland wordt witgewassen, een deel dat in Nederland wordt gegenereerd en in het buitenland wordt witgewassen, en een deel dat in het buitenland wordt gegenereerd maar in Nederland wordt witgewassen. Elk van die categorieën heeft een (omvangrijk) dark number. Alleen al in de laatste categorie zal het vermoedelijk om enorme bedragen gaan. Daar komt bij dat het onderscheid tussen fraude (illegaal) en 'agressieve belastingplanning' (rechtma-

37 Voor een uitgebreide kritiek, zie de CBA witwassen 2012, pp. 60-66.

tig) vaak niet te maken is zonder alle details te kennen. Maar die details onttrekken zich nu juist aan het zicht door het gebruik van allerlei ingewikkelde constructies.

Zonder dat we dit met cijfermateriaal kunnen onderbouwen, blijkt uit interviews en dossieranalyse dat de loanbackconstructie en de gefingeerde omzet tot de meestgebruikte vormen van witwassen behoren. Overigens kan wel een ruwe maar niettemin beredeneerde benadering van de totale omvang gemaakt worden. Witwassen is het onvermijdelijke sluitstuk van de georganiseerde criminaliteit. Wil een crimineel over zijn geld kunnen beschikken, dan zal het overgrote deel ervan witgewassen moeten worden. Alleen dat deel dat direct contant in de legale economie wordt gespendeerd of waarmee andere criminele activiteiten worden gefinancierd, wordt niet economisch witgewassen. Die premisse leidt tot de conclusie dat de totale witwasmarkt bij benadering een vergelijkbare omvang moet hebben als de inkomsten uit criminaliteit. Die zal jaarlijks in de miljarden lopen.

2.13.3 Huidige gevolgen

Aan het fenomeen witwassen kunnen diverse nadelige gevolgen worden toegeschreven. Het meest in het oog springen de financiële gevolgen, maar er zijn ook andere, zoals verweving van boven- en onderwereld, normvervaging en economische gevolgen. We zullen de belangrijkste hieronder behandelen.

De *financiële gevolgen* zijn vermogensafname door verlies van geld of goed. Vermogensafname wordt hier opgevat als fiscaal nadeel. Er kan bijvoorbeeld gedacht worden aan het betalen van zwart geld boven op de koopsom van een vastgoedobject om de overdrachtsbelasting te drukken, het ontduiken van heffingen of belastingen, en het naar beneden bijstellen van de waarde of hoeveelheid van de werkelijke hoeveelheid geïmporteerde of geëxporteerde goederen. Ook het inschakelen van *brokers* zorgt ervoor dat werkzaamheden, transacties en winsten niet door de overheid kunnen worden belast.
Behalve van vermogensafname is er soms ook sprake van vermogenstoename. Door wit te wassen wordt namelijk geprobeerd om vermogen (crimineel geld, vaak ook onbelast) in het financiële systeem te brengen en aan bepaalde legale entiteiten (personen of ondernemingen) toe te schrijven. Hier kan dan vervolgens belasting over worden geheven, een vermogenstoename dus.
Betrouwbare schattingen van de totale vermogenstoe- of -afname in Nederland als gevolg van witwassen zijn niet voorhanden. De bijdrage aan het nationaal inkomen in Nederland van bepaalde illegale activiteiten (waaronder drugshandel) wordt door het Centraal Bureau voor de Statistiek op 2,6 miljard euro gesteld. Diverse vormen van fraude zijn daarbij niet meegerekend.
Het fiscale nadeel ten gevolge van witwassen wordt geschat op een bedrag van ten minste honderden miljoenen euro's.

Verweving onder- en bovenwereld - Er is waarschijnlijk geen enkele criminele activiteit waarbij op zo'n uitgebreide schaal sprake is van verweving als bij witwassen. De voorbeelden ervan zijn legio: het bezit van of de zeggenschap over bedrijven die als dekmantel kunnen fungeren, het vermengen van crimineel geld met de legale omzet van een bedrijf, investeringen in vastgoed, het gebruiken van talrijke soorten legale facilitatoren voor transacties en constructies, het sponsoren van sportclubs, donaties aan geloofsgemeenschappen, et cetera. De gevolgen hiervan zijn niet in geld uit te drukken. Het (sluipende) gevaar schuilt er vooral in dat het onderscheid tussen goed en kwaad eigenlijk niet meer te maken is, waardoor te goeder trouw handelende mensen ongewild betrokken raken bij louche praktijken. Witwassen heeft daarmee een ondermijnende werking.

Economische gevolgen - Hoewel er op nationaal niveau geen sprake is van verstoring van de sociaal-economische verhoudingen, wordt wel het vertrouwen in het financiële stelsel geschaad en laat zich op lokaal niveau en kleinere schaal soms de negatieve invloed gelden van oneerlijke concurrentie. De onderneming van de crimineel hoeft geen winst te maken en kan daardoor goedkopere producten of diensten aanbieden dan de legale concurrent. Of de onderneming ontduikt toezicht, zoals in het geval van illegale geldtransactiekantoren, waardoor ze minder onkosten heeft. Ook kan worden gedacht aan de invloed van ondernemingen die feitelijk geen bestaansrecht zouden hebben op grond van het plaatselijke winkelaanbod. Een sterke oververtegenwoordiging van één soort onderneming (bijvoorbeeld ijssalons, shoarmazaken, belwinkels) is hier een aanwijzing voor.
Andere mogelijke effecten van witwassen op sociaal-economische verhoudingen die in de internationale literatuur worden benoemd, zijn louter hypothetisch beredeneerd maar nog niet feitelijk aangetoond, zoals vertekeningen op het gebied van consumptie, investeringen en spaargelden, stijgende prijzen, veranderingen in import en export, economische groei of rem, werkgelegenheid, veranderingen in wisselkoersen, grotere beschikbaarheid van krediet, hogere *capital inflows,* veranderingen in directe buitenlandse investeringen en liquiditeitsproblemen van de financiële sector.
Het is met zekerheid te stellen dat veel witgewassen geld in Nederlands vastgoed terechtkomt. Alleen al de betrokkenheid van tal van financieel facilitatoren in de vastgoedbranche duidt hierop. Het is echter niet bekend wat de omvang hiervan is. Het is daardoor ook onduidelijk in hoeverre crimineel geld dat in vastgoed wordt belegd, (lokaal) invloed heeft op de huizenprijzen op de vastgoedmarkt. Bovendien speelt hier nog een ander probleem. Wanneer Nederlands vastgoed door een buitenlandse entiteit wordt aangeschaft of beheerd, kan de eigenaar van deze entiteit ervoor kiezen uit het zicht te blijven, bijvoorbeeld door via een offshore-constructie een Nederlands vastgoedobject te kopen. We weten in Nederland dan niet wie de werkelijke eigenaar is.

Politieke en bestuurlijke beïnvloeding - De nationale politiek in Nederland wordt niet door witwassen beïnvloed. Er is geen enkele indicatie dat witgewassen geld dat uit criminaliteit is verkregen op grote schaal gebruikt wordt om op nationaal niveau besluitvormingsprocessen te beïnvloeden.
Op lokaal niveau is soms wel sprake van enige invloed. De meest spraakmakende zaken betreffen vier lokale politici die voor witwassen zijn vervolgd. Twee personen ontvingen smeergeld van vastgoedondernemers. Hierbij kan gesteld worden dat er sprake was van lokale ondermijnende overheidsbeïnvloeding op het gebied van aanbestedingsprocedures.

Gezondheid - In verband met witwassen zijn in de periode 2012-2015 drie doden en minstens twintig gewonden gevallen. Sommige gewonden liepen ernstig letsel op door schietpartijen. Dit is opmerkelijk want witwassen wordt doorgaans als een slachtofferloos delict voorgesteld. Geweld in relatie tot witwassen is niettemin verklaarbaar. Het komt tot uitbarsting als iemand zijn geld niet ontvangt of kwijtraakt door misgelopen witwastrajecten. Of wanneer niet-liquide middelen, zoals beleggingen in huizen, niet snel genoeg liquide kunnen worden gemaakt of minder opleveren dan aanvankelijk was voorgesteld. Ook komt het voor dat een financieel dienstverlener simpelweg de boel heeft opgelicht. Door het ontbreken van reguliere middelen om conflicten te beslechten wordt dan met enige regelmaat de toevlucht tot geweld genomen.

2.13.4 Verwachtingen

Er zullen zich de komende jaren financieeltechnische ontwikkelingen voordoen die van grote invloed zijn op de financiële sector. De traditionele bankensector staat een tijd van veel veranderingen te wachten. Een van de belangrijkste ontwikkelingen betreft de toepassing van de blockchaintechnologie. Dit is de technologie die onder meer gebruikt wordt voor cryptocurrency's zoals de bitcoin. Maar dat is slechts een van de toepassingen. In feite gaat het om een openbaar grootboek waarin allerlei transacties worden vastgelegd, variërend van de (ver)koop van onroerend goed tot aandelentransacties en het opmaken van aktes. De essentie van de blockchaintechnologie is dat de tussenpersoon bij transacties overbodig wordt. Partijen bij transacties kunnen rechtstreeks met elkaar zakendoen omdat het grootboek openbaar is en wereldwijd gedistribueerd wordt. Hierdoor worden bijvoorbeeld notarissen, financieel dienstverleners, makelaars en andere intermediairs in beginsel overbodig, voor zover het hun niet-wettelijke taken betreft.
De vraag is of en zo ja welke invloed deze onvermijdelijk voortschrijdende ontwikkeling heeft op witwassen. Het antwoord daarop is niet eenduidig. Enerzijds biedt het criminele mogelijkheden, anderzijds kan ook de bestrijding er haar voordeel mee doen.
Bitcoins bijvoorbeeld worden niet als wettig betaalmiddel erkend. Daarmee vallen bitcoins niet onder de reikwijdte van de Wet op het financieel toezicht (Wft)[38] en houdt De Nederlandsche Bank ook geen toezicht op deze virtuele valuta of de ondernemingen die hierin handelen. Hierdoor kunnen bitcoinhandelaars geen officiële melding van verdachte

38 Er zijn plannen om de bitcoin onder wettelijk toezicht te brengen. Op welke termijn is echter onbekend.

transacties doen bij de Financial Intelligence Unit Nederland (FIU). Althans, het ontbreekt hun dan aan wettelijke bescherming tegen de klant die zich door de melding misschien gedupeerd voelt en de melder een proces aandoet. Dit biedt kansen aan criminelen om wit te wassen.
Anderzijds verschaft het gebruik van de blockchain (die per definitie openbaar is) ook de overheid real time toegang tot allerlei transacties. Als vastgoeddeals straks via de blockchain verlopen, kunnen ze door het openbare karakter direct door de overheid worden ingezien of gecontroleerd door deze af te zetten tegen allerlei relevante databanken.
Hoe een en ander per saldo zal uitpakken is ongewis.

In de Veiligheidsagenda 2015-2018 is aangegeven dat de opsporing zich sterk op allerlei soorten facilitatoren dient te richten die het criminele proces ondersteunen. Het ligt in de lijn der verwachting dat de aanpak van financieel facilitatoren daarom verder zal worden geïntensiveerd. Facilitatoren spelen een centrale rol bij veel witwasconstructies.

Er zijn diverse internationale ontwikkelingen die van invloed kunnen zijn op de praktijk van het witwassen. Door bijvoorbeeld de openbaarmaking van de Panama-papers is er veel aandacht voor belastingontwijking en -ontduiking. Er bestaat zowel bij publiek als politiek verontwaardiging over de enorme bedragen die ermee gemoeid zijn en de bedenkelijke moraal die eraan ten grondslag ligt. Bovendien zijn landen die dergelijke constructies toestaan ook gemakkelijk bruikbaar voor het witwassen van crimineel geld.
Daarom wordt verwacht dat Europa actiever gaat optreden tegen belastingontwijking en daardoor minder aantrekkelijk zal worden om onbelast of fout vermogen uit het zicht te parkeren. Dat zal als gevolg hebben dat andere, verdere bestemmingen aantrekkelijker worden. Niet alleen Caribische eilanden komen dan als mogelijkheid in beeld, maar ook Azië (Hongkong, Singapore, Dubai). Ook Delaware in de Verenigde Staten is vanwege de constructies die daar mogelijk zijn een goede optie.

Een Europese trend is de terugdringing van het gebruik van chartaal geld. In Nederland worden consumenten aangemoedigd om zo min mogelijk contant te betalen. In sommige winkels kan alleen nog maar worden gepind. De redenen daarvoor zijn divers. Het is een kostenbesparing voor de winkelier, bevordert een snellere doorstroom van klanten en verlaagt het risico op overvallen. Denemarken heeft het plan om als eerste land een cashloze samenleving te worden. Dat doel zou in 2030 moeten worden bereikt. Maar ook Zweden en Noorwegen hebben plannen in die richting. In diverse Europese landen (Italië, België) zijn inmiddels grenzen aan betalingen met contant geld gesteld.
Een andere manifestatie van hetzelfde fenomeen is dat de Europese Centrale Bank (ECB) op 4 mei 2016 heeft besloten het 500 eurobiljet af te schaffen. Naar verluidt zou het regelmatig gebruikt worden bij criminele transacties. Het bankbiljet zal geleidelijk verdwijnen wanneer het vanaf eind 2018 niet langer uitgegeven wordt. Het is nadien nog wel een geldig betaalmiddel, maar zal in de jaren daarop via het bankverkeer worden ingenomen.

Afschaffen van chartaal geld kan tal van geweldsdelicten en vermogenscriminaliteit in relatie tot contant geld (overvallen, straatroven, afpersingen, diefstallen) doen afnemen. Het kan verder belastingontduiking en witwassen tegengaan omdat girale betalingen altijd sporen nalaten, in tegenstelling tot chartale betalingen.
Omdat de implicaties zo groot zijn, zal naar verwachting in de komende jaren chartaal geld nog niet worden afgeschaft. Het ontmoedigen van het gebruik van chartaal geld en het bevorderen van giraal geld, zal met de tijd kunnen leiden tot criminaliteitsverschuivingen. Minder straatroven, maar meer creditcardfraude en meer gehackte bankgegevens. Het is aannemelijk te veronderstellen dat ook het gebruik van *prepaid debetcards* en cryptocurrency's zal gaan toenemen, alsmede manieren om digitaal geld onzichtbaar voor de overheid te maken.

Loanback en gefingeerde omzet zullen de belangrijkste vormen van witwassen blijven. Binnen de loanbackconstructie zal het instrument van crowdfunding toenemen.
Met betrekking tot gefingeerde speelwinst zal de nieuwe wet op de kansspelen nieuwe mogelijkheden bieden. Vooral het legaliseren van online gokken zal hierin een rol gaan spelen.
Door de strengere controle op contante geldstromen en het afschaffen van het 500 eurobiljet ligt het in de rede dat *trade based money laundering* een grotere vlucht zal nemen.
De snelle ontwikkelingen op het gebied van digitale technologie zullen ook hun sporen nalaten bij het financiële verkeer. De rol van de New Payment Products and Services zal toenemen. Deze kunnen in het betalingsverkeer namelijk beter kosten besparen dan de reguliere banksector. Dit gaat echter wel gepaard met een risico op verslechtering van de compliance. Ook is de drempel om een Payment Service Provider (PSP) te beginnen minder hoog dan het lijkt. Een enkel individu met technologische knowhow kan al een PSP opstarten. Dat maakt dat ook malafide PSP's kunnen worden opgezet.
Voor de overige vormen van witwassen worden weinig veranderingen verwacht.

De gevolgen van witwassen voor de Nederlandse samenleving in de periode 2012-2017 zijn in een eerdere paragraaf uitgebreid beschreven. Een belangrijke constatering was dat we de omvang (de hoeveelheid crimineel geld) niet kennen, maar dat te beredeneren valt dat de Nederlandse overheid enkele honderden miljoenen aan belastinginkomsten derft. Daarnaast – en dat is evenmin precies te becijferen – draagt crimineel geld ook bij aan het nationale inkomen van Nederland.
Behalve financiële consequenties kent witwassen een hele reeks aan andere ongewenste gevolgen. Die zijn samen te vatten onder de algemene noemer van ondermijning. Door het inschakelen van allerlei financieel facilitatoren gaat het dan vooral om verweving van onder- en bovenwereld. Van economische schade en politieke en bestuurlijke beïnvloeding is eigenlijk alleen op lokaal niveau sprake. Daardoor is de impact op de Nederlandse samenleving als geheel klein.

Een vaak onderbelicht fenomeen is het gebruik van geweld binnen de witwassector; dit is de laatste jaren toegenomen en de verwachting is dat het aantal doden en gewonden de komende jaren wederom enkele tientallen zal bedragen.
Voor de komende jaren worden diverse veranderingen verwacht binnen de financiële sector. Die zullen vooral technologisch van aard zijn en effect hebben op de *manieren* waarop wordt witgewassen. De gevolgen – zowel kwantitatief als kwalitatief – zijn hiervoor echter betrekkelijk weinig gevoelig en zullen weinig veranderen.

2.13.5 Kwalificatie van dreiging

Witwassen is het 'sluitstuk' van georganiseerde criminaliteit. Om vrijelijk over het crimineel verdiende geld te kunnen beschikken, is het noodzakelijk er een schijnbaar legale herkomst aan te geven. De verwachte ontwikkelingen voor de jaren 2017-2021 rond witwassen laten eenzelfde beeld zien als de huidige situatie. Er doen zich weliswaar (technologische) ontwikkelingen voor op het gebied van de financiële dienstverlening, maar in hoeverre die van invloed zijn op het fenomeen witwassen is onzeker. Zo bestaat er een trend om chartaal geld terug te dringen, is geïnvesteerd in de analyse van *big data* waardoor signalen van witwassen eerder worden opgemerkt, worden op termijn de biljetten van 500 euro uit de circulatie genomen, lijkt de blockchaintechnologie (in de vorm van bitcoins) in de komende jaren een belangrijke rol te gaan spelen, wordt de aanpak van facilitatoren voortgezet en zijn er internationale afspraken over de bestrijding van witwassen. Sommige van deze ontwikkelingen zullen een remmende invloed hebben op witwassen, andere zullen witwassen eenvoudiger maken. De uitkomst per saldo is ongewis. Van belang blijft dat witwassen de motor van het criminele bedrijf is, dat er miljarden mee gemoeid zijn, dat de financiële schade in de honderden miljoenen euro's loopt, het bepaalde vormen van ondermijning met zich meebrengt en er in voorkomende gevallen sprake is van geweld. Deze overwegingen maken dat witwassen een **dreiging** voor de Nederlandse samenleving vormt.

3 Georganiseerde vermogenscriminaliteit

3.1 Inleiding

Vermogenscriminaliteit is een verzamelterm voor strafbare feiten die verwant zijn aan diefstal van geld en/of goederen. Het brede scala aan verschijningsvormen komt slechts deels aan bod. Het gaat vooral om de vormen die in georganiseerd verband worden gepleegd en de nadruk ligt op vermogenscriminaliteit die de grenzen van politie-eenheden overschrijdt. De volgende vormen komen aan bod:

- woninginbraak
- bedrijfsinbraak
- winkeldiefstal
- kraken op geldautomaten
- overval
- ladingdiefstal
- autocriminaliteit
- heling
- afpersing

3.2 Woninginbraak

3.2.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Georganiseerde vermogenscriminaliteit. Nationaal Dreigingsbeeld 2017.* Dat rapport is een verslag van onderzoek naar zes vormen van vermogenscriminaliteit, woninginbraak is er daar een van. De auteurs van het onderzoeksrapport zijn Jessica van Mantgem, Anne Mooij, Ewout Stoffers, Emilie Verschuuren, Debbie Mac Gillavry en Marsha de Bell, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*

Aan het eind van deze paragraaf wordt de kwalificatie van dreiging beschreven. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is beargumenteerd en vastgesteld in een andere context door een groep van beoordelaars (de consensusgroep).

Bij woninginbraken gaat het om diefstal van geld en/of goederen uit woningen waarbij sprake is van braak, het illegaal openbreken van een woning.

3.2.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

Na een periode waarin het aantal geregistreerde woninginbraken steeg, van 2007 tot 2012, daalt het aantal nu weer, zie tabel 15.

Tabel 15. Ontwikkeling van het aantal woninginbraken in de periode 2012-2015

	2012	2013	2014	2015
Absoluut aantal	91.716	87.508	71.135	64.560
Percentage afname		-5%	-19%	-9%
Percentage opgehelderd	9%	9%	9%	7%
Percentage poging	28%	30%	31%	31%

Ten opzichte van 2012 is het aantal woninginbraken in 2015 gedaald met 30 procent, van bijna 92.000 naar ruim 64.500 woninginbraken. Een deel van de woninginbraken wordt gepleegd door criminelen in georganiseerd verband. Volgens onderzoek uit 2009 en 2012 ligt dat aandeel op 20 à 30 procent. Recentere gegevens omtrent de betrokkenheid van georganiseerde criminaliteit zijn niet voorhanden. Als de georganiseerde criminaliteit ook nu nog een aandeel van 20 procent heeft, dan zijn ten minste 12.500 van de geregistreerde woninginbraken gepleegd door georganiseerde criminele samenwerkingsverbanden.

Het ophelderingspercentage blijft gelijk, met een lichte daling in 2015 (hoewel het percentage uit 2015 waarschijnlijk nog iets hoger uitkomt door na-ijleffecten in de registraties). Effectief betekenen deze cijfers dat er in 2015 een paar duizend woninginbraken minder zijn opgehelderd dan in 2012. Bijna een derde van de in 2015 geregistreerde woninginbraken bleef beperkt tot een poging.

Het aantal geregistreerde verdachten van woninginbraken is de afgelopen jaren afgenomen. In 2012 werden 8600 verdachten aangehouden, in 2014 waren dit er ruim 6300.

Aard

In de afgelopen jaren is er een aantal veranderingen of verschuivingen zichtbaar in de wijze waarop woninginbraken worden gepleegd.

Nachtelijke inbraken nemen af, van 18 procent in 2007 naar 12 procent in 2014. Het merendeel van de woninginbraken, ruim 60 procent, wordt gepleegd in de middag- en de avonduren.
Het ‘cilindertrekken’ als inbraakmethode lijkt sinds 2012 vaker voor te komen. Aan de andere inbraakmethoden en het gebruik van inbrekerswerktuig is weinig veranderd.
Een nieuw gesignaleerde werkwijze is het inbreken in sleutelkluisjes waar thuiszorgmedewerkers de huissleutels van hulpbehoevende bewoners uit kunnen halen. Daarbij forceert een inbreker het kluisje, dat meestal naast of in de voordeur is verankerd. In 2015 zijn onge-

veer 460 van dit soort inbraken gepleegd. Voor 75 van deze inbraken is vastgesteld dat ze zijn gepleegd door een en dezelfde dadergroep van twintig jongeren.
Een methode die ook vaker wordt gesignaleerd, is het meenemen van een kluis. Hoogstwaarschijnlijk gebeurt dat omdat kluizen steeds beter beveiligd zijn en ter plekke moeilijk te openen zijn.

De gestolen buit is grotendeels onveranderd. Sieraden, tafelzilver, horloges en geld zijn onverminderd populair. Wel is er in de afgelopen jaren een sterke toename in het aantal gestolen tablets geweest. Die toename is ongeveer even sterk als de afname in het aantal gestolen computers.
Solistische woninginbrekers proberen hun buit meestal direct via helers van de hand te doen; een klein deel is voor eigen gebruik (geld, elektronica). Mobiele buitenlandse bendes daarentegen slaan de buit vaak op. Al in het NDB2012 is deze buitafscherming geconstateerd. Uit recent onderzoek blijkt dat ze daarvoor tijdelijke begraafplekken in nabijgelegen bosjes of struiken gebruiken, of speciaal geprepareerde ruimten in auto's, woningen en loodsen. Eenmaal uit de opslag wordt een groot deel van de spullen en het geld verscheept naar familieleden en vrienden in het thuisland.

Corruptie lijkt niet veel toegepast te worden bij de uitvoering van woninginbraken. Het blijft beperkt tot incidenten, zoals recente gevallen waarbij een medewerker van een reisbureau en een medewerker van een verzekeringsmaatschappij behulpzaam waren bij het verstrekken van gegevens over slachtoffers en buit. Dadergroepen wenden zich ook tot gemakkelijk beïnvloedbare personen die, al dan niet tegen betaling, risicovolle klusjes willen uitvoeren of als katvanger willen fungeren.

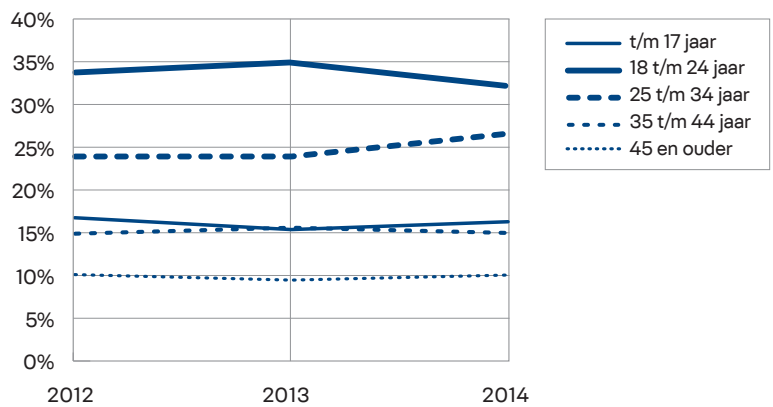
Er zijn enkele ontwikkelingen waaruit blijkt dat woninginbrekers profiteren van technologische vooruitgang om hun criminele praktijken te stroomlijnen. De belangrijkste is het gebruik van navigatiemogelijkheden van smartphones bij het lokaliseren van doelwitten en het plannen van aan- en wegrijdroutes. Onduidelijk is op welke schaal deze middelen worden gebruikt.
Er is geen bewijs gevonden voor het veronderstelde gebruik van informatie op Facebook, Twitter of andere sociale media bij het plannen of uitvoeren van woninginbraken. Sociale media worden wel gebruikt voor afscherming. Samenwerkende woninginbrekers bijvoorbeeld ontmoeten of spreken elkaar virtueel in plaats van fysiek. Voor opsporingsteams van de politie is het daardoor lastiger verdachtengroepen in kaart te brengen.

Er zijn geen aanwijzingen gevonden dat er bij een woninginbraak vaker geweld wordt gebruikt. Het aandeel inbraken met geweld is onveranderd 0,6 procent. Het gaat hier vermoedelijk om een ondergrens, omdat woninginbraken die *onbedoeld* uitmonden in het gebruik van geweld in de registraties kunnen zijn weggeschreven als woningovervallen. Woninginbraken die *bedoeld* uitmonden in het gebruik van geweld zijn feitelijk woningovervallen en worden meestal ook als zodanig geregistreerd.

Ouderen worden vaker het slachtoffer van de babbeltruc, een bijzondere variant op een woninginbraak. Vooral senioren van 85 jaar en ouder zijn hierbij het doelwit. Bij deze groep hebben daders, vergeleken met jongere doelwitten, een hogere buitverwachting en verwachten ze minder weerstand. Anders dan de laatste jaren nogal eens wordt beweerd, zijn ouderen niet vaker het slachtoffer van de 'reguliere' woninginbraken. Iets meer dan een kwart van de slachtoffers van woninginbraken is 65 jaar of ouder en dat is in overeenstemming met het aandeel ouderen in de bevolking. Voor deze reguliere woninginbraken geldt dus dat de woning en de buitverwachting de keuze voor een woninginbraak bepalen, niet de (leeftijd van de) bewoner.

In het vorige NDB werd gesteld dat woninginbrekers steeds jonger worden. De huidige cijfers (gebaseerd op het peiljaar 2014) zijn hiermee in tegenspraak. Zowel het aandeel minderjarige verdachten (t/m 17 jaar) als het aandeel jongvolwassen verdachten (18 t/m 24 jaar) is ten opzichte van 2012 langzaam afgenomen, zie figuur 7. Daarentegen groeit het aandeel verdachten in de leeftijd van 25 tot en met 34 jaar.

Figuur 7. Leeftijdsverdeling van de totale verdachtenpopulatie in de periode 2012-2014



Ondanks de daling in het aandeel jongere inbrekers blijft de groep jongvolwassenen de grootste groep geregistreerde woninginbrekers. Op een bevolkingsaandeel van 10 procent vertegenwoordigen zij 33 procent van de verdachtenpopulatie in 2014.

Het grootste deel van de ruim 6300 (in 2014) geregistreerde woninginbrekers heeft de Nederlandse nationaliteit. Daarna volgen de relatief kleine groepen Marokkanen, Polen, Roemenen, Turken, Litouwers en Bulgaren. Afgaand op hun bevolkingsaandeel zijn de niet-Nederlandse nationaliteiten oververtegenwoordigd in de verdachtenpopulatie. De oververtegenwoordiging is het sterkst voor verdachten met de Roemeense, Marokkaanse en Litouwse nationaliteit.

Tabel 16. Het aandeel van personen in de verdachtenpopulatie en de bevolking, naar nationaliteit

Nationaliteit verdachten	2014	Bevolkingsaandeel 2014
Nederland	82,1%	95,2%
Marokko	3,9%	0,3%
Polen	2,8%	0,5%
Roemenië	2,0%	0,1%
Turkije	0,8%	0,5%
Litouwen	0,7%	0,0%
Bulgarije	0,6%	0,1%

Sinds 2012 zijn er geen noemenswaardige verschuivingen zichtbaar in de verdeling van nationaliteiten over de geregistreerde verdachtenpopulatie.

Een groot deel van de hier besproken inbrekers betreft gelegenheidsinbrekers. De in het vorige dreigingsbeeld gesignaleerde trend van een afnemend aantal drugsverslaafde gelegenheidsinbrekers en een groeiend aantal gelegenheidsinbrekers verslaafd aan luxe heeft zich, volgens diverse respondenten, in de afgelopen jaren doorgezet.

Woninginbraken die in georganiseerd verband plaatsvinden, worden gepleegd door min of meer vaste dadergroepen, door mobiele bendes uit het buitenland en door dadergroepen die een wisselende samenstelling kennen waarbij de wisselende groepsleden allen uit eenzelfde netwerk afkomstig zijn. Vooral de laatstgenoemde groepen springen de laatste paar jaar in het oog. Het gaat om groepen waarvan de leden flexibel en mobiel zijn: ze opereren in verschillende groepjes en zijn zowel regionaal als landelijk actief. Ze houden zich niet alleen bezig met gewelddadige woninginbraken, maar plegen ook overvallen en straatroven. De groepsleden zijn relatief jong (12 tot en met 24 jaar) en relatief vaak van allochtone herkomst. Ze hebben lak aan het lokale gezag en zijn *streetwise.* Ze blijven uit handen van politie en justitie doordat ze goed op de hoogte zijn van gebruikte opsporingsmiddelen en strafrechtprocedures.

In het vorige dreigingsbeeld werd verwacht dat het aantal inbraken gepleegd door mobiele bendes uit Midden- en Oost-Europa zou gaan toenemen. Of dit is gebeurd, is niet duidelijk. Destijds werden deze groepen verantwoordelijk gehouden voor minimaal 14 procent van de opgeloste woning- en bedrijfsinbraken in Nederland. De laatste jaren zijn inbraakgolven opgemerkt waarbij mobiele bendes woninginbraken pleegden op zoek naar autosleutels van dure voor de deur geparkeerde auto's. Mobiele bendes verblijven tijdelijk op campings, op vakantieparken en in appartementen in grote steden.

3.2.3 Huidige gevolgen

De gevolgen van woninginbraak zijn hoofdzakelijk psychisch en financieel van aard. Soms is ook sprake van fysieke gevolgen, overlast en ondermijning.

Psychische gevolgen manifesteren zich vooral in emotionele schade. Het gaat om gevoelens van onveiligheid, angst en verdriet om verlies van (dierbare) bezittingen. Die klachten uiten zich bijvoorbeeld in onrustig slapen, chronische nervositeit of gespannenheid. Uit recent onderzoek blijkt dat 60 procent van de slachtoffers van een recente woninginbraak verwacht een maand tot een half jaar last te hebben van dit soort gevolgen. Bij gewelddadige woninginbraken, waarbij onbedoeld een confrontatie tussen bewoner(s) en inbreker(s) plaatsvindt, is de kans op psychische schade groter en kan de schade nog ernstiger zijn. Bij benadering werden er in 2015 ongeveer vierhonderd van dit soort woninginbraken gepleegd. Onbekend is hoe vaak deze gewelddadige inbraken leidden tot fysiek gewonden.

De financiële gevolgen bestaan overwegend uit het verlies van de gestolen goederen en de kosten van herstelwerkzaamheden aan of in de woning. Op basis van cijfers uit de wetenschap, van een verzekeraar en van de Stichting Nationale Inbraakpreventie Weken wordt de huidige financiële schade van woninginbraken geraamd op ongeveer 175 miljoen euro per jaar. Per inbraak is dat een schadepost van ongeveer 2700 euro per jaar. Als we ervan uitgaan dat 20 tot 30 procent van de geregistreerde woninginbraken door criminelen in georganiseerd verband wordt gepleegd, is minstens een vijfde van dit bedrag, 35 miljoen euro, het gevolg van georganiseerde woninginbraken.

Jongeren die zich met woninginbraken bezighouden, veroorzaken overlast in de lokale woongemeenschap. Volgens verschillende bronnen maken deze criminele jongeren zich schuldig aan mishandeling, intimidatie en bedreiging. In sommige buurten drukken criminelen die bovenlokaal actief zijn hun stempel op de lokale veiligheid. Als negatieve rolmodellen voeden ze de lokale criminaliteit. Hier ligt vervaging van normbesef op de loer.

3.2.4 Verwachtingen

Verwacht wordt dat het aantal woninginbraken voorlopig verder afneemt. De afname betreft vooral het aantal woninginbraken gepleegd door (gelegenheids)inbrekers die lokaal actief zijn. Dat kan voor een groot deel worden toegeschreven aan de effectieve aanpak van lokale veelplegers. Ook in de nabije toekomst zal die aanpak nog effect hebben, omdat lokale veelplegers een groot deel van de woninginbraken voor hun rekening nemen. Het aantal woninginbraken neemt ook af doordat burgers zelf meer preventieve maatregelen nemen, zoals het installeren van automatiseringsapparatuur waarmee huizen beter worden beveiligd. De gelegenheid voor inbraak neemt daardoor af.

Verwacht wordt dat de Nederlandse samenleving onverminderd last zal blijven houden van georganiseerde dadergroepen die woninginbraken plegen en dat de grip op de bovenregionaal functionerende groepen en netwerken niet verbetert. Dat heeft een aantal oorzaken.

De samenwerking tussen de politie-eenheden verloopt nog steeds vrij stroperig en het veiligheidsbeleid is sterk lokaal georiënteerd. De succesvolle persoonsgerichte aanpak van lokale veelplegers bijvoorbeeld wordt niet bovenregionaal toegepast, omdat politie-eenheden hun prioriteiten vooral in de eigen regio hebben. Dadergroepen die bovenregionaal of landelijk werken, profiteren van die vrije ruimte. Zij kunnen ongehinderd doorgaan met hun criminele activiteiten.
Ook de ZSM-afdoening door het Openbaar Ministerie (een in 2012 ingevoerd systeem om na aanhouding van een verdachte zo spoedig mogelijk over het afdoeningstraject te beslissen bij veelvoorkomende misdrijven) heeft als negatief bijeffect dat er op verdachten niet wordt doorgerechercheerd. Dat heeft als gevolg dat netwerken of criminele groepen daardoor nooit helemaal worden blootgelegd en dus ook niet worden aangepakt.
Uit opsporingsonderzoeken en gesprekken met politiefunctionarissen blijkt dat met name internationale dadergroepen Nederland een aantrekkelijk land vinden om woninginbraken te plegen. Zij 'roemen' de ZSM-afdoening en de lage strafmaat, zoals blijkt uit tapverslagen, omdat ze na aanhouding veelal binnen een dag weer buiten staan. Bovendien zijn de opbrengsten in Nederland hoog en is er een markt van vraag en aanbod waar gestolen waar relatief gemakkelijk te gelde kan worden gemaakt.
Deze ontwikkelingen leiden tot de verwachting dat de schade als gevolg van georganiseerde woninginbraken niet zal afnemen.

3.2.5 Kwalificatie van dreiging

In 2015 zijn in Nederland ongeveer 64.500 woninginbraken geregistreerd. Daarvan zijn er, als we afgaan op de meest recente schattingen, ten minste 12.500 gepleegd door georganiseerde criminele samenwerkingsverbanden.
Jaarlijks lopen duizenden slachtoffers van woninginbraken emotionele schade op door gevoelens van onveiligheid en door verdriet ten gevolge van verlies van dierbare bezittingen. Minstens vierhonderd mensen raken ieder jaar getraumatiseerd bij gewelddadige woninginbraken doordat zij een confrontatie met een of meer inbrekers hebben en daarbij in sommige gevallen ook fysiek letsel oplopen.
De financiële schadepost ten gevolge van woninginbraken is geschat op 175 miljoen euro. Daarvan wordt, naar schatting, ten minste 35 miljoen euro veroorzaakt door georganiseerde woninginbrekers.

In lijn met de huidige trend wordt de komende jaren weliswaar een verdere afname verwacht van het totale aantal woninginbraken, maar een groot deel van die afname komt voor rekening van lokale (gelegenheids)inbrekers. Het lokaal georiënteerde veiligheidsbeleid, de lokaal gerichte persoonsgerichte aanpak en de ZSM-afdoening zijn effectief bij lokale inbrekers maar veel minder bij georganiseerde, bovenregionale dadergroepen. Nederland blijft voor deze dadergroepen aantrekkelijk vanwege de gepercipieerde lage strafmaat, de hoge opbrengsten en de mogelijkheden om ook in Nederland gestolen waar af te zetten. Daarom verwachten we geen daling van het aantal woninginbraken dat door georganiseerde, bovenregionale dadergroepen wordt gepleegd. En daarmee zal ook de schade als gevolg van die

woninginbraken groot blijven. De financiële en emotionele gevolgen van bijkomend geweld en verlies van dierbare bezittingen zijn in hun totaliteit dusdanig ernstig dat woninginbraken ook de komende jaren een **dreiging** zijn voor de Nederlandse samenleving.

3.3 Bedrijfsinbraak

3.3.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Georganiseerde vermogenscriminaliteit. Nationaal dreigingsbeeld 2017.* Dat rapport is een verslag van onderzoek naar zes vormen van vermogenscriminaliteit, bedrijfsinbraak is er daar een van. De auteurs van het onderzoeksrapport zijn Jessica van Mantgem, Anne Mooij, Ewout Stoffers, Emilie Verschuuren, Debbie Mac Gillavry en Marsha de Bell, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf wordt de kwalificatie van dreiging beschreven. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is beargumenteerd en vastgesteld in een andere context door een groep van beoordelaars (de consensusgroep).

Volgens relevante wetsartikelen voor dit onderwerp is de definitie van bedrijfsinbraak: het door middel van braak wegnemen van geld en/of goederen uit bedrijven. Braak is het illegaal openbreken van een gebouw, in dit geval een bedrijf (winkel, sportcomplex, bank, hotel, school, ander bedrijfspand), om er binnen te gaan. Braak geldt als een strafverzwarende omstandigheid bij diefstal.

In deze paragraaf worden ramkraken op winkels en andere bedrijven ook onder bedrijfsinbraken geschaard omdat dit, ondanks de specifieke modus operandi, een vorm van bedrijfsinbraak is. De kraken op geldautomaten komen in de gelijknamige paragraaf in dit dreigingsbeeld aan bod.

3.3.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

Sinds het vorige dreigingsbeeld is het aantal bedrijfsinbraken met bijna een kwart afgenomen tot iets minder dan 36.000 inbraken in 2015 (zie tabel 17).

Tabel 17. Aantal geregistreerde bedrijfsinbraken naar jaar, pogingen en opgehelderde inbraken

	2012	2013	2014	2015
Aantal inbraken	46.583	44.418	39.157	35.795
Aantal pogingen	9.464	9.252	7.922	7.547
Aantal opgehelderd	5.712 (12,3%)	5.986 (13,5%)	5.243 (13,4%)	4.471 (12,5%)

Bron: BVI

Die afname is overeenkomstig de destijds geschetste verwachtingen. Het aantal pogingen tot inbraak is in de jaren 2012 tot 2015 eveneens afgenomen, maar procentueel ongeveer gelijk gebleven, rond de 20 procent van het totaal. Het ophelderingspercentage schommelt jaarlijks rond de 13 procent.

Niet iedereen doet aangifte of meldt een inbraak bij de politie. Uit een onderzoek uit 2014 van accountantskantoor PwC en de Vrije Universiteit van Amsterdam naar economische criminaliteit bij bedrijven blijkt dat er bij 'traditionele criminaliteit, gepleegd door een externe dader', in 50 procent van de gevallen bij de politie aangifte wordt gedaan en dat 22 procent gemeld wordt. Het werkelijke aantal bedrijfsinbraken zou op basis van dit onderzoek dan bijna 30 procent hoger zijn dan het geregistreerde aantal bedrijfsinbraken.

In alle branches nam het aantal bedrijfsinbraken de afgelopen periode af, bij banken en geld- en wisselkantoren is de daling het meest spectaculair. In deze branche daalde het aantal inbraken met bijna 60 procent. Behalve door de sterk verbeterde beveiliging komt dat mogelijk ook doordat steeds meer bankzaken online worden afgehandeld, er daardoor steeds minder bankfilialen en geld- en wisselkantoren zijn en deze ook steeds minder contant geld aanwezig hebben.

In 2012 was er sprake van een forse daling van het aantal ramkraken ten opzichte van 2011. In 2013 was er een lichte stijging zichtbaar, het aantal bleef wel onder het niveau van voor 2012. Of dit het begin is geweest van een nieuwe trend is niet bekend, omdat ramkraken sinds 2014 niet meer als zodanig worden geregistreerd in de politiesystemen.

Aard

De modi operandi die bij bedrijfsinbraken het meest voorkomen zijn, nog steeds, de *hit-and-run*-methode en de Bulgaarse methode. Bij hit-and-run worden de ramen ingegooid en bij de Bulgaarse methode wordt de cilinder van het slot afgebroken. Hierin is de laatste jaren niet veel veranderd. Soms wordt er wel sterker gereedschap gebruikt of volgen soortgelijke inbraakmethoden elkaar op als reactie op ontwikkelingen in beveiliging.

Er zijn wel enkele nieuwe ontwikkelingen met betrekking tot de branches waar bedrijfsinbraken worden gepleegd en de gestolen goederen die daarbij worden buitgemaakt. Zo worden groenvoorzieners, boerderijen, tuinders en loonwerkers steeds vaker slachtoffer van bedrijfsinbraak. De goederen die bij dit soort bedrijven gestolen worden, zijn landbouwvoertuigen, materialen, machines en brandstof. De laatste jaren zijn zonnepanelen bij zowel bedrijven als particulieren en bouwmaterialen en gereedschappen op bouwterreinen zeer gewild.
Uit onderzoek uit 2015 van de Land- en Tuinbouw Organisatie Nederland blijkt dat inbraken op het platteland steeds vaker voorkomen. Volgens Europol gebeurt dit niet alleen in Nederland, maar is het een Europese trend. Dadergroepen opereren internationaal en zijn

vaak afkomstig uit het buitenland. Ze zijn flexibel, mobiel en goedgeorganiseerd met een duidelijke taakverdeling, en ze stelen op bestelling.

Uit verschillende onderzoeken blijkt dat daders soms hulp krijgen van binnen een bedrijf door werknemers die informatie geven over beveiligingscamera's, alarminstallaties of de specifieke locatie van de buit. Dit is onveranderd sinds het vorige dreigingsbeeld.

Ook de kenmerken van de daderpopulatie zijn nog dezelfde. De daders zijn voornamelijk jonge mannen tussen de 16 en 25 jaar oud. Ze gaan vaak gezamenlijk te werk. Soms lijken deze daders structureler en in georganiseerd verband samen te werken, omdat er sprake is van soortgelijke modi operandi bij verschillende delicten. Dit speelt bijvoorbeeld bij de winkelinbraken in de Randstad, waarbij twee tot vier personen aankomen op een scooter, inbreken via de voorkant, de buit in tassen of dozen doen en deze vervolgens met scooter en al in een busje laden. Dit busje laten ze staan om te voorkomen dat ze opgemerkt worden nadat de inbraak gemeld is. In de dagen daarna wordt het busje opgehaald. Deze daders worden zelden aangehouden. Bedrijfsinbraken worden gepleegd door zowel gelegenheidsdaders als in een meer georganiseerd verband door mobiele bendes. Het is onbekend welk aandeel in georganiseerd verband wordt uitgevoerd. De data in de politiesystemen geven daar geen uitsluitsel over.

3.3.3 Huidige gevolgen

Bedrijfsinbraken zorgen vooral voor financiële schade en overlast voor de slachtoffers. Van fysiek letsel en psychische schade is volgens respondenten meestal geen sprake, omdat er bijna nooit medewerkers aanwezig zijn tijdens de inbraak.

De financiële schade bestaat niet alleen uit de waarde van de gestolen buit, maar ook uit de kosten voor reparatie van de aangerichte schade, onkosten voor het aanvullen van de gestolen goederen en gederfde inkomsten.
Volgens cijfers van het Verbond van Verzekeraars uit 2013 is de gemiddelde schade per claim 3400 euro en de totale schade van diefstal en inbraak bij bedrijven in dat jaar 70 miljoen euro. De schade heeft een grotere impact op kleine bedrijven dan op grote bedrijven.

3.3.4 Verwachtingen

Over het algemeen is de verwachting dat het aantal bedrijfsinbraken de komende jaren verder zal afnemen. De specifieke ontwikkelingen die hier invloed op hebben, liggen op het terrein van beveiliging en preventie, de prioriteitstelling bij de politie, de buitverwachting en meer algemene maatschappelijke ontwikkelingen ten aanzien van digitalisering en economie.

In tijden van economische crisis heeft beveiliging niet de hoogste prioriteit. Nu de economie weer aantrekt, wordt er ook weer meer geïnvesteerd in beveiligingsmaatregelen. Dat heeft naar verwachting een remmend effect op bedrijfsinbraken. Een belangrijke ontwikkeling is

de verbetering van het cameratoezicht. De kwaliteit van de beelden wordt steeds beter en door middel van *Live View* kunnen de beelden steeds vaker direct worden doorgestuurd van de meldkamer van een particuliere beveiligingsorganisatie naar de meldkamer van de politie. Hierdoor kan er sneller alarm geslagen worden en kan de pakkans toenemen. Dit heeft naar verwachting een remmend effect op het aantal bedrijfsinbraken.

Een andere ontwikkeling die van invloed kan zijn, heeft betrekking op de beoogde buit. In supermarkten en drogisterijen zijn de inbraken vaak gericht op sigaretten. Er bestaan echter plannen om sigaretten alleen nog via speciale winkels van de overheid te verkopen, om rookwaar zo minder breed verkrijgbaar te maken en de controle op de leeftijd van klanten te vergemakkelijken. Dit kan leiden tot een verplaatsing van het probleem. Behalve dat dergelijke overheidswinkels het doelwit kunnen worden van bedrijfsinbraak, kunnen inbrekers hun pijlen ook gaan richten op andere goederen en andere bedrijven.

Beveiligingsorganisaties en de politie profiteren steeds meer van geavanceerde digitale mogelijkheden om daders op te sporen, zoals slimme camera's, datamining en geavanceerde computermodellen. Een goed voorbeeld is het Criminaliteits Anticipatie Systeem (CAS) dat ontwikkeld is door de politie en de Vrije Universiteit van Amsterdam. Dit systeem geeft op een kaart aan in welke delen van de stad de komende periode naar verwachting veel bedrijfsinbraken zullen gaan plaatsvinden. Ook apps kunnen behulpzaam zijn bij bestrijding en preventie. Potentiële slachtoffers kunnen bijvoorbeeld gebruikmaken van de app Veilige Horeca, met een checklist en adviezen om de veiligheid te verbeteren. De digitalisering heeft mogelijk ook effect op de daders. Zij verplaatsen hun activiteiten wellicht van de reële wereld naar de virtuele wereld, omdat er online nieuwe mogelijkheden ontstaan die voor criminelen lucratief zijn.

Door een gebrek aan informatie over ramkraken in de afgelopen jaren is het eigenlijk onmogelijk om verwachtingen te formuleren. Ramkraken hebben minder prioriteit en sinds 2014 worden ramkraken niet meer apart (landelijk) geregistreerd. Welk effect dat de komende jaren zal hebben, is onbekend; remmend is het in ieder geval niet.

Op basis van de geformuleerde verwachtingen zullen de gevolgen van bedrijfsinbraken naar verwachting in 2021 van dezelfde orde zijn als de huidige gevolgen: vooral financiële schade en overlast voor de slachtoffers.

3.3.5 Kwalificatie van dreiging

De gevolgen van bedrijfsinbraken zijn vrijwel uitsluitend financieel van aard, naast enige overlast die wordt veroorzaakt door de bedrijfsinbraken. In het vorige dreigingsbeeld was de verwachting dat het aantal bedrijfsinbraken zou gaan dalen en die verwachting is uitgekomen. Voor de komende vier jaar wordt er weer een daling verwacht. Doordat het economisch beter gaat, kunnen bedrijven weer meer investeren in beveiligingsmaatregelen en kan de pakkans groter worden door meer en kwalitatief beter cameratoezicht. In 2013 bedroeg de

totale schade naar schatting 70 miljoen euro, deels veroorzaakt door gelegenheidsdaders en deels door georganiseerde criminelen. Het aantal bedrijfsinbraken is sinds 2013 met een kwart verminderd. Bij een verdere daling zal ook de schade verder afnemen. Hoewel het in totaal om tienduizenden bedrijfsinbraken per jaar gaat, is er in tegenstelling tot bij woninginbraken nauwelijks sprake van persoonlijk fysiek of psychisch letsel. Daarom vormen bedrijfsinbraken evenals vier jaar geleden de komende jaren **geen concrete dreiging** voor de Nederlandse samenleving.

3.4 Winkeldiefstal

3.4.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Georganiseerde vermogenscriminaliteit. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar zes vormen van vermogenscriminaliteit, winkeldiefstal is er daar een van. Dat onderzoek is voor dit dreigingsbeeld uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn Jessica van Mantgem, Anne Mooij, Ewout Stoffers, Emilie Verschuuren, Debbie Mac Gillavry en Marsha de Bell, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

3.4.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

In het NDB2012 zijn diverse manieren beschreven waarop (georganiseerde) winkeldiefstal plaatsvindt. Het gebruik van geprepareerde tassen en kleding behoort hiertoe en soms worden magneten gebruikt om veiligheidslabels te verwijderen. De georganiseerde vorm van winkeldiefstal wordt vrijwel altijd gekenmerkt door een strakke taakverdeling waarbij de werkwijze gebaseerd is op het afleiden van het winkelpersoneel. Er staat iemand op de uitkijk en soms is er sprake van een vluchtauto. De groepsleden die de diefstallen plegen, zijn opvallend goed voorbereid en schermen hun handelingen zo veel mogelijk af. Mogelijk dat dit bijdraagt aan het ontbreken van geweldgebruik door deze groepen. Het is een strategie om uit beeld van de politie te blijven. Bovendien is het gebruik van geweld niet nodig voor een succesvolle uitvoering. Wanneer zich geweld voordoet bij winkeldiefstal, betreft dit vooral gelegenheidsdaders die betrapt worden. De modus operandi is in de laatste jaren niet veranderd en zal volgens zegslieden ook niet snel veranderen, omdat de werkwijze voldoende lucratief is.

In de literatuur en in gesprekken met experts wordt georganiseerde winkeldiefstal voornamelijk in verband gebracht met internationaal georganiseerde dadergroepen. Over autochtone dadergroepen in Nederland is in dit onderzoek niets gevonden. In het NDB2012 werden

vier soorten internationaal actieve dadergroepen onderscheiden: hit-and-run-groepen, *subcultural based networks, foreign based networks* en sedentaire dadergroepen.

In vergelijking met het NDB2012 is in 2016 geen verandering geconstateerd in de betrokkenheid van soorten dadergroepen. Bij georganiseerde winkeldiefstal komt het grootste aandeel voor rekening van internationaal actieve groepen. Respondenten geven aan dat winkeldiefstallen waarbij internationaal actieve dadergroepen betrokken zijn, voor een belangrijk deel worden gepleegd door de tweede categorie dadergroepen, de subcultural based networks; deze dadergroepen sluiten zich aan bij (criminele) groepen in Nederland die hetzelfde thuisland hebben als zij. Dit strookt met bevindingen uit literatuuronderzoek en past in het beeld van de registraties over verdachten die geen vast adres in Nederland hebben. Ook uit opsporingsonderzoeken blijkt dat slechts een enkele verdachte in Nederland woont.
Het aandeel van subcultural based networks is niet uniek voor Nederland. In de hele Europese Unie gebruiken internationaal actieve dadergroepen *(diaspora)communities* om netwerken van contacten te creëren en voor logistieke ondersteuning. Tevens kan worden geconcludeerd dat mobiele dadergroepen de contacten in hun netwerken bewust bestendigen, vanuit winstbelang. Dadergroepen opereren steeds meer internationaal, op een netwerkachtige manier en zijn steeds meer dynamisch in hun contacten. De rol van helers in Nederland is daarbij interessant. Zij spelen soms niet alleen een rol bij de afzet van goederen, maar regelen ook verblijfplaatsen voor buitenlandse winkeldieven en zetten opdrachten bij hen uit, omdat zij weten waar vraag naar is.
In vergelijking met het NDB2012 zijn internationale dadergroepen nog steeds veelzijdig in hun activiteiten: afhankelijk van de politiële en justitiële aandacht verschuift de focus van criminaliteit.

Alles bij elkaar genomen hebben zich wat betreft de aard van het delict georganiseerde winkeldiefstal in de afgelopen vier jaar betrekkelijk weinig ontwikkelingen voorgedaan.

Omvang

Vooropgesteld moet worden dat het aangiftepercentage van winkeldiefstal dat wordt geschat op 9 procent, laag is. Er zijn globaal vier redenen om geen aangifte te doen: er is te weinig bewijs, de winkelier is onverzekerd, de schade is te gering en het vertrouwen dat er iets met de aangifte gebeurt is klein.
Sinds 2008 kent het totale aantal geregistreerde winkeldiefstallen een schommelend verloop. In de periode 2008-2011 nam het aantal met 10 procent toe. In de periode 2012-2015 nam het aantal met 5 procent af tot zo'n 40.000. Over de gehele periode (2008-2015) bezien is sprake van een gelijkblijvend aantal. Dit aantal is echter een ondergrens, omdat de aangiftebereidheid laag is.
Het aandeel van georganiseerde dadergroepen op het totale aantal winkeldiefstallen is niet eenduidig uit de registraties af te leiden. Die conclusie werd al getrokken in het NDB2012 en

is ook in dit onderzoek geldig. Respondenten vermoeden dat winkeldiefstal in verreweg de meeste gevallen wordt gepleegd door gelegenheidsdaders.

3.4.3 Huidige gevolgen

In het NDB2012 werd vermeld dat schattingen van de financiële schade door winkeldiefstal uiteenlopen. Zelfs het aangeven van een range waarbinnen de schade zich zou moeten bevinden, was lastig. Voor dit onderzoek is gebruikgemaakt van de bron die door de respondenten het meest werd aangehaald: de jaarlijkse *Global Retail Theft Barometer*. In deze internationale barometer winkeldiefstal werd de financiële schade in Nederland door winkeldiefstal voor 2013 geschat op 520 miljoen euro. Voor het NDB is het belangrijk te weten welk deel hiervan in georganiseerd verband wordt gepleegd. De meningen daarover lopen uiteen, hebben betrekking op verschillende perioden en onduidelijk is vaak waarop die meningen gebaseerd zijn. Er ligt in ieder geval nauwelijks onderzoek aan ten grondslag. Zonder precieze aantallen te noemen, wijt de brancheverenigingvoor winkeliers, Detailhandel Nederland, een groot deel van deze schade aan rondtrekkende bendes. In *Opportuun,* het huisblad van het Openbaar Ministerie, wordt naar aanleiding van één concrete zaak geschat dat (in 2009) de detailhandel 250 miljoen euro schade lijdt door rondtrekkende dadergroepen. Het gaat niet uitsluitend om winkeldiefstal, maar ook om bedrijfsinbraken, autodiefstal en plofkraken. Een respondent van het Centrum voor Criminaliteitspreventie en Veiligheid schat het huidige aandeel van gelegenheidsdaders bij winkeldiefstal op 80 procent en daarmee het aandeel georganiseerde daders op 20 procent. Omdat het steeds om schattingen gaat die niet altijd goed te vergelijken zijn, kunnen geen conclusies getrokken worden. Maar het lijkt erop dat het relatief kleine aantal winkeldiefstallen dat wordt gepleegd door internationaal actieve dadergroepen geassocieerd kan worden met een relatief groot deel van de financiële schade van dit delict.

Wanneer we de omzet van de detailhandel in Nederland als perspectief nemen, zien we een jaarlijkse omzet van ongeveer 100 miljard euro. Hoewel we de exacte schade door georganiseerde winkeldiefstal niet weten, kan veilig aangenomen worden dat het een fractie van de omzet is. Zonder de hinder die winkeliers ondervinden van winkeldiefstal te willen bagatelliseren, moet in aanmerking worden genomen dat de schade verdisconteerd wordt in de prijzen.

De gevolgen van winkeldiefstal zijn voornamelijk financieel. Er zijn weliswaar andere vormen van schade, zoals emotionele gevolgen voor winkelpersoneel, maar uit onderzoek blijkt dat de professionele winkeldieven de confrontatie met personeel mijden. Confrontaties (eventueel met geweld) vinden vooral plaats met gelegenheidsdieven. Dat neemt niet weg dat dit soort gevolgen kan leiden tot ziekteverzuim en daling van de arbeidsproductiviteit. Hoe omvangrijk deze gevolgen zijn, is onbekend.

3.4.4 Verwachtingen

De omvang van winkeldiefstal gepleegd door georganiseerde dadergroepen zal met de huidige aanpak gelijk blijven of zelfs toenemen. Ten eerste, omdat winkeldiefstal een winstgevend delict is met relatief weinig risico's: de pakkans is laag en bij aanhouding zijn de gevolgen voor de daders beperkt. Ten tweede, omdat de huidige lokaal georiënteerde aanpak en de relatief lage straffen in Nederland georganiseerde winkeldiefstal in de kaart spelen. Georganiseerde dadergroepen uit het buitenland houden bij het kiezen van hun doelland rekening met allerlei zaken, zoals strafklimaat, pakkans en beveiliging. Een derde argument voor de verwachting dat de omvang van winkeldiefstal door internationaal actieve dadergroepen minstens gelijk zal blijven of anders zal toenemen, is de waarschijnlijkheid van de bestendiging of zelfs de kans op groei van criminele netwerken in Nederland. Internationaal actieve dadergroepen hebben belang bij het efficiënt organiseren van de uitvoering van hun criminele activiteiten en het efficiënt vervoeren en afzetten van gestolen producten. Op dit moment is al te merken dat door internationaal actieve dadergroepen bewust wordt ingezet op het vergroten van het criminele netwerk in Nederland.
De modus operandi van georganiseerde winkeldiefstal zal niet opvallend veranderen. Net als bij inbraak en overige diefstal is dat niet nodig voor een succesvolle uitvoering.

Door een beter economisch klimaat (minder werkloosheid) in Nederland en meer investeringen in beveiligingsmaatregelen zal het aandeel van gelegenheidsdaders verminderen. Daardoor neemt de totale omvang van winkeldiefstal op korte termijn nog iets verder af. Conform het schommelende patroon dat de geregistreerde omvang al jarenlang heeft, wordt verwacht dat op de langere termijn de omvang weer zal toenemen.

Over de ernst en omvang van de gevolgen van georganiseerde winkeldiefstal in de komende periode kan geen uitspraak gedaan worden, er zijn te veel factoren waarvan te weinig bekend is.

3.4.5 Kwalificatie van dreiging

Verwacht wordt dat de komende jaren het totale aantal winkeldiefstallen verder zal afnemen. Die afname komt vooral voor rekening van gelegenheidsdieven. De economie trekt aan, de werkloosheid neemt af en bedrijven investeren weer meer in beveiligingsmaatregelen. Dit zal vooral effect hebben op gelegenheidsdieven. Het aantal winkeldiefstallen gepleegd door georganiseerde dadergroepen zal naar verwachting gelijk blijven of zelfs toenemen, afhankelijk van de groei van criminele netwerken van internationaal actieve dadergroepen.
Hoewel er relatief veel statistieken bekend zijn van winkeldiefstal, is het deel van de winkeldiefstallen dat in georganiseerd verband plaatsvindt onbekend. De meningen daarover lopen uiteen, hebben betrekking op verschillende perioden en onduidelijk is vaak waarop die meningen gebaseerd zijn. De informatie is in sommige gevallen met elkaar in strijd. Daardoor is de omvang van de bijbehorende financiële schade niet goed vast te stellen. Uit de beschikbare schattingen lijkt wel de conclusie aannemelijk dat het relatief kleine aantal

internationaal actieve dadergroepen verantwoordelijk is voor een relatief groot aandeel in de financiële schade.

Behalve tot financiële schade kan winkeldiefstal leiden tot ziekteverzuim en daling van de arbeidsproductiviteit. Hoe omvangrijk deze gevolgen zijn, is onbekend. Andere vormen van schade (ondermijning, geweldgebruik) zijn vrijwel afwezig.

Omdat er te weinig onderbouwing is voor een acceptabele schatting van de omvang en ernst van de te verwachten schade en eveneens voor het deel dat door georganiseerde dadergroepen wordt gepleegd, vormt georganiseerde winkeldiefstal voor de komende vier jaar een **witte vlek.**

3.5 Kraken op geldautomaten

3.5.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Georganiseerde vermogenscriminaliteit. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek dat in de eerste helft van 2016 is uitgevoerd voor dit dreigingsbeeld. De auteurs van het onderzoeksrapport zijn Jessica van Mantgem, Anne Mooij, Ewout Stoffers, Emilie Verschuuren, Debbie Mac Gillavry en Marsha de Bell, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017*.
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

In het NDB2012 werden de kraken op geldautomaten nog aangeduid als plofkraken en maakten onderdeel uit van de ramkraken. Door wijzigingen in de modi operandi dekt de term *plofkraken* niet meer helemaal de lading. Net als destijds doen zich plofkraken voor waarbij door middel van een explosief of gas een geldautomaat wordt vernield of opgeblazen. Maar sinds kort zijn er ook incidenten waarbij een kabel of band wordt gebruikt om de geldautomaat open of omver te trekken. Reden waarom hier is gekozen voor *kraken op geldautomaten.* Deze nieuwe term omvat zowel ramkraken als plofkraken op geldautomaten, maar ook andere werkwijzen zoals ‘trekkraken’. De ramkraken op andere doelwitten dan geldautomaten zijn voor dit dreigingsbeeld ondergebracht bij de bedrijfsinbraken.
Vanwege de gevaarzetting van de kraken op geldautomaten worden deze kraken gezien als een zwaarder delict dan een reguliere bedrijfsinbraak. De kraken op geldautomaten vallen onder de misdrijven waarbij opzettelijk brand wordt gesticht, een ontploffing teweeg wordt gebracht of een overstroming wordt veroorzaakt (artikel 157 Wetboek van Strafrecht).

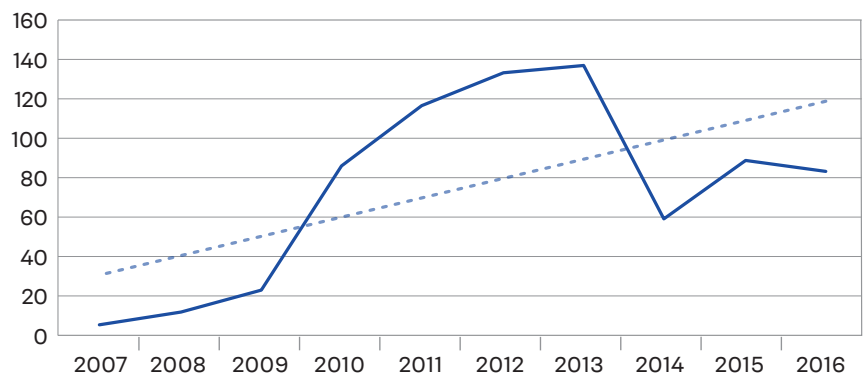
3.5.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

De toename van het aantal kraken op geldautomaten ten tijde van het vorige dreigingsbeeld heeft zich in 2012 en 2013 voortgezet (zie figuur 8). Na de 117 kraken in 2011 en 133 in 2012, bereikte het aantal kraken op geldautomaten een voorlopig hoogtepunt in 2013 met een aantal van 137. Daarna ligt het aantal op een beduidend lager niveau: 59 in 2014 en 89 in 2015. In de tweede helft van 2015 neemt het aantal kraken sterk af, terwijl het aantal kraken in Duitsland net over de grens met Nederland sterk toeneemt. In 2016 staat de teller op 83 kraken, ongeveer eenzelfde niveau als in 2015. Hoewel de trend over de jaren heen stijgend is, moeten we ook concluderen dat de aantallen een tamelijk grillig verloop hebben.

In de periode 2010-2012 zijn ongeveer drie van de tien kraken succesvol, dat wil zeggen dat er geld buitgemaakt is. In 2013 en 2014 neemt het slagingspercentage af, mogelijk als gevolg van maatregelen die de banken hebben genomen. In de eerste helft van 2015 stijgt niet alleen het aantal kraken, maar ook het slagingspercentage. Dit zou samenhangen met de nieuwe modus operandi van de 'trekkraak', die begin 2015 zijn intrede doet.

Figuur 8. Aantal kraken op geldautomaten in de periode 2007-2016, met trendlijn



Bron: Van Nobelen & Mesu (2012) en Database Informatievoorziening High Impact Crime en Mobiel banditisme

Aard

Waar voorheen butaan- of propaangas werd gebruikt, wordt sinds 2012 voornamelijk de combinatie zuurstof en acetyleen gebruikt. Daarnaast is er een toenemend gebruik van explosieven.

De keuze van het doelwit is niet willekeurig, maar hangt samen met het gemak waarmee een kluis te kraken is en toegang tot de kluisruimte kan worden verkregen, de geschiktheid van de locatie en de aanwezigheid van vluchtroutes. Sinds 2012 lijkt de keuze van het object sterk bepaald te worden door de beveiligingsmaatregelen die door de banken zijn getroffen. De banken met de minste beveiliging zijn het aantrekkelijkste doelwit. Wanneer de ene bank tot betere beveiliging van de automaten overgaat, zien we al snel dat automaten van andere banken uitgekozen worden.

Zo hebben we een verschuiving van Rabobank naar ABN AMRO en vervolgens naar ING gezien. Uiteindelijk werd naar Duitsland uitgeweken.
Met betrekking tot de locatie is er ook een duidelijke verschuiving te zien. In eerste instantie werden locaties gekozen in de landelijke gebieden dicht bij snelwegen, daarna locaties nabij provinciale wegen en tot slot begaven de daders zich richting de grote steden.
In 2015 heeft een opvallende verschuiving in de werkwijze plaatsgevonden. Tegelijk met de afname van de 'traditionele' ram- en plofkraken vond er een toename plaats van kraken op losstaande geldautomaten van de ING die veelal geplaatst zijn in een supermarkt van Albert Heijn. Nadat de pui is ingeramd met een voertuig, of is ingeslagen, wordt door de daders met een kabel of band, die aan een voertuig wordt bevestigd, de geldautomaat omver- of opengetrokken: de 'trekkraak'. Daarna wordt de kluis opengebroken en kunnen de daders bij de geldcassettes. Deze nieuwe modus operandi is volgens respondenten gemakkelijker en veiliger dan een traditionele kraak, omdat er geen specifieke kennis over gas en explosieven vereist is en krakers en omwonenden geen risico lopen door onoordeelkundige inzet van dergelijke stoffen.

Uit opsporingsinformatie blijkt dat er verschillende dadergroepen zijn die zich bezighouden met kraken op geldautomaten. De samenstelling van deze groepen is min of meer fluïde. De vaste harde kern komt terug, de schil eromheen is uitwisselbaar.
Er zijn vier van dergelijke groepen gevonden: één uit Amsterdam en omgeving, één uit Utrecht en omgeving en één uit het zuiden van het land. Naast deze drie groepen is er nog een atypische groep daders, afkomstig uit Noord-Holland. Bij de laatstgenoemde groep gaat het om personen van middelbare leeftijd met een Nederlandse achtergrond. Zij zijn gemiddeld ouder dan de meeste daders. Zij hebben daarnaast ook een afwijkende modus operandi: ze gebruiken wel gas, maar prepareren voertuigen met metalen rambalken, in tegenstelling tot de houten rambalken die door de andere dadergroepen worden gebruikt, ook spuiten ze de camera af met verf.

3.5.3 Huidige gevolgen

De kraken op geldautomaten hebben allereerst financiële gevolgen voor het bedrijfsleven. Daarnaast kunnen omwonenden en getuigen hinder en persoonlijke gevolgen ondervinden.

De financiële schade bij kraken op geldautomaten is aanzienlijk. Niet alleen kunnen de buitbedragen hoog oplopen, ook de materiële schade aan geldautomaten en panden is in veel gevallen groot, zeker bij het gebruik van explosieven. Hoe groot de totale schade exact is, weten we niet. Schattingen van respondenten wijzen op een jaarlijkse schade van enkele miljoenen euro's.

Omwonenden van een kraak op een geldautomaat ondervinden daarvan hinder en soms zijn de gevolgen voor personen ernstiger. Er zijn enkele gevallen bekend van bedreiging van getuigen met een vuurwapen. Bij sommige kraken is de schade aan de bovenliggende woning zo groot dat ontruiming noodzakelijk is. Verder ondervinden mensen hinder als hun

auto wordt gestolen en gebruikt bij een kraak. De aftocht na een kraak gebeurt doorgaans per voertuig met hoge snelheid. Dit zorgt voor gevaarlijke situaties op de openbare weg: recent kostte dit in Duitsland het leven van een medeweggebruiker.

3.5.4 Verwachtingen

Na het lage aantal kraken de afgelopen twee jaar, zal het aantal de komende jaren weer gaan toenemen. Dit wordt vooral veroorzaakt door de terugkeer naar Nederland van de krakers die nu in Duitsland actief zijn. Dit zal vermoedelijk pas gebeuren als men in Duitsland betere beveiligingsmaatregelen treft. De kans dat dit op korte termijn gebeurt, is niet zo groot.
Zoals gebleken is, laten krakers van geldautomaten zich sterk leiden door beveiligingsmaatregelen. Wanneer de banken hun beveiligingsmaatregelen opschroeven naar het niveau waarop ramkraken geen reële optie meer zijn, bestaat de kans dat de dadergroepen een andere modus operandi ontwikkelen of zich gaan toeleggen op andere vormen van criminaliteit. Zo is niet ondenkbaar dat de daders zich zullen gaan specialiseren in digitale aanvallen op geldautomaten, of zich gaan verdiepen in andere vormen van hightechcrime.

Ook in de toekomst zullen de gevolgen grotendeels financieel van aard zijn, de verwachting is immers dat deze daders of door zullen gaan met het kraken van geldautomaten, of op een andere (illegale) wijze aan hun geld zullen zien te komen. Indien er steeds zwaarder geschut wordt gebruikt, zal er een toename van materiële schade te zien zijn.

3.5.5 Kwalificatie van dreiging

Er is bij kraken op geldautomaten vooral sprake van financiële schade. Het gebruik van explosieven zorgt voor gevaarlijke situaties en kan leiden tot angstgevoelens bij omwonenden.
Na een aanvankelijke toename van het aantal kraken op geldautomaten in 2012 en 2013 is het aantal in 2015 afgenomen tot 89, en dat was in 2016 ook het geval. Een deel van de afname wordt verklaard doordat de daders zich verplaatst hebben naar Duitsland. Daar is in dezelfde jaren een duidelijke stijging te zien van het aantal kraken op geldautomaten, wat weer verklaard wordt door de toenemende beveiliging in Nederland. Verwacht wordt dat deze daders weer actiever worden in Nederland als de Duitse politie de aanpak intensiveert en Duitse banken maatregelen nemen.

De aantallen kraken van geldautomaten zijn momenteel niet zo hoog en de financiële schade bedraagt enkele miljoenen euro's. Ook bij enige toename in de komende jaren blijft de financiële schade en overlast door het kraken op geldautomaten beperkt, waardoor het de komende jaren **geen concrete dreiging** vormt voor de Nederlandse samenleving.

3.6 Overvallen

3.6.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Georganiseerde vermogenscriminaliteit, Nationaal dreigingsbeeld 2017.* Dat rapport is een verslag van onderzoek naar zes vormen van vermogenscriminaliteit, overvallen is er daar een van. De auteurs van het onderzoeksrapport zijn Jessica van Mantgem, Anne Mooij, Ewout Stoffers, Emilie Verschuuren, Debbie Mac Gillavry en Marsha de Bell, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf wordt de kwalificatie van dreiging beschreven. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is beargumenteerd en vastgesteld in een andere context door een groep van beoordelaars (de consensusgroep).

Bij een overval worden met (bedreiging met) geweld goederen ontvreemd. Een overval vindt plaats in een afgeschermde ruimte of op een waardetransport in de openbare ruimte. Dit onderscheidt een overval van een straatroof of een diefstal gevolgd door geweld.

3.6.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

In 2015 zijn er ruim zevenhonderd overvallen minder gepleegd dan in 2012 (zie tabel 18). Dat is een afname van 37 procent. Het laatste jaar stagneerde de daling. Opvallend is dat in hetzelfde jaar het aantal aangehouden verdachten fors lager uitviel.

Tabel 18. Overvallen en verdachten in de periode 2012-2015: absolute aantallen

	2012	2013	2014	2015
Aantal overvallen	1982	1633	1267	1239
Aantal verdachten	1815	1463	1236	957

Bron: DLIO, LORS-BVH/BVI

Sinds 2012 is het aantal overvallen op alle doelwitten (woningen, horeca en detailhandel) gedaald. De afname bij woningovervallen is het minst groot.

Aard

Er zijn de afgelopen jaren geen grote veranderingen geweest in de wijze waarop overvallen worden gepleegd. Overvallen worden relatief vaak gepleegd in de grote steden, veruit de meeste in Amsterdam en Rotterdam. Ook het donkeredageneffect is onverminderd actueel. In de wintermaanden worden meer overvallen gepleegd dan in de zomermaanden. Vermoedelijk schatten overvallers de pakkans in de wintermaanden lager in omdat het langer donker is. Er zijn minder mensen op straat en omdat het koud is, valt het ook minder op als er verhullende kleding wordt gedragen.

Bij overvallen is het lastig onderscheid te maken tussen georganiseerde en niet-georganiseerde criminaliteit, maar de meeste overvallen lijken geen georganiseerde criminaliteit. Bij een overval die door meerdere daders gepleegd wordt, betreft het lang niet altijd georganiseerde criminaliteit in de zin dat er op een structurele wijze wordt samengewerkt, het zijn eerder gelegenheidscoalities. Professionele, meer georganiseerde overvallers richten zich op objecten waarover zij weten dat er veel te halen is (geldtransporten, juweliers en bepaalde woningen). Ze zijn bereid verder te reizen. Ze bereiden de overval goed voor en maken gebruik van vermommingen, zware wapens, vluchtauto's en dergelijke.

Bij vermogenscriminaliteit – waaronder overvallen – is de laatste jaren een nieuw soort veelpleger gesignaleerd die afwijkt van het traditionele, veelal verslaafde type. Deze 'nieuwe' veelpleger opereert niet solistisch, maar werkt samen met anderen. Het zijn netwerken van jonge mannen die elkaar kennen en die in wisselende samenstelling vermogensmisdrijven plegen. Ze zijn relatief jong (12-24 jaar), relatief vaak van Marokkaanse of Antilliaanse herkomst en deinzen er niet voor terug geweld te gebruiken. Zij zijn goed op de hoogte van de politietactieken en -strategieën en weten zich goed af te schermen. Daarnaast opereren zij minder lokaal en overschrijden eenheidsgrenzen. Ze maken waarschijnlijk doelbewust gebruik van het gegeven dat de politie, ondanks de overgang naar een nationale politie, (nog steeds) minder goed in staat is om eenheidsgrensoverschrijdende dadergroepen aan te pakken.

3.6.3 Huidige gevolgen

Overvallen hebben gevolgen voor de gezondheid, omdat er een confrontatie plaatsvindt tussen daders en slachtoffers waarbij er sprake is van dreiging met geweld en soms ook daadwerkelijk van gebruik van geweld. Bij een op de vijf overvallen valt er een gewonde. Dat betekent dat er in 2015 bij de ruim 1200 overvallen zo'n 240 gewonden vielen. Jaarlijks overlijden er ook enkele slachtoffers als gevolg van een overval.

Behalve fysieke gevolgen lopen de slachtoffers ook het risico van psychische gevolgen. De mate waarin slachtoffers psychische schade ondervinden, is moeilijk vast te stellen. De impact is in veel gevallen groot, zeker als een overval in de woning van het slachtoffer plaatsvindt. Ook de omgeving van het slachtoffer kan emotionele schade ondervinden en de veiligheidsbeleving kan erdoor beïnvloed worden.

Een overval brengt ook financiële schade met zich mee, al is de omvang daarvan moeilijk te bepalen. De informatie over de buit wordt slecht geregistreerd. En bij gebrek aan betrouwbare gegevens over de buitgemaakte spullen is het lastig iets te zeggen over (ontwikkelingen in) de omvang van de financiële schade.

Overvallers ontwikkelen zich soms succesvol tot beroepscriminelen. Zij groeien op in probleemwijken en ontlenen enige status aan het criminele gedrag. In sommige (probleem)-wijken fungeren ze voor een aantal jongeren als criminele rolmodellen. Voor deze jongeren kan dat leiden tot een vervagend normbesef en de start van een criminele carrière.

3.6.4 Verwachtingen

In 2011 is het Actieprogramma Ketenaanpak Overvalcriminaliteit gestart en zijn er meerdere maatregelen genomen om overvallen aan te pakken. Een aantal van die initiatieven loopt de komende jaren nog door. Zo blijft de Taskforce Overvallen voorlopig bestaan en hebben diverse partijen onlangs een convenant getekend met het oog op samenwerking om het aantal overvallen op geld- en waardetransporten en geld- en waardedepots te verminderen. Deze initiatieven hebben de komende jaren mogelijk een remmende werking op het aantal overvallen.

Politie en justitie hebben de afgelopen jaren succesvol geïnvesteerd in de aanpak van overvallen, met een daling van het aantal overvallen als gevolg. Het ophelderingspercentage lag tot en met 2014 relatief hoog. Maar nu het aantal overvallen flink gedaald is, bestaat het risico dat de extra capaciteit weer aan andere prioriteiten zal worden toegewezen. De politie wordt momenteel geconfronteerd met andere grote problemen, zoals de vluchtelingenproblematiek en het terrorisme. Het is dan ook de vraag of de intensieve aanpak van de afgelopen tijd de komende jaren kan worden volgehouden. De hic-teams (highimpactcrime) en de overvallenteams zijn deels verdwenen of zijn minder groot dan voorheen. Als er minder overvallen opgelost worden, blijven er meer daders vrij rondlopen. Daders van overvallen houden het zelden bij één delict; de kans op meer overvallen neemt dan toe.

Woningen zijn in vergelijking met andere objecten gemiddeld genomen minder goed beveiligd en daardoor kwetsbaarder. Europol signaleert een toename van het aantal woningovervallen in Europa en waarschuwt tevens voor de toename van vermogenscriminaliteit tegen ouderen. Hoewel wij dat nu nog niet zien, is dat ook voor Nederland de komende jaren niet ondenkbaar. De bevolking vergrijst en door bezuinigingen in de zorg zullen ouderen langer zelfstandig blijven wonen.

De kwetsbaarheid van het doelwit zal een rol blijven spelen. Sommige doelwitten zijn nu eenmaal moeilijker te beveiligen dan andere doelwitten. Winkels en horecagelegenheden blijven relatief eenvoudig toegankelijk. En hoewel het elektronisch betalingsverkeer gestaag zal blijven toenemen, blijft daar ook de komende jaren contant geld voorhanden.

De meeste overvallen hebben geen relatie met georganiseerde criminaliteit, maar er zijn overvallers die wel meer georganiseerd overvallen plegen, zoals de eerder beschreven nieuwe veelplegers. Zij laten zich veel meer leiden door de buitverwachting en zullen zich minder snel laten afschrikken door beveiligingsmaatregelen dan gelegenheidsdaders. Deze nieuwe veelplegers zijn lastig aan te pakken en zullen de komende jaren onverminderd actief zijn.

De politie heeft moeite met eenheidsgrensoverschrijdende daders van vermogenscriminaliteit. Dezelfde moeite heeft de politie met buitenlandse criminele groeperingen die actief zijn in Nederland. Zo plegen Oost-Europese criminele samenwerkingsverbanden vermogenscriminaliteit in meerdere Europese landen. Ook in Nederland zijn zij actief, soms ook op het terrein van overvallen, en dat zullen zij de komende jaren blijven.

De ondergrens van het aantal overvallen dat jaarlijks gepleegd wordt, lijkt (bijna) bereikt. De verwachting is dat er de komende tijd een einde zal komen aan de jarenlange daling en dat het aantal overvallen dan weer iets zal gaan toenemen.

3.6.5 Kwalificatie van dreiging

In 2011 is het Actieprogramma Ketenaanpak Overvalcriminaliteit gestart en zijn er meerdere maatregelen genomen om het overvalprobleem aan te pakken. Die maatregelen hebben hun vruchten afgeworpen: het aantal overvallen is de afgelopen jaren gedaald. Ondanks die daling blijft de gezondheidsschade bij slachtoffers aanzienlijk. Bij de ruim 1200 overvallen in 2015 vielen er 240 gewonden en waren er enkele doden te betreuren. Ook de emotionele schade is aanzienlijk bij zowel de directe slachtoffers als bij omwonenden. Over de financiele gevolgen is weinig informatie voorhanden.
Volgens diverse experts lijkt de ondergrens bereikt en zal naar verwachting het aantal overvallen de komende jaren licht stijgen. Verwacht wordt dat de gezondheidsschade in 2021 minimaal gelijk is aan die in 2015. Over de financiële gevolgen worden geen verwachtingen uitgesproken. Hoewel het merendeel van de overvallen geen georganiseerde criminaliteit lijkt, is enkel de verwachte gezondheidsschade in 2021 dermate ernstig dat overvallen de komende vier jaar als een **dreiging** worden gezien voor de Nederlandse samenleving.

3.7 Ladingdiefstal

3.7.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Ladingdiefstal. Nationaal dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek dat in de eerste helft van 2016 is uitgevoerd voor dit dreigingsbeeld. De auteur van het onderzoeksrapport is Floris Korteweg, werkzaam bij de politie. De bronnen die hij bij zijn onderzoek heeft gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Onder ladingdiefstal verstaan we de diefstal van goederen die zich bevinden binnen de logistieke keten van verplaatsing van de ene locatie naar de andere. Locaties voor opslag (met uitzondering van de opslag bij de producent), overslag en distributie liggen binnen de logistieke keten. In het *Actieplan Transportcriminaliteit 2015-2016* is het domein verder ingeperkt tot de diefstallen vanaf parkeerplaatsen en bedrijventerreinen. Diefstallen van

lading uit bedrijven en van goederen uit logistieke centra worden volgens deze nadere domeinafbakening dus niet meegenomen. Verder gaat het bij ladingdiefstal om voertuigen van meer dan 3500 kilo.

3.7.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Het Team Vervoer en Transport (TVT) van de Landelijke Eenheid van de politie houdt sinds 2010 informatie bij over de aard en de omvang van de ladingdiefstallen die bij de politie bekend geworden zijn. Tabel 19 toont de ontwikkeling van het aantal ladingdiefstallen in Nederland. Hierbij zijn twee opmerkingen op hun plaats. De eerste is dat de cijfers betrekking hebben op het aantal ladingdiefstallen dat is gepleegd in Nederland en op de ladingdiefstallen in het buitenland die door een gedupeerde Nederlandse transporteur in Nederland zijn gemeld. De tweede opmerking betreft de vermelde aantallen: die vormen een ondergrens van het daadwerkelijke aantal ladingdiefstallen. Dit komt doordat transporteurs soms geen aangifte doen, bijvoorbeeld als de lading niet verzekerd is of als ze aangifte doen te tijdrovend vinden, bang zijn voor reputatieschade of van mening zijn dat de politie niets met de aangifte doet.

Tabel 19. Ladingdiefstal in de wegtransportsector 2011-2015, inclusief pogingen

	2011	2012	2013	2014	2015
Diefstal van alleen lading	768	287	430	381	303
Diefstal van voertuig met lading	61	60	37	46	45
Totaal	**829**	**347**	**467**	**427**	**348**

In 2011 was het aantal ladingdiefstallen het grootst. Aangenomen wordt dat de resultaten die in enkele grote opsporingsonderzoeken zijn geboekt en de inspanningen van de branche om ladingdiefstallen tegen te gaan, hebben geleid tot een afname in de jaren daarna.

Diefstal van alleen lading (inclusief pogingen) gaat in ruim de helft van de gevallen (53%) gepaard met zeilsnijden, zie tabel 20. Hierbij wordt in het zeil van zeilentrailers gesneden om te kijken of de lading de moeite waard is om te stelen; zeilentrailers zijn bij uitstek gevoelig voor ladingdiefstal. Toch wordt er nog steeds veel gebruikgemaakt van deze minder veilige manier van transport.

Tabel 20. Drie soorten van ladingdiefstal zonder voertuig in 2015

	Poging	Voltooid	Totaal
Ladingafgifte d.m.v. oplichting	0	5	**5**
Diefstal lading	42	95	**137**
Diefstal lading d.m.v. zeilsnijden	87	74	**161**
Totaal	**129**	**174**	**303**

Bij ladingafgifte door middel van oplichting doet men zich op online vrachtuitwisselingssystemen voor als legale transporteur om zodoende onder valse voorwendselen ladingen op te halen bij expediteurs. De verwachting ten tijde van het vorige dreigingsbeeld was dat oplichting via online vrachtuitwisselingssystemen zou gaan toenemen. Die verwachting is niet uitgekomen: het aantal gevallen van deze vorm van oplichting bedraagt slechts enkele per jaar.

Veel bedrijven in het beroepsgoederenvervoer bevinden zich in de zuidelijke regio's van Nederland en daar lopen ook de belangrijkste doorvoerroutes. Dit verklaart waarom de meeste ladingdiefstallen, net als in voorgaande perioden, in het zuiden van ons land plaatsvinden. Ook wat betreft de pleegplek is er maar weinig veranderd sinds het NDB2012: de meeste ladingdiefstallen vinden plaats op parkeerplaatsen. Wel vinden er recent wat meer incidenten plaats op de openbare weg, vermoedelijk vanwege een gebrek aan verzorgingsplaatsen en parkeergelegenheid voor vrachtwagens in de nachtelijke uren. Als buit kiest men net als ten tijde van het vorige dreigingsbeeld goederen met een hoge verkoopwaarde in het illegale circuit, zoals computerapparatuur, merkkleding, schoeisel, voeding en genotmiddelen.

Het lijkt erop dat ladingdieven goed op de hoogte zijn van de opsporingsmiddelen en methodieken die door de politie worden ingezet. Zelf maken ze van diverse vormen van afscherming gebruik. Zo worden er huurauto's ingezet, gestolen auto's, gestolen kentekenplaten, gps- en gsm-*jammers* en communiceren zij via werktelefoons of portofoons. Ook verleggen ladingdieven tijdelijk hun werkgebied na acties van de politie, bijvoorbeeld naar België of Duitsland. Nieuwe ontwikkelingen zijn volgens respondenten van het TVT het gebruik van Duitse huurauto's en het rijden via parallelwegen naar verzorgingsplaatsen. Zo vermijden ladingdieven kentekenregistratie bij het op- en afrijden van verzorgingsplaatsen langs de autosnelwegen.
Afgaand op de gegevens van het TVT en de interviews met politiefunctionarissen en belangrijke actoren uit de transportbranche, constateren we weinig nieuwe ontwikkelingen: werkwijzen, kenmerken van daders en verschijningsvormen van ladingdiefstal zijn sinds het vorige dreigingsbeeld grotendeels gelijk gebleven.

Een nieuwe werkwijze waarvan de laatste tijd melding wordt gemaakt, is ladingdiefstal uit een rijdende vrachtwagen gepleegd vanuit een rijdende auto. Goederen worden op locatie A geladen. Tijdens het vervoer van A naar B wordt er niet gestopt. Bij aankomst op locatie B zijn kostbare goederen ontvreemd. Buitenlandse groeperingen zouden zich met deze 'rijdende ladingdiefstallen' bezighouden. In Nederland zijn enkele meldingen van deze diefstallen gedaan. Tot op heden heeft onderzoek naar deze gevallen geen uitsluitsel kunnen geven over de ware toedracht. Vooralsnog is het onwaarschijnlijk dat hier sprake is van een nieuwe trend.

3.7.3 Huidige gevolgen

De financiële schade van ladingdiefstallen is onbekend. Politieregistraties bieden hier geen uitkomst. Bij aangiften of meldingen van ladingdiefstal wordt namelijk zelden een schadebedrag vermeld. Pogingen om verzekeraars melding te laten doen van claims van ladingdiefstallen hebben tot dusver onvoldoende respons opgeleverd: het Registratie Applicatiesysteem (RAP) bevat te weinig meldingen om daaruit conclusies te kunnen trekken over de omvang van de financiële schade.

Afgezien van de financiële schade veroorzaakt ladingdiefstal ook overlast aan de betrokken partijen. Niet alleen aan de betrokken chauffeur en transportonderneming, maar in bepaalde mate ook aan de opdrachtgever van het transport en de producenten en afnemers van de goederen.

Gebruik van geweld bij ladingdiefstal is uitzonderlijk. In 2014 was sprake van één incident en in 2015 van twee incidenten waarbij geweld gebruikt is tegen een chauffeur.

Het overgrote deel van de ladingdiefstallen is kleinschalig en kent een eenvoudige modus operandi. Interne betrokkenheid ontbreekt bij deze diefstallen en er is geen sprake van verweving van legale en illegale activiteiten. Daar staat een kleiner deel van de ladingdiefstallen tegenover dat wat complexer van uitvoering is en waarbij hulp van binnen de logistieke sector vereist is. Te denken valt aan oplichtingszaken waar de dadergroepen inlogcodes nodig hebben voor afgesloten sites of pincodes voor het ophalen van de lading. Ook wordt soms gebruikgemaakt van valsheid in geschrifte of worden bedrijven opgericht om een legale status te suggereren. Om dit soort oplichting goed uit te voeren is kennis van de logistieke sector vereist. Bij dergelijke ladingdiefstallen doet zich een bepaalde mate van verweving voor; deze gevallen zijn echter beperkt in aantal.

3.7.4 Verwachtingen

De belangrijkste factoren die van invloed zijn op de ontwikkeling van ladingdiefstal in de nabije toekomst, zijn volgens de geraadpleegde experts de invoering van beleidsmaatregelen in het kader van publiek-private samenwerking en het toenemende gebruik van digitale technologie.

De huidige publiek-private samenwerking staat omschreven in het Actieplan Transportcriminaliteit 2015-2016. Dit actieplan richt zich vooral op ladingdiefstal en liep tot eind 2016. Politie en justitie willen echter een bredere aanpak van transportcriminaliteit. Zo willen zij niet alleen aandacht voor criminaliteit waarvan de transportsector slachtoffer wordt, maar ook voor criminaliteit waarin de transportsector faciliteert: bijvoorbeeld bij het onder deklading vervoeren van drugs of bij mensensmokkel en mensenhandel. De politie wil een centraal loket inrichten met gespecialiseerde medewerkers die 24 uur per dag bereikbaar zijn om aangiften van transportcriminaliteit, waaronder ladingdiefstal, op te nemen. Verwacht wordt dat dit de aangiftebereidheid voor ladingdiefstal zal vergroten, waardoor er

in de toekomst een beter beeld ontstaat van de aard en omvang. De sector zal actief campagne (blijven) voeren om aangifte te stimuleren.
Er is onderzoek gepland dat moet uitwijzen hoe het gebruik van kastenwagens in plaats van zeilentrailers kan worden gestimuleerd, evenals het gebruik van beveiligde parkeerplaatsen. Tegelijkertijd streeft men naar uitbreiding van het aantal beveiligde parkeerplaatsen, certificering van parkeerplaatsen en betere bewegwijzering ernaartoe. Het is belangrijk dat de publiek-private samenwerking geborgd blijft, zodat dergelijke plannen gerealiseerd worden en kunnen bijdragen aan de bestrijding van ladingdiefstal.

De transportsector maakt in toenemende mate gebruik van digitale technologie. Hierdoor kan men lading beter beveiligen, bijvoorbeeld door het gebruik van referentienummers en barcodes om de personen te identificeren die de lading ophalen. Deze veranderingen bieden echter ook kansen voor criminelen als de digitale systemen niet goed zijn beveiligd of als er onvoldoende kennis bij bedrijven is voor het gebruik daarvan. Voorlichting over en bewustwording van de gevaren die kleven aan digitale toepassingen binnen de transportsector kunnen de branche weerbaarder maken tegen criminaliteit.
De Europese transportministers hebben de wens uitgesproken in 2019 zelfrijdende voertuigen te introduceren die moeten zorgen voor een veiliger, duurzamer en efficiënter vervoer. Afgezien van de haalbaarheid van de termijn van invoering, ontstaat hierdoor voor criminelen ook een nieuwe werkwijze voor ladingdiefstal: het hacken van zelfrijdende vrachtwagens.
De voortschrijdende techniek maakt het mogelijk om steeds kleinere en goedkopere zenders in de lading te verwerken. Ladingdieven maken daarom gebruik van *jammers* om de signalen van zenders te verstoren, zodat niet duidelijk is waar de goederen naartoe worden vervoerd. Door gebruik te maken van een passieve zender die slechts sporadisch een signaal uitzendt, kan detectie door criminelen worden voorkomen. Weer een andere technologische toepassing betreft het gebruik van 'slimme' camera's voor een betere beveiliging van terreinen.
De ontwikkelingen in de technologie bieden kansen voor een betere beveiliging en een beter zicht op de logistieke keten. Ook voor de aanpak en opsporing van ladingdiefstal bieden technologische ontwikkelingen mogelijkheden. Daar staat tegenover dat als de sector niet goed weet om te gaan met de nieuwe technieken er juist kansen ontstaan voor criminelen.

3.7.5 Kwalificatie van dreiging

De afgelopen jaren is het aantal geregistreerde incidenten van ladingdiefstal meer dan gehalveerd van 829 in 2011 tot 348 in 2015. Een goede publiek-private samenwerking heeft hieraan bijgedragen en deze samenwerking zal de komende jaren mogelijk zorgen voor een verdere daling van het aantal ladingdiefstallen. Technologische ontwikkelingen bieden mogelijkheden voor een betere beveiliging die eveneens kunnen leiden tot een daling van het aantal ladingdiefstallen.
De maatschappelijke gevolgen van ladingdiefstal zijn vooral financieel van aard, al is onbekend om welk bedrag het gaat. De overige gevolgen zijn minder ernstig te noemen. Er is geen of slechts in geringe mate sprake van ondermijning en tot een confrontatie tussen

chauffeur en ladingdieven komt het maar zelden. Wel is er nogal eens interne betrokkenheid vanuit bedrijven bij ladingdiefstal. Dan gaat het vaak om werknemers die nuttige informatie verstrekken over de *whereabouts* van de lading.

De afgelopen vier jaar is het aantal ladingdiefstallen flink verminderd. De komende jaren worden er geen ontwikkelingen verwacht die de afnemende trend zouden kunnen doen keren. Hoewel de huidige en de te verwachten financiële schade voor de Nederlandse samenleving onbekend zijn, bestaat vanwege de afnemende trend de verwachting dat de gevolgen van ladingdiefstal de komende jaren minder ernstig zullen zijn. Ladingdiefstal vormt daarmee **geen concrete dreiging.**

3.8 Afpersing

3.8.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Afpersing in Nederland. Themarapportage in het kader van het Nationaal dreigingsbeeld georganiseerde criminaliteit 2017.* Dit rapport bevat het verslag van een onderzoek dat voor dit dreigingsbeeld is uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrapport zijn werkzaam bij de Landelijke Eenheid en de Eenheid Oost-Nederland van de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Afpersing is een bijzondere vorm van diefstal met geweld en/of bedreiging. Het onderscheid bestaat erin dat de dader van dit misdrijf het geld of de goederen niet wegneemt maar *doet afgeven,* als gevolg van geweld of de dreiging daarmee. In sommige gevallen betreft de afpersing geen geld of goederen, maar gaat het om de (professionele) diensten die een slachtoffer kan leveren. Het geweld of de dreiging daarmee is niet kortdurend, maar houdt minstens een week aan.

Vormen van afpersing die inherent zijn aan een andere criminele activiteit worden niet beschreven in deze rapportage. Bij mensenhandel worden slachtoffers vrijwel altijd afgeperst. Voor zover dat binnen de seksindustrie gebeurt, wordt dit beschreven in de paragraaf over seksuele uitbuiting. Het gedwongen afsluiten van telefoonabonnementen wordt beschreven in de paragraaf over arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening, en in het hoofdstuk over fraude en witwassen. *Ransomware,* een digitale vorm van afpersing waarbij bestanden op de computer worden vergrendeld, wordt behandeld in het hoofdstuk over cybercrime.

3.8.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

In deze rapportage worden twee hoofdvormen van afpersing onderscheiden: afpersing in het bedrijfsleven en persoonsgerichte afpersing. Binnen deze categorieën kennen we de protectieafpersing, afpersing na een zakelijk conflict, faciliteringsafpersing, culturele afpersing, gelegenheidsafpersing en afpersing in het criminele milieu. De laatste twee vormen zijn persoonsgericht.

Bij *protectieafpersing* wordt in een rechtstreeks contact aan ondernemers 'gevraagd' beschermgeld te betalen. Het kan gaan om bescherming tegen onbekende kwaadwillenden, maar vaak gaat het om bescherming tegen de afpersers zelf. Meestal willen de afpersers contant betaald worden, maar soms willen zij de onderneming of een belang erin in bezit krijgen of portiersdiensten leveren. Uit verschillende bronnen worden al langere tijd signalen ontvangen over dergelijke praktijken. De afpersers hebben een gewelddadig imago en lijken niet terug te deinzen voor (extreem) geweld. Slachtoffers zijn bang en geïntimideerd, waardoor aangiften veelal ontbreken. Er is een toename in de berichtgeving over veronderstelde afpersing van horeca-eigenaren door leden van *outlaw motorcycle gangs* (OMG's). De betrokkenheid van OMG's bij afpersing is niet nieuw, Europol stelt dat protectieafpersing een bekende criminele activiteit is waar OMG's in Europa zich vaak aan schuldig maken. Ook de Nederlandse politie beschrijft dat (leden van) OMG's betrokken zijn bij protectieafpersingen. Uit de verschillende politiesystemen zijn voor de periode 2012-2015 meer dan honderd mogelijke gevallen gevonden van OMG-gerelateerde afpersingen. In geval van protectieafpersingen lijkt het te gaan om seriematige afpersingen in georganiseerd verband.

Een deel van de *afpersingen na een zakelijk conflict* is incidenteel en komt min of meer bij toeval tot stand. Zo zijn er gevallen bekend waarin schuldeisers niet tevreden zijn met een rechterlijke uitspraak en alsnog hun gelijk willen halen door met geweld te dreigen. In een aantal gevallen hebben de afpersers visitekaartjes getoond van incassobureaus. De namen van deze bureaus kunnen soms aan OMG's worden gerelateerd. In sommige gevallen wordt een zakelijk conflict gecreëerd, bijvoorbeeld bij antiek- en kunsthandelaars. De afpersers doorlopen een aantal stappen alvorens de afpersing begint. De relatie start zakelijk en wordt gaandeweg vriendschappelijker; de organisator van de afpersing geeft het slachtoffer 'spontaan' een cadeau. Enige tijd later koopt hij bij het slachtoffer een kunstwerk. Het slachtoffer kan daarbij onder druk worden gezet om een niet te hoge prijs te vragen. De afpersing begint op het moment dat de dader aangeeft ontevreden te zijn over de aankoop en zijn geld direct terug wil hebben (juridisch is er dan sprake van afpersing). Zo zijn er diverse varianten van zakelijke conflicten die uitlopen op afpersing.

Bij *faciliteringsafpersing* is geld niet de belangrijkste drijfveer, maar de diensten die de facilitator (notaris, advocaat, accountant) te bieden heeft. Bepaalde goederen en rechtspersonen kunnen bijvoorbeeld alleen van eigenaar wisselen als daar een notaris bij betrokken is.

Notarissen en advocaten kunnen verwijtbaar betrokken zijn bij criminele activiteiten, maar zij kunnen ook afgeperst worden. Uit verschillende bronnen blijkt dat faciliteringsafpersing voorkomt, maar de aard en omvang ervan is lastig vast te stellen door het gebrek aan concrete cijfers en voorbeelden.

Binnen etnische gemeenschappen in Nederland zou sprake zijn van *culturele afpersing.* Etnische minderheden zijn kwetsbaarder dan autochtonen, omdat zij vaak familieleden in het land van oorsprong hebben. In dat geval hoeft de afperser niet eens te dreigen met geweld; vaak volstaat een vage verwijzing naar kinderen, partner of moeder in het buitenland. Voorbeelden daarvan zien we in de Chinese en de Afghaanse gemeenschappen. In paragraaf 3.10 over heling is sprake van Afghaanse markthandelaars die gedwongen worden om gestolen goederen af te nemen van Afghaanse helers. De afpersers maken gebruik van de afschrikwekkende reputatie die ze opbouwden tijdens de oorlog in hun moederland. Ook wordt melding gemaakt van afpersing binnen de Turkse en Ethiopische gemeenschappen. Door de aanzwellende stroom migranten vormen zich meerdere etnische groepen. Door verschillende omstandigheden kunnen zij slachtoffer worden van culturele afpersing, vooral als zij hier illegaal verblijven. Doordat de gemeenschappen over het algemeen gesloten zijn, is er weinig over bekend.

Ten slotte bespreken we twee vormen van persoonsgerichte afpersing: gelegenheidsafpersing en afpersing in het criminele milieu.
Bij *persoonsgerichte afpersingen* zijn verschillende voorbeelden bekend waarin afpersers gebruik hebben gemaakt van een gelegenheid om iemand af te persen. Deze kan gecreëerd zijn of zich toevallig voordoen. Gecreëerde gelegenheden zijn soms geraffineerd opgezet, waarbij iemand langzaam maar zeker in de val wordt gelokt. Dit is vergelijkbaar met de variant bij bedrijfsafpersingen waarin een zakelijk conflict wordt gecreëerd. De gelegenheid is vaak leidend bij dergelijke afpersingen, daders zijn dan ook op zoek naar een eenvoudig doelwit of slachtoffer. Het gaat om allerlei vormen van afpersing die gemeenschappelijk hebben dat één persoon slachtoffer is. Zo kan worden gedreigd met het publiceren van compromitterende foto's of het bekendmaken van prostitutiebezoek of seksuele contacten met een minderjarige. Ook *sextortion* behoort tot deze vorm van afpersing.

Ten aanzien van *afpersingen in het criminele milieu* is in het vorige dreigingsbeeld al vastgesteld dat diverse OMG-leden zich daar structureel aan schuldig maken. Dit gegeven wordt in dit dreigingsbeeld bevestigd: OMG-leden persen andere (kleinere) criminelen af, bijvoorbeeld in de hennepwereld. Ook persen zij oud-leden af. Er zijn aanwijzingen dat het hier gaat om een bewuste strategie; kwetsbare personen worden gerekruteerd of melden zich vrijwillig en worden op een goede dag met een *bad standing* uit de club gezet, met alle nadelige financiële gevolgen van dien voor de betrokkene. Naast de manifeste rol van dit type afpersingen, is er fragmentarisch zicht op de 'klassieke' penoze die zich toelegt op afpersing van hun collega's, waar een ('afpersings)recht' van de sterkste geldt.

Voor een aantal criminele groepen vormt afpersing een belangrijke bron van inkomsten. Bij die groepen gaat het dan vooral om protectieafpersing en gecreëerde zakelijke conflicten. Er zijn sterke aanwijzingen dat de betrokkenheid van OMG's bij bedrijfsafpersingen in de afgelopen jaren is gegroeid. Ze houden zich soms ook bezig met het uitvoeren van illegale incasso's. Mocht een andere afpersingsgelegenheid zich voordoen, dan benutten deze groepen die in de regel ook.
De geregistreerde signalen over afpersingen door OMG's hebben telkens betrekking op (leden van) radicale OMG's. In de literatuur wordt een onderscheid gemaakt tussen conservatieve en radicale OMG's. Conservatieve leden richten zich primair op broederschap, 'het vrije leven' en motorrijden. Voor de radicale bikers staat het (criminele) gewin voorop. Voor sommige radicale chapters in Nederland vormt afpersing het dominante verdienmodel. Zij maken gebruik van de angst die bij veel mensen voor OMG's bestaat.
Persoonsgerichte afpersingen die *face to face* worden uitgevoerd zijn vaak het werk van criminele groeperingen. Vooral de anonieme persoonsgerichte afpersingen zijn het werk van eenlingen, al doen deze zich vaak voor als lid van een grotere groep.

Omvang

Over de omvang van afpersing in Nederland is weinig bekend. Om voor de hand liggende redenen wordt slechts zelden aangifte gedaan. Dit resulteert in een omvangrijk dark number. Wat we weten is fragmentarisch van aard en moeilijk te interpreteren vanwege het ontbreken van een historische context of een eenduidige registratie. Het ene onderzoek vermeldt dat er jaarlijks 55 aangiften van bedrijfsafpersing worden gedaan, een ander onderzoek heeft het over 1450 aangiften van afpersing in 2014, terwijl in 2007 670 keer aangifte zou zijn gedaan. De stijging heeft waarschijnlijk te maken met gijzeling van computers met ransomware en sextortion. Diverse slachtofferenquêtes geven percentages van slachtofferschap van bedrijven die variëren van 0,14 tot 10 procent. Een zoekvraag in het politiebestand BlueSpot Monitor over de periode 2012-2015 levert, afhankelijk van de filters, aantallen op die variëren van 1810 tot 8320 meldingen. De meeste van deze meldingen hadden betrekking op sextortion en het gedwongen afsluiten van telefoonabonnementen. Het is kortom een moeilijk te ontwarren brij aan cijfers, die op vele verschillende manieren en over verschillende perioden zijn verzameld en waaruit geen betrouwbare schatting van de omvang kan worden gedestilleerd.

3.8.3 Huidige gevolgen

Door het ontbreken van cijfers over de omvang is het ondoenlijk om de ernst van de gevolgen in te schatten. Wel kan een aantal mogelijke gevolgen beschreven worden.
In de eerste plaats zijn er individuele fysieke, psychische en financiële gevolgen voor de slachtoffers van afpersing. Het is onbekend in hoeveel gevallen deze schade zich voordoet. Ook zonder betrouwbare schatting van de ernst van afpersing kan geconcludeerd worden dat er een zekere mate van ondermijning van de rechtsorde en rechtspleging bestaat. Groepen die zich structureel bezighouden met afpersing, en dan vooral met protectie-

afpersing, kunnen als alternatieve overheid functioneren. Zij nemen dan twee traditionele overheidstaken over: het geweldsmonopolie en het recht op belastingheffing.
In een aantal steden of regio's zijn er groepen die zich onaantastbaar gedragen of hebben gedragen. Deze groepen hebben zich onder meer schuldig gemaakt aan bedrijfsafpersing of culturele afpersing. Afpersing vormt vaak een onderdeel van een breder criminaliteitsprobleem, waar andere vormen van georganiseerde en ernstige criminaliteit, fraude en vermenging van onder- en bovenwereld, een rol kunnen spelen. Het ultieme risico bestaat dat er illegale economieën en zogenoemde (etnische) monoculturen ontstaan waar de politie en andere opsporingsdiensten nauwelijks een informatiepositie meer hebben.

3.8.4 Verwachtingen

Er zijn weinig aanknopingspunten waarop verwachtingen over aard, omvang en ernst kunnen worden gebaseerd. Er is geen onderzoek dat eenduidige relaties legt tussen afpersing en allerlei criminaliteitsrelevante factoren, zoals economische omstandigheden of technologische ontwikkelingen. Een factor van belang kan zijn dat conflicten in het buitenland hun invloed zullen doen gelden in Nederland. De recent opgelaaide strijd tussen de Turkse overheid en de Koerdische PKK maakt dat Koerdische strijders en pro-Turkse strijders geld nodig hebben. Het is niet uitgesloten dat daardoor het aantal afpersingen in Nederland toe zal nemen. Zijdelings hieraan gerelateerd is de migrantenstroom. Zoals eerder werd opgemerkt, vormen in het bijzonder de illegale migranten een kwetsbare groep. De verwachting is dat binnen deze groep het aantal afpersingen zal toenemen. Zo zijn tientallen immigranten telefonisch benaderd door iemand die zich uitgaf als medewerker van de Immigratie- en Naturalisatiedienst (IND). Hij gaf aan dat er problemen waren met de verblijfsvergunning en dat er betaald moest worden. Als er niet betaald zou worden, dan zou het slachtoffer uit Nederland verwijderd worden.

De verwachting dat zich gevolgen zullen voordoen op het individuele fysieke, psychische en financiële vlak is gerechtvaardigd, evenals de verwachting over gevolgen voor de rechtsorde en rechtspleging. Voor het overige tasten we goeddeels in het duister.

3.8.5 Kwalificatie van dreiging

Het delict afpersing is met onzekerheden omgeven. Onbekend is wat de omvang en de ernst ervan zijn. Ook zijn er weinig aanknopingspunten om plausibele verwachtingen uit te spreken. Voor zover dat met grote voorzichtigheid wel gebeurt, loopt de richting van de verwachtingen verschillende kanten op. Daarom krijgt afpersing de kwalificatie **witte vlek.**

3.9 Georganiseerde autocriminaliteit

3.9.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Georganiseerde autocriminaliteit. Deelproject voor het Nationaal dreigingsbeeld 2017.* De auteurs van het onderzoeksrapport zijn Susan Wubbels en Dirk in 't Hout, beiden werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf wordt de kwalificatie van dreiging beschreven. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is beargumenteerd en vastgesteld in een andere context door een groep van beoordelaars (de consensusgroep).

Georganiseerde autocriminaliteit bestaat – binnen de context van het NDB – uit diefstal van auto's en diefstal van auto-onderdelen. Gestolen auto's kunnen in hun geheel verkocht worden, volledig gestript worden voor de onderdelen of worden gebruikt bij andere criminele activiteiten zoals ramkraken en liquidaties.

3.9.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Omvang

De afgelopen jaren is het aantal gestolen auto's gedaald van 11.396 in 2012 tot 10.091 in 2015. Deze daling wordt verklaard doordat er minder auto's van drie jaar of jonger zijn gestolen. De diefstal van auto's van vier tot acht jaar oud is daarentegen juist iets gestegen. De Stichting Aanpak Voertuig Criminaliteit en de Stichting VbV (Verzekeringsbureau Voertuigcriminaliteit) denken dat deze verschuiving komt door nieuwe eisen en verbeterde beveiliging van de nieuwste modellen auto's per 1 januari 2015.

De laatste jaren worden er steeds minder gestolen auto's teruggevonden. In 2015 is van alle gestolen auto's 37 procent teruggevonden. Van de jonge auto's (≤ 3 jaar) is slechts 27 procent teruggevonden. Het terugvindpercentage zegt mogelijk iets over de professionaliteit van de autodief. Een daling van het percentage kan het gevolg zijn van verdere professionalisering van deze criminele sector. Jonge auto's zijn een aantrekkelijk doelwit voor professionele autodieven. Voor zowel gestolen jonge auto's als gestolen oudere auto's geldt dat wanneer ze volledig gestript zijn voor de onderdelen ze ook niet meer teruggevonden worden.

Volgens experts wordt bijna de helft van de in Nederland gestolen auto's gestript voor de onderdelen, zo'n 40 procent van de gestolen auto's verdwijnt naar het buitenland en 10 procent wordt in Nederland verkocht. Met de verkoop van gestolen auto's en auto-onderdelen houden zich, onder andere, malafide garagebedrijven bezig die in een netwerk van autohandelaars hun waar afzetten.

Aard

Er wordt steeds meer digitale technologie gebruikt in auto's. Het gaat onder meer om technologie die de auto verbindt met de buitenwereld. De auto heeft bijvoorbeeld een internetverbinding met de fabrikant of de dealer waardoor storingen tijdig gesignaleerd worden of er een melding komt wanneer de auto onderhoud nodig heeft. Ook biedt de digitale technologie mogelijkheden voor geïntegreerde diensten zoals *keyless entry* en de bediening van de auto met een smartphone. De zwakke schakels bij deze ontwikkelingen zijn de informatiebeveiliging en de beveiliging van de internetverbinding. Zo is het hackers gelukt om toegang te krijgen tot een Tesla en een type Chrysler, waarna het motormanagement kon worden beïnvloed en de remmen volledig konden worden uitgeschakeld. Als de beveiliging niet op orde is, kunnen criminelen de auto openen, starten en ermee wegrijden. Daarnaast geeft het criminelen ook nieuwe mogelijkheden, zoals het afpersen van de fabrikant of de eigenaar van de auto door te dreigen met ongelukken.

Door het toegenomen gebruik van digitale technologie vergt het stelen van auto's steeds vaker elektronische en digitale manipulatie en daarvoor is specialistische kennis nodig. Dit heeft geleid tot een steeds verdere professionalisering van autodiefstal en de organisatiegraad die daarmee gemoeid is. Sommige criminele groeperingen kopen bij het verschijnen van een nieuw type auto een exemplaar dat zij volledig uit elkaar halen om uit te zoeken hoe de auto het beste gestolen kan worden. Deze kennis wordt doorverkocht aan andere groeperingen. Dat beperkt zich niet tot Nederland. Zo zijn er Nederlandse autodieven die apparatuur kopen bij een bedrijf in Beiroet dat zich gespecialiseerd heeft in de ontwikkeling van apparatuur om nieuwe auto's open te maken.

Nederland fungeert ook nog steeds als transitland en bestemmingsland van gestolen voertuigen uit nabijgelegen landen. De gestolen auto's worden in Nederland omgekat en vervolgens doorverkocht naar andere landen. Afrika, het Midden-Oosten en Oost-Europa zijn populaire bestemmingen voor gestolen auto's en gestolen auto-onderdelen. Een deel van de in het buitenland gestolen auto's wordt in Nederland bij malafide autobedrijven verkocht en bij demontagebedrijven gestript voor de onderdelen. Internet speelt een groeiende rol bij de afzet van deze auto-onderdelen. Het aanbod op internet is de afgelopen jaren flink gestegen.

De Nederlandse wereld van autocriminaliteit bestaat uit een bont gezelschap van daders. Dit is niet verwonderlijk gezien het internationale speelveld van autocriminaliteit. Als het gaat om gestolen auto's en gestolen onderdelen voor de binnenlandse markt, is de daderpopulatie overwegend Nederlands van samenstelling. Wanneer het gaat om import of export van gestolen auto's en gestolen onderdelen, komen er meerdere spelers in beeld en zijn allerhande etnische samenstellingen van dadergroepen mogelijk. Overigens speelt etniciteit een beperktere rol bij de samenstelling van de dadergroepen dan voorheen vaak werd aangenomen. Nagenoeg alle dadergroepen en andere betrokken partijen wisselen regelmatig van samenstelling.

3.9.3 Huidige gevolgen

In 2014 is de directe financiële schade van jonge auto's alleen al 96 miljoen euro. Daar komt nog de schade van oudere auto's bij. De Stichting Verzekeringsbureau Voertuigcriminaliteit schat de directe schade van autodiefstal en de diefstal van auto-onderdelen op ruim 150 miljoen euro. Daarnaast is er sprake van een grote mate van verweving in de autobranche. Zo maakt 30 procent van de schadeherstelbedrijven zich schuldig aan heling door het kopen van onderdelen van gestolen en gestripte auto's. Die onderdelen worden vervolgens gebruikt voor reparaties van auto's van klanten. De verwevenheid wordt versterkt doordat klanten onderhandelen over de prijs en vaak vragen naar goedkopere tweedehands onderdelen. Verder worden er bij reguliere autobedrijven auto's omgekat of gestript. Ook fungeert Nederland als transitland voor elders in Europa gestolen auto's en worden gestolen auto's gebruikt voor andere criminele activiteiten zoals ramkraken en liquidaties.

Behalve financiële en ondermijnende gevolgen heeft de handel in gestolen auto's en auto-onderdelen ook gevolgen voor de verkeersveiligheid en in het bijzonder voor de persoonlijke veiligheid van verkeersdeelnemers. Zo is gebleken dat gestolen airbags niet altijd goed werken en zijn er voertuigen aangetroffen die waren samengesteld uit twee auto's waarbij de twee delen met puntlassen aan elkaar waren gezet. Deze auto's voldoen niet aan de gestelde veiligheidseisen en vormen een gevaar voor de consument. Hoeveel van die onveilige auto's er rondrijden is niet bekend.

3.9.4 Verwachtingen

Het gebruik van digitale technologie in auto's neemt de komende jaren snel toe. Het is niet meer voorbehouden aan enkel de duurdere modellen. Ook in goedkopere modellen zullen steeds meer geïntegreerde diensten worden aangeboden, waardoor steeds meer auto's via internet in verbinding staan met bijvoorbeeld de dealer, autofabrikant en eigenaar. Door deze toename worden de eerder beschreven nieuwe criminele mogelijkheden een aantrekkelijker verdienmodel voor criminelen.

De toename van het gebruik van digitale technologie in auto's zal de komende jaren leiden tot een verdere professionalisering van autodieven. Dat gaat volgens experts gepaard met een hogere organisatiegraad bij autodiefstallen, omdat de investering in kennis en materiaal te kostbaar is voor een individuele autodief.

Criminelen zullen zich waarschijnlijk nog vaker gaan richten op de verkoop van onderdelen, omdat het door de toegenomen complexiteit en afhankelijkheid van digitale technologie steeds lastiger wordt om gestolen auto's om te katten en te voorzien van een andere identiteit. De gestolen onderdelen worden in toenemende mate via internet verkocht en die groei zal de komende jaren doorzetten.

De verweving tussen autocriminaliteit en de autobranche is hoog en zal de komende jaren naar verwachting eerder verder toenemen dan afnemen. Een voorbeeld ter illustratie is de opkomst van poetsbedrijven. Deze bedrijven verdwijnen soms net zo snel als ze verschijnen en de concurrentie is hoog. Ze werken voor meerdere opdrachtgevers om auto's showroomklaar te maken en kunnen bewust of onbewust meewerken aan het verwijderen van diefstalsporen.

Er bestaat twijfel over het aantal autodiefstallen dat we de komende jaren kunnen verwachten. Aan de ene kant kan het aantal gestolen auto's verder dalen als gevolg van de toegenomen beveiliging van auto's. Dat zou een voortzetting zijn van de dalende trend die al jaren geleden met de invoering van de startonderbreker is ingezet. Aan de andere kant kan er een einde komen aan de dalende trend en kan het aantal gestolen auto's de komende jaren gelijk blijven of zelfs gaan toenemen. De vraag naar gestolen auto's en auto-onderdelen blijft bestaan en ook de beveiliging van voertuigen lijkt steeds weer omzeild te worden, doordat criminelen zich verder professionaliseren en vaker samenwerken. Zij zullen dan steeds sneller nieuwe beveiligingsmethoden weten te kraken, waardoor beveiliging geen blijvende remmende factor zal zijn.

3.9.5 Kwalificatie van dreiging

In het vorige dreigingsbeeld is bij de kwalificatie van dreiging alleen uitgegaan van de gevolgen van georganiseerde auto*diefstal.* In dit dreigingsbeeld is uitgegaan van de gevolgen van georganiseerde auto*criminaliteit*, en dat houdt in dat er nu ook rekening is gehouden met de gevolgen van diefstal van auto-onderdelen en het gebruik van gestolen auto's bij andere criminele activiteiten, en dat draagt bij aan de ernst van de gevolgen. Op basis van de ernst van de huidige gevolgen, zoals hierboven beschreven, is georganiseerde autocriminaliteit een dreiging. Als de daling van het aantal diefstallen niet verder doorzet vanwege de aanhoudende vraag naar gestolen auto's en gestolen auto-onderdelen, dan blijft georganiseerde autocriminaliteit de komende jaren een dreiging. Mocht er wel sprake zijn van een verdere daling omdat de autobranche erin slaagt de criminelen een stap voor te blijven bij het beveiligen van auto's, dan leidt dat ook tot een afname van de negatieve gevolgen voor de Nederlandse samenleving, waardoor er (mogelijk) in 2021 geen sprake meer is van een concrete dreiging. Omdat er geen eenduidigheid is in de hierboven geschetste verwachtingen en deze beide voor mogelijk worden gehouden, is georganiseerde autocriminaliteit gekwalificeerd als **voorwaardelijke dreiging** voor de Nederlandse samenleving.

3.10 Heling

3.10.1 Inleiding

De basis voor deze paragraaf vormt het (vertrouwelijke) rapport *Georganiseerde vermogenscriminaliteit. Nationaal Dreigingsbeeld 2017.* Dat rapport doet verslag van onderzoek naar zes vormen van vermogenscriminaliteit, heling is er daar een van. Dat onderzoek is voor dit dreigingsbeeld uitgevoerd in de eerste helft van 2016. De auteurs van het onderzoeksrap-

port zijn Jessica van Mantgem, Anne Mooij, Ewout Stoffers, Emilie Verschuuren, Debbie Mac Gillavry en Marsha de Bell, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*
Aan het eind van deze paragraaf staat de kwalificatie van dreiging centraal. Deze kwalificatie is niet afkomstig uit het onderzoeksrapport, maar is vastgesteld en beargumenteerd in een andere context door een groep van beoordelaars (de consensusgroep).

Heling is een misdrijf dat volgt op een eerder gepleegd vermogensdelict. Het betreft immers het verwerven, voorhanden hebben en overdragen van een door misdrijf verkregen goed. Heling wordt vaak gekwalificeerd als een slachtofferloos delict. Er is zelden een direct benadeelde die aangifte van heling doet bij de politie. Ook is de ernst van het misdrijf van dien aard dat de aangiftebereidheid vaak laag is. Met andere woorden, heling is geen aangiftedelict, in tegenstelling tot de andere vormen van georganiseerde vermogenscriminaliteit. Doordat er weinig aangifte van heling wordt gedaan, zijn de registratiecijfers van heling bij de politie vooral een weergave van de prioriteitstelling en de inspanningen door de politie om heling te bestrijden. Ze zeggen weinig over de werkelijke omvang van heling in Nederland.

3.10.2 Ontwikkelingen in aard en omvang sinds het NDB2012

Aard

Uit de literatuur, opsporingsonderzoeken en gesprekken met politiemensen en vertegenwoordigers van brancheorganisaties wordt duidelijk dat heling van gestolen waar plaatsvindt via verschillende afzetkanalen. De meestgenoemde afzetkanalen zijn winkels, (zwarte) markten, internet, het buitenland en semipublieke ruimten.
Gestolen waar afkomstig van woninginbraken of winkeldiefstallen wordt afgezet bij handelaars. Het gaat in de meeste gevallen om opkopers die hun eigen afzetmogelijkheden hebben, bijvoorbeeld via een winkel of een bedrijf dat gespecialiseerd is in de handel in bepaalde typen goederen. Deze opkopers worden volgens de politie vooral bediend door veelplegers die meestal als eenlingen en af en toe in een klein verband van lokale dieven opereren. Volgens politie-experts faciliteert deze opkopersbranche de afzet van gestolen waar op grote schaal. In eerder onderzoek werd al gesteld dat een fors deel van de bij woninginbraak buitgemaakte goederen wordt ingeleverd bij opkopers. Daarbij doen politie-experts schattingen die oplopen tot 80 procent, hoewel onduidelijk is waar deze schattingen op gebaseerd zijn.

Burgers en bedrijven die een goed willen kopen, kunnen via de website of een app van Stopheling controleren of het goed als gestolen geregistreerd staat. Treffers van diefstal kunnen via een meldknop worden doorgegeven aan de politie. Het Digitaal Opkopers Register (DOR) verplicht bepaalde opkopers van goederen in een digitaal register bij te houden wat zij inkopen, alsmede de naam en het adres van de aanbieder. Hoewel nog lang niet alle opkopers aangesloten zijn op het DOR, is al wel een omvangrijk netwerk van malafide opkopers blootgelegd dat nauw samenwerkte met criminele samenwerkingsverbanden (csv's) die zich bezighielden met georganiseerde woninginbraken en winkeldiefstallen.

Buit afkomstig van georganiseerde winkeldiefstallen lijkt minder vaak bij opkopers te worden afgezet, omdat grote hoeveelheden voor opkopers doorgaans lastig te verantwoorden zijn in hun administratie. Vaker vinden goederen uit winkeldiefstallen hun weg naar markthandelaars in Nederland of, in mindere mate, naar afnemers in het buitenland. Onderzoek heeft aangetoond dat die afzet veelvuldig verloopt via csv's van helers. Zij hebben een aanzienlijk netwerk van afnemers en toeleveranciers en knippen grote partijen gestolen waar op in kleine, verkoopbare partijen.
Consumentenartikelen afkomstig uit bedrijfsinbraken, zoals sigaretten en parfums, worden grotendeels via markthandelaars afgezet. Moeilijk verplaatsbare buit, zoals werktuigmaterieel uit de agrarische sector of de bouwsector, wordt meestal over de weg vervoerd naar Oost-Europa en daar afgezet.
Ook internet komt als afzetkanaal voor gestolen waar naar voren. Volgens politierespondenten gebruiken steeds meer mensen internet om gestolen waar, zoals sieraden, (elektrische) fietsen en smartphones, aan te bieden. Illustratief is de particuliere heler die van verschillende dieven inkoopt en ruim 10.000 advertenties op Marktplaats heeft staan. Hoewel die activiteit niet als georganiseerde criminaliteit is aan te merken, fungeert zo'n heler, net als bij de opkopers het geval is, als belangrijke facilitator voor de grootschalige afzet van gestolen waar die uit (georganiseerde) vermogenscriminaliteit afkomstig is.
Op een vergelijkbare manier zijn ook andere (rechts)personen op internet actief. Zo zijn er de laatste jaren steeds meer goudwisselkantoren die online adverteren dat zij via de post – en dus anoniem – sieraden in kunnen kopen. Ook is er een groeiend aantal Facebookgroepen waar particulieren uit buurtgroepen hun tweedehands goederen te koop aanbieden. Daar zitten helers en stelers tussen die met een zekere regelmaat gestolen waar afzetten. En dan zijn er de Faceboekgroepen die een strikt digitaal 'deurbeleid' hanteren. In die groepen zijn verkopers actief die massaal gestolen smartphones, laptops en fietsen te koop aanbieden. De groepen zijn niet openbaar en kennen een strengere controle op wie iemand is, als verkoper en als koper. Kopers die te vertrouwen zijn, krijgen toegang tot de 'etalage'. Er is informatie dat medewerkers van grote fietsenwinkels via Facebook gestolen fietsen verkopen die door de fietsenwinkels zijn opgekocht. Doordat de fietsenwinkelmedewerker fietsen privé verkoopt, blijft de clandestiene handel van de fietsenwinkel buiten de boeken en het opkopersregister. Ook zijn er aanwijzingen dat websites op het darknet worden gebruikt voor het aanbieden van gestolen waar.

Er treden met enige regelmaat verschuivingen op in de gestolen goederen waarin wordt gehandeld. Bepalend voor die verschuivingen zijn de verwachtingen omtrent de buit, de gelegenheden om in de gestolen waar te handelen en de pakkans. Het samenspel van die factoren bepaalt in welke goederen helers handelen. Voor de rest maakt het hun niet veel uit waar ze in handelen, of dat nu babymelkpoeders of elektrische fietsen zijn. Die goederen hebben de laatste jaren aan populariteit gewonnen onder het dieven- en helersgilde. Er valt veel aan te verdienen, de afzetmarkt is groot en de pakkans laag.

Om vergelijkbare redenen zijn ook de meer traditionele goederen, zoals gouden sieraden, alweer een paar jaar opnieuw *hot*. Er is een hoge buitverwachting door een gunstige goudkoers en de afzet bij en door malafide opkopers is aantrekkelijk omdat gestolen gouden sieraden direct worden omgesmolten en dus niet meer traceerbaar zijn.
De handel in gestolen, hoogwaardige elektronica, zoals laptops, iPads en smartphones, is minder aantrekkelijk geworden volgens helers. Zij geven aan dat hun buitverwachting lager is door verzadiging van de West-Europese afzetmarkt en dat door het toegenomen gebruik van *track-and-tracetechnologie* de pakkans vergroot is. Dat lijkt minder te gelden voor georganiseerde bendes. Uit opsporingsonderzoeken blijkt dat csv's de pakkans simpelweg verkleinen door gestolen partijen elektronica eerst te controleren op eventuele gps-*trackers* om de partij vervolgens snel door te zetten naar landen waar meer dan voldoende vraag is naar betaalbare, hoogwaardige elektronica.
Ook de handel in gestolen metaal en ijzer is nog altijd lucratief, vooral in vergelijking met omliggende landen. Dat komt doordat veel metaalhandelaars in Nederland nog contant uitbetalen aan aanbieders van metaal en ijzer. Dit in tegenstelling tot België en Duitsland, waar veel metaalopkopers zijn overgestapt op girale betaling.
De handel in gestolen gereedschappen afkomstig uit woninginbraken is een nichemarkt geworden. Sinds de financiële crisis is er meer tweedehands gereedschap op de markt gekomen, waardoor de afzetmarkt voor gestolen gereedschappen is geslonken en de buitverwachting naar beneden is bijgesteld. Er zijn in de afgelopen jaren opsporingsonderzoeken naar grootschalige winkeldiefstallen uitgevoerd waarin gereedschap als buit naar voren kwam. Het ging in die gevallen om diefstallen uit bouwmarkten, gepleegd door Oost-Europese mobiele bendes. Veel van die diefstallen vinden plaats op bestelling. De gereedschappen worden afgezet in landen in Oost-Europa.
In dat verband kan ook gesproken worden over de toegenomen aandacht voor materialen en hoogwaardige apparatuur uit de agrarische sector. Volgens Utrechts onderzoek uit 2013[39] worden die goederen in opdracht van Litouwse helers op het platteland gestolen door Oost-Europese mobiele bendes. Ook gestolen grondwerkapparatuur en bouwmaterieel afkomstig van afgelegen bedrijfs- en bouwterreinen vindt de laatste jaren meer aftrek.
Ten slotte zijn drogisterij-artikelen nog altijd populair voor diefstal en heling. Op talrijke markten in het land kunnen deze gestolen goederen eenvoudig worden afgezet, zonder dat de aanbieders zich zorgen maken over eventuele vervolging. Uit diverse opsporingsonderzoeken komt de Beverwijkse Bazaar naar voren als plaats waar veel georganiseerde helingpraktijken plaatsvinden. De omvang van deze praktijken is moeilijk vast te stellen. Op basis van de bestudeerde opsporingsdossiers kunnen we wel stellen dat het hier om omvangrijke, goedgeorganiseerde criminele handel gaat. De csv's laten meerdere criminele bendes in heel Europa stelen. Ze verkopen met grote regelmaat grote hoeveelheden gestolen waar aan meerdere markthandelaars op de Beverwijkse Bazaar, direct of via tussenhandelaars.

39 D. Siegel (2013). *Mobiel banditisme. Oost- en Centraal-Europese rondtrekkende criminele groepen in Nederland*. Apeldoorn: Politie & Wetenschap.

Dreiging met geweld en het gebruik van geavanceerde afschermingsmethoden duiden op grote belangen en een hoge organisatiegraad. Een andere aanwijzing dat hier sprake is van omvangrijke helingpraktijken ontlenen we aan het feit dat ten minste dertig Afghaanse markthandelaars op de Beverwijkse Bazaar verkoopprijzen hanteren die onder de reguliere inkoopprijs liggen. Dat is een sterke aanwijzing dat zij hun waar uit diefstal moeten hebben verkregen. Wat opvalt is dat veel van deze ondernemers exact dezelfde prijzen voor exact dezelfde goederen vragen. Dit duidt op onderlinge afspraken om concurrentie te voorkomen.

Omvang

Heling is een delict waarvan de omvang erg moeilijk is vast te stellen. Dat komt vooral doordat heling geen aangiftedelict, maar een haaldelict is. Over het algemeen wordt geen aangifte gedaan van gevallen van heling. Kopers van gestolen waar zijn weliswaar getuige van het delict, maar om voor de hand liggende redenen doen zij daar geen aangifte van. De kloof tussen het aantal diefstallen en het aantal aangiften van heling is daarvoor illustratief: in 2015 werden 544.000 diefstallen geregistreerd en slechts 6500 gevallen van heling.
Nu zal sommige buit niet geschikt zijn om te verkopen (geld bijvoorbeeld) en behouden dieven de buit ook wel voor eigen gebruik, maar het overgrote deel van de gestolen goederen is bedoeld om te worden afgezet. Gelet op het aantal diefstallen is heling daarmee een wijdverspreid fenomeen.
Naar inschatting van experts is 30 procent van de opkopers malafide. Het zou dan gaan om duizenden opkopers verspreid over het hele land. Die inschatting is gebaseerd op stelselmatige controles van het DOR, op talrijke verhoren van verdachten en op observaties en getuigenverhoren. Deze malafide opkopers faciliteren bij de verkoop van gestolen waar.

3.10.3 Huidige gevolgen

Geweld

De machtspositie van een aantal csv's doet zich gelden in gevallen waarbij ondernemers in de bovenwereld onder druk worden gezet om gestolen goederen af te nemen. Het feit dat een groot deel van die ondernemers niet op papier wil verklaren, betekent dat de angst groot is. Het gaat naar schatting om enkele tientallen ondernemers. Al met al gaan er enkele tientallen tot honderden mensen gebukt onder de dreiging met geweld. Het gaat dan niet alleen om afgeperste markthandelaars of hun families, maar ook om controleurs van opkopers die bedreigd worden en om tipgevers die vanuit een bepaalde (lokale) gemeenschap zouden willen verklaren over malafide handelspraktijken. In enkele gevallen vallen er doden en gewonden ten gevolge van helingpraktijken.

Financieel/economisch

De gevolgen van heling bestaan voor een belangrijk deel uit financiële schade voor de Nederlandse samenleving. Het gaat dan vooral om inkomstenderving voor het bedrijfsleven. Dat leidt ook tot verminderde inkomsten voor de Nederlandse schatkist door derving van btw-afdrachten. Het aanbod van gestolen waar heeft ook gevolgen die de financiële

schade enigszins temperen. Koopjesjagers die bepaalde goederen niet voor de gangbare handelsprijzen bij de reguliere detailhandel (willen) kopen, kopen nu wel. De verkoop van gestolen waar zorgt dus voor meer uitgaven en daardoor wordt de economische bedrijvigheid gestimuleerd.
Op het gebied van de economie leiden omvangrijke helingpraktijken tot oneerlijke concurrentie en lokaal verdringing van legale bedrijven. Vooral bonafide opkopers en ondernemers die in elektronica, sieraden, auto's en auto-onderdelen handelen, kampen lokaal met die oneerlijke concurrentie.

Ondermijning
Er zijn helers die zich openlijk met de verkoop van gestolen waar bezighouden. Het gaat om ondernemers die hun helingpraktijken inbedden in een legale bedrijfsstructuur, opgaan in een grote massa van bonafide collega-ondernemers en deel uitmaken van een branche waar tussenhandel gangbaar is. Op het eerste gezicht lijkt er vaak niets mis met de portalen van malafide ondernemers die op markten, in winkelstraten, in woonwijken of vanaf bedrijventerreinen hun producten en diensten aanbieden. Voor de consument maken zij 'gewoon' onderdeel uit van het reguliere handelscircuit. Aan de voordeur is het voor consumenten lastig op te maken of de partij met wie zij zakendoen bonafide of malafide is. Daardoor nemen zij soms ongewild en ongemerkt deel aan helingpraktijken.
Onderzoek laat zien dat er in Nederland helende facilitatoren zijn die stelers en afnemers bij elkaar brengen. Zij zorgen ervoor dat de handel in gestolen waar rendeert. Sommigen doen dat al jarenlang, in relatieve openheid en op grote schaal. Daardoor bestaat in Nederland een aanzienlijke afzetmarkt voor gestolen waar. Dit speelt heling in de kaart. Voor afnemers van gestolen waar, consumenten en bedrijven, kan een indruk ontstaan dat er sprake is van een gedoogbeleid. Dat draagt bij aan vervaging van normbesef. Bij een opkoper, bij een autohandelaar of op lokale markten lijken consumenten in toenemende mate de keuze voor een goedkoop goed van bedenkelijke afkomst te kunnen appreciëren. Blijkbaar is het voor zowel verkopers als kopers gemeengoed dat gestolen waar wordt verkocht. Markten en opkoopbedrijven waar deze praktijken veelvuldig plaatsvinden, zijn aan te merken als locaties die aanleiding geven tot normvervaging. Dat leidt tot meer heling en doet de criminele activiteiten die daaraan voorafgaan, toenemen.

3.10.4 Verwachtingen
Naar verwachting zal het Digitaal Opkopers Register (DOR) in de komende jaren landelijk geïmplementeerd worden. Hierdoor kunnen helende opkopers en hun criminele toeleveranciers lastiger zakendoen. Ze weten dat ze worden geregistreerd en dat ze bij fysieke controle van het register of een hit met de politiesystemen direct tegen de lamp kunnen lopen. Hierdoor zullen vooral gelegenheidshelers gaan afhaken. Georganiseerde helers, veelplegers of andere criminelen die zich voor hun broodwinning van heling afhankelijk hebben gemaakt, laten zich niet afschrikken door de invoering van het DOR of bewustwordingscampagnes. Op korte termijn wordt verwacht dat zij gestolen goederen blijven aanbieden door bijvoorbeeld valse identiteitsgegevens of valse papieren te gebruiken bij legale opkopers.

Ook zullen zij waar aanbieden bij opkopers die nog niet op het DOR zijn aangesloten. Uit recente telefoontaps blijkt dat ook. Daarin vragen zij zich af bij welke gemeenten ze nog met 'hun spul' terecht kunnen omdat 'de opkopers daar nog geen register hebben'.
Op langere termijn, als het DOR in heel Nederland is doorgevoerd, zullen georganiseerde helers andere afzetkanalen gebruiken. Dat baart zorgen. Veel respondenten verwachten namelijk dat internet vaker als afzetkanaal zal worden gebruikt. Helers krijgen zodoende een groter nationaal en internationaal bereik en zijn ook lastiger op te sporen. Consumenten worden bovendien minder uitgenodigd om (zich af) te vragen wat de herkomst van een goed is. En verkopers op internet kunnen de herkomst van hun gestolen goederen eenvoudig maskeren.
Een andere factor die leidt tot de verwachting dat heling in georganiseerd verband zal aanhouden, is de manier waarop de samenleving met heling en de gevolgen daarvan omgaat. In sommige branches en op sommige lokale afzetmarkten is volgens respondenten sprake van aanhoudende en doorzettende normvervaging. Het wordt steeds normaler dat er bij de handel in auto's en auto-onderdelen, in goud en sieraden, in tweedehands goederen, in drogisterij-artikelen, in luxe elektronica, in fietsen en wat dies meer zij, koopjes worden gescoord die vermoedelijk uit diefstal afkomstig zijn. Het lijkt erop dat helingpraktijken in onze samenleving steeds meer worden geaccepteerd.

De toekomstige gevolgen van heling zullen naar verwachting niet anders zijn dan de huidige en bewegen zich vooral op het financieel-economische en ondermijnende vlak. Dat deze gevolgen zich voordoen, staat buiten kijf. Wat de ernst ervan is, valt niet vast te stellen omdat betrouwbare, cijfermatige gegevens ontbreken. Ook is onbekend voor welk deel heling in georganiseerd verband plaatsvindt.

3.10.5 Kwalificatie van dreiging

Nederland heeft een klimaat waarin heling gedijt, omdat het geen topprioriteit heeft bij opsporingsinstanties en er veel vraag is naar goedkope goederen. Onderzoek wijst uit dat veel mensen er geen moeite mee hebben om goederen te kopen waarvan de herkomst onbekend is. Dit zal waarschijnlijk de komende jaren niet veranderen. Hoewel nadelige gevolgen van heling zich zullen blijven voordoen, wordt heling gekwalificeerd als **witte vlek**, omdat de omvang van de huidige en te verwachten financieel-economische schade niet bekend is. Evenmin is bekend in hoeverre de schade te wijten is aan de georganiseerde vorm van heling.

Deel 3

Cybercrime en milieucriminaliteit

1 Inleiding

In deel 2 zijn 34 criminele verschijnselen besproken en voorzien van een kwalificatie van dreiging. In dit derde deel volgen nog twee belangrijke onderwerpen: cybercrime en milieucriminaliteit. Deze twee criminele verschijnselen worden in dit deel behandeld, omdat geen van beide een kwalificatie van dreiging heeft gekregen. De redenen hiervoor zijn in het geval van milieucriminaliteit anders dan in het geval van cybercrime.

Cybercrime leent zich niet voor een kwalificatie van dreiging, omdat het niet kan worden beschouwd als losstaand crimineel verschijnsel. Er is sprake van een steeds sterker wordende verweving tussen cybercrime en traditionele vormen van criminaliteit. Cybercrime is daarmee eerder een thema-overstijgende werkwijze dan een crimineel verschijnsel en werkwijzen worden in het Nationaal dreigingsbeeld niet voorzien van een kwalificatie van dreiging.
De meer specifieke hightechcrimevarianten van cybercrime lenen zich ook niet voor een kwalificatie van dreiging volgens de methode van het Nationaal dreigingsbeeld. Behalve dat deze varianten niet allemaal niet tot het domein van de georganiseerde criminaliteit behoren, blijkt uit het onderzoek dat, per variant, de omvang en de schadelijke gevolgen voor de Nederlandse samenleving onbekend zijn. Dat zou leiden tot een kwalificatie die geen recht doet aan het belang van het toenemende gebruik van geavanceerde digitale middelen in de georganiseerde criminaliteit.

Milieucriminaliteit kent vele verschijningsvormen, zoals afvaldumping, illegale import van diergeneesmiddelen, het (weg)mengen van giftige stoffen in stookolie en het niet naleven van veiligheidsvoorschriften in risicobedrijven. In de meeste gevallen zijn het legale ondernemingen die zich met deze praktijken bezighouden. Door regels en richtlijnen uit milieuwet- en -regelgeving niet na te leven, willen ze kosten besparen om zo op illegale wijze extra geld te verdienen.
De verschillende verschijningsvormen van milieucriminaliteit laten zich qua omvang lastig in kaart brengen. Dat heeft een aantal oorzaken. Wanneer legale en illegale activiteiten binnen de reguliere bedrijfsvoering van een onderneming verweven zijn, is het constateren van misdrijven vaak moeilijk. Als regelovertreding al wordt vastgesteld, is het nog geen sinecure om opzet daarbij aan te tonen. Of en hoe vaak er sprake is van misdrijven, blijft daardoor meestal onbekend.

Ook factoren als schaalvergroting binnen sommige branches in het milieudomein en internationale handelsstromen vertroebelen het zicht van controle- en handhavingsdiensten op het milieudomein. Complexe milieuwetten en -regels overlappen elkaar soms gedeeltelijk en zijn soms met elkaar in tegenspraak. Dat maakt interpretatie ervan lastig, bemoeilijkt de vraag welke instantie voor welke handhavings- of opsporingstaak verantwoordelijk is en leidt ertoe dat controles niet altijd plaatsvinden of te weinig of niet adequaat worden uitge-

voerd. In relatie tot de omvangrijke activiteiten in het milieudomein kampen veel handhavings- en opsporingsdiensten met capaciteitsproblemen en een tekort aan specialistische kennis en deskundigheid. Onder andere hierdoor vindt relatief weinig strafrechtelijk onderzoek plaats.

Deze factoren maken dat de aard en omvang van milieucriminaliteit voor een deel onbekend blijven. Al met al is er te weinig informatie beschikbaar om conform de NDB-methodiek de aard, omvang, toekomstverwachtingen en gevolgen van milieucriminaliteit te beschrijven en mede op basis daarvan een kwalificatie van dreiging toe te kennen. Zouden we wel tot kwalificeren overgaan, dan zouden veel verschijningsvormen van milieucriminaliteit gekwalificeerd worden als 'witte vlek'. Dat zou de ernst van milieucriminaliteit geen recht doen. Daarom is gekozen voor een andere benadering.

2 Cybercrime en gedigitaliseerde criminaliteit

2.1 Inleiding

Er is een heel scala aan actoren actief in cyberspace die een dreiging vormen voor de cybersecurity. Dat zijn onder meer beroepscriminelen, statelijke actoren, terroristen, hacktivisten en cybervandalen. De groeiende dreiging voor de cybersecurity van Nederland wordt volgens het *Cybersecuritybeeld Nederland 2016* van het Nationaal Cyber Security Centrum vooral veroorzaakt door beroepscriminelen en statelijke actoren. Dit hoofdstuk richt zich voornamelijk op de groeiende dreiging die uitgaat van beroepscriminelen die zich bezighouden met cybercrime en gedigitaliseerde criminaliteit. Criminaliteit gepleegd door statelijke actoren, terroristen, hacktivisten en cybervandalen komt slechts zijdelings aan bod, omdat deze niet tot het domein van georganiseerde criminaliteit behoort. Voor het domein van terrorisme en spionage zijn er rapportages van de Nationaal Coördinator Terrorismebestrijding en Veiligheid, de Algemene Inlichtingen- en Veiligheidsdienst en het Nationaal Cyber Security Centrum die voorzien in de kennis- en informatiebehoefte.

De groeiende interesse van beroepscriminelen voor cybercrime en digitalisering van commune delicten (gedigitaliseerde criminaliteit) past in de algemene tendens van toenemende digitalisering in de samenleving. Geavanceerde digitale mogelijkheden zijn voor iedereen toegankelijk en te gebruiken zonder veel voorkennis. Rode draad binnen deze mogelijkheden zijn de steeds betere encryptietechnieken, die zorgen voor een steeds betere beveiliging (cybersecurity) van zowel legale als illegale handelingen en activiteiten. Aan criminelen bieden ze de kans anoniem te opereren en zich af te schermen voor opsporingsactiviteiten.

De basis voor dit hoofdstuk vormt het (vertrouwelijke) rapport *Cybercrime en gedigitaliseerde criminaliteit. Nationaal dreigingsbeeld 2017.* De auteurs van het onderzoeksrapport zijn Kristiaan Schuppers, Nikita Rombouts, Peter Zinn en Hielke Praamstra, allen werkzaam bij de politie. De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017*.

Er wordt in het onderzoek onderscheid gemaakt tussen cybercrime en gedigitaliseerde criminaliteit. Bij cybercrime gaat het om criminaliteit waarbij informatie- en communicatietechnologie (ICT) zowel het middel als het doelwit is. Cybercrime kent technieken en middelen enerzijds en verschijningsvormen anderzijds. Bij technieken en middelen gaat het om hacken, malware, botnets, DDoS-aanvallen en *social engineering.* Bij verschijningsvormen gaat het om het doel waarmee de technieken en middelen worden ingezet, zoals verstoring van ICT, afpersing, diefstal van datasets met persoonsgegevens en fraude met betaalmiddelen.

Sommige varianten van cybercrime worden hightechcrime genoemd, hoofdzakelijk vanwege het innovatieve en ondermijnende karakter. Tot deze hightechcrimevarianten van cybercrime behoren aanvallen op vitale infrastructuren, aanvallen op het financiële stelsel, bedrijfsspionage en hacktivisme. Hoewel deze varianten deels niet tot het domein van de georganiseerde criminaliteit behoren, wijden wij er in dit hoofdstuk wel aandacht aan vanwege hun innovatieve karakter en mogelijke implicaties voor cybercrime en gedigitaliseerde criminaliteit.
Bij gedigitaliseerde criminaliteit is ICT een middel om (traditionele vormen van) criminaliteit te plegen. ICT kan een rol spelen in elk van de fasen van het criminele proces, bij zowel de voorbereiding als de uitvoering als de afronding. Zo kunnen de sociale media dienen als ontmoetingsplaats, het darkweb als handelsplaats en kan witwassen plaatsvinden met behulp van bitcoins. Digitale technologie vergroot de reikwijdte van criminelen en biedt goede mogelijkheden om criminele activiteiten af te schermen voor opsporing en justitie.

In de praktijk is het onderscheid tussen cybercrime en gedigitaliseerde criminaliteit niet zo strikt. Er is sprake van een steeds sterkere verweving tussen cybercrime, gedigitaliseerde criminaliteit en traditionele vormen van criminaliteit. Binnen het domein van georganiseerde criminaliteit is het gebruik van digitale technologie in al haar facetten eerder een thema-overstijgende werkwijze dan dat er sprake is van nieuwe digitale vormen van georganiseerde criminaliteit.

In dit hoofdstuk wordt een beeld gegeven van de ontwikkelingen die de afgelopen jaren bij cybercrime en gedigitaliseerde criminaliteit hebben plaatsgevonden en van de invloed die deze ontwikkelingen hebben gehad op de (daders van) georganiseerde criminaliteit. Daarnaast worden verwachtingen geformuleerd voor de komende jaren: wat te verwachten ontwikkelingen op het gebied van ICT zijn, hoe die zich verhouden tot de georganiseerde criminaliteit en welke mogelijke gevolgen dat heeft voor de Nederlandse samenleving.

2.2 Ontwikkelingen van cybercrime en gedigitaliseerde criminaliteit

De huidige tijd kenmerkt zich door de snelle opeenvolgende ontwikkelingen van digitale technologie, ontwikkelingen die invloed hebben op de hele samenleving, het criminele deel incluis. In het Nationaal dreigingsbeeld van 2004 werd de invloed van deze nieuwe ontwikkelingen op de georganiseerde criminaliteit vooralsnog beperkt geacht. De nieuwe mogelijkheden werden destijds voornamelijk gebruikt om te communiceren. Wel werd verwacht dat criminele samenwerkingsverbanden in toenemende mate gebruik zouden gaan maken van de mogelijkheden op dit vlak, bijvoorbeeld om afgeschermd te communiceren. De ontwikkelingen bleken sneller te gaan dan destijds verwacht werd. In het NDB2008 speelde bij meerdere onderwerpen internet al een belangrijke rol en niet uitsluitend als communicatiemiddel. Onderwerpen die voorbijkwamen, waren onder andere virtuele seks, witwassen en de verkoop van kweekbenodigdheden voor hennepkwekerijen via internet.

De verwachting in 2008 was dat de digitalisering van het criminele bedrijf gelijke tred zou houden met de digitalisering in de samenleving. Die verwachting is tot op heden bewaarheid. In het NDB2012 werd de digitale technologie als alomtegenwoordig beschouwd en voor het huidige NDB geldt hetzelfde, met de toevoeging dat digitale technieken tegenwoordig geraffineerder en professioneler gebruikt worden dan voorheen.

2.2.1 Cybercrime

Afpersing

Cybercrime wordt steeds agressiever en ook wordt steeds directer de confrontatie aangegaan met slachtoffers. Het gaat dan vooral om afpersing waarbij de computer van een slachtoffer versleuteld wordt door *ransomware.* Daardoor kan het slachtoffer niet meer bij zijn persoonlijke gegevens. Het slachtoffer wordt gevraagd te betalen voor de sleutel om weer toegang te krijgen tot zijn informatie. Slachtoffers worden op slinkse wijze verleid om bijvoorbeeld te klikken op besmette hyperlinks op internetpagina's of in mailtjes. Sinds 2013 worden zowel particulieren als bedrijven in toenemende mate slachtoffer van ransomware. Ransomware wordt over het algemeen ongericht verspreid maar soms ook gericht naar specifieke bedrijven.

Vooral het midden- en kleinbedrijf (MKB) en (semi)overheidsorganisaties zijn kwetsbaar, omdat hun ICT niet altijd up-to-date is en vaak slecht beveiligd. Zo zijn ziekenhuizen in de Verenigde Staten en Duitsland slachtoffer geworden van afpersing via ransomware. Bij Nederlandse ziekenhuizen is dit – voor zover bekend – nog niet voorgekomen, maar het wordt door experts wel mogelijk geacht dat ook zij hiermee geconfronteerd zullen worden. De aangiftebereidheid bij bedrijven is laag, omdat bedrijven weinig vertrouwen hebben in de wijze waarop de aangiften door de politie worden opgepakt. Bovendien zijn ze bang voor reputatieverlies. Door de geringe aangiftebereidheid ontbreekt een goed zicht op de omvang van aanvallen met ransomware.

Behalve ransomware worden ook DDoS-aanvallen gebruikt voor afpersingsdoeleinden. Door het gebruik van DDoS wordt een website onbereikbaar. Vooral websites waar transacties worden gedaan zijn slachtoffer, zoals webshops, financiële websites en websites van de reisbranche.

Fraude

Uit de onderzoeken naar horizontale fraude blijkt dat de digitale ontwikkelingen gretig omarmd zijn bij het plegen van fraude (zie ook deel 2, Fraude en witwassen). Bij meerdere verschijningsvormen van horizontale fraude spelen een of meer cybercrime-elementen een duidelijke rol: fraude met internetbankieren, fraude met creditcardgegevens, fraude met online handel, factuurfraude en CEO-fraude. De cybercrime-elementen waar het om gaat, zijn het gebruik van malware en hacking. Ook de werkwijzen phishing en social engineering spelen bij deze fraudevormen een rol.

Bij fraude met internetbankieren werd in 2012 vooral gebruikgemaakt van *banking malware* waarbij de directe communicatie tussen bank en klant vervangen werd door een communicatie tussen klant-crimineel-bank, het zogenoemde *man-in-the-middle*-principe. Dat is sinds die tijd flink afgenomen, omdat de geautomatiseerde detectie van malware bij banken sterk is verbeterd. Tegenwoordig wordt vooral phishing (zonder malware) gebruikt. Mensen worden er via een mail toe verleid naar een bepaalde website te gaan, waar naar hun inloggegevens wordt gevraagd. Ook dat is de laatste jaren afgenomen. Volgens experts is dat te danken aan een betere detectie en opsporing van netwerken van moneymules (geldezels). Deze verbetering is mede gerealiseerd dankzij de Electronic Crime Taskforce, een samenwerkingsverband van de vier grote banken van Nederland, International Card Services BV (ICS), het Openbaar Ministerie en de politie om digitale bancaire criminaliteit te bestrijden.

Bij fraude met creditcardgegevens is er volgens Europol in de meeste lidstaten van de Europese Unie sprake van een verschuiving van zogenoemde *card-presentfraude* naar zogenoemde *card-not-presentfraude.* Digitaal zijn er grote hoeveelheden betaalkaartgegevens beschikbaar door onder andere datalekken, deels als gevolg van *data stealing malware* en social engineering. Deze vorm van fraude speelt slechts een kleine rol in Nederland. Er wordt in ons land relatief weinig met creditcards betaald en veel meer met het beter beveiligde iDEAL.

Bij fraude met online handel zijn meer technisch complexe cybercrime-elementen terug te vinden dan vier jaar geleden. Zo is het namaken van webwinkels de afgelopen jaren professioneler geworden en zijn nepwebwinkels niet of nauwelijks van echte te onderscheiden. De makers van de valse websites zorgen – op naam van een katvanger – voor een inschrijving bij de Kamer van Koophandel, een kantoorpand, een telefoonnummer (met telefoniste) en een bestaand adres. De valse websites zijn lastig uit de lucht te krijgen, doordat ze veelal in Azië en Amerika (Panama) worden gehost. Ook zijn er voorbeelden waarbij hotmail- en Gmailaccounts gehackt zijn om marktplaatsaccounts te achterhalen. Zo'n account wordt dan gebruikt om te adverteren met een webwinkel die ofwel *fake* is ofwel ook gehackt. Op dit moment lijkt er sprake van een verschuiving van frauduleuze verkopen via bekende online handelsplaatsen en nepwebwinkels naar frauduleuze verkopen via sociale media. Er worden bijvoorbeeld goederen aangeboden via Facebook.

Ook bij CEO-fraude en factuurfraude worden weleens technisch complexere cybercrime-elementen aangetroffen. Alleen is niet duidelijk of het hier een nieuwe ontwikkeling betreft. Bij CEO-fraude wordt een persoon of een afdeling van een bedrijf zogenaamd door de CEO van dat bedrijf benaderd om een fors bedrag over te maken naar een bepaalde bankrekening. Hiervoor wordt een bedrijf weleens gehackt om informatie te krijgen die bruikbaar is voor het plegen van de fraude. Bij factuurfraude wordt soms een man-in-the-middle-werkwijze gehanteerd om tussen de leverancier en afnemer in te komen en een factuur met gewijzigd rekeningnummer te versturen ten gunste van de crimineel.

Diefstal van persoonsgegevens

In de context van cybercrime gaat het bij de diefstal van persoonsgegevens om diefstal van digitale datasets met persoonsgegevens na bijvoorbeeld het hacken van servers. Voor deze vorm van diefstal kunnen verschillende beweegredenen zijn. Zo kunnen de gegevens worden gestolen vanuit financiële motieven (doorverkopen van gegevens of afpersen) of vanuit ideologische motieven. Zogenoemde *whitehat*-hackers testen vanuit nobele motieven de beveiliging van servers door te proberen deze te hacken.

In 2014 telden vooral de Verenigde Staten meerdere voorbeelden van grootschalige datalekken van persoonlijke gegevens van klanten bij webwinkels, grote winkelketens en banken en van cliënten van ziektekostenverzekeraars en medische instellingen. Vanwege de grootschaligheid wordt 2014 wel Year of the Mega Breaches genoemd. Ook daarna zijn er in het buitenland grootschalige datalekken geweest; in de databases waaruit gelekt werd, stonden ook gegevens van Nederlanders. In Nederland hebben – voor zover bekend – dergelijke grote hacks niet plaatsgevonden.
In 2015 zijn er buiten Nederland enkele grote hacks geweest. Zo was er een hack op het Amerikaanse Office of Personnel Management (OPM), waarvan de gegevens zouden kunnen worden misbruikt voor contraspionage en het onder druk zetten of chanteren van overheidsmedewerkers. Ook was er een hack op Ashley Madison, een online datingsite, waarin werd geëist dat de website zou worden opgeheven.
In Nederland zijn er hacks geweest op speelgoedfabrikant V-tech en huishoudketen Brabantia, maar de achterliggende motieven zijn onbekend. Sinds 2016 bestaat in Nederland de verplichting datalekken te melden bij de Autoriteit Persoonsgegevens. Op 15 december 2016 stond de teller op bijna 5500 meldingen. De datalekken die bekend zijn geworden, zijn volgens de Autoriteit Persoonsgegevens vooral het gevolg van slordigheid en niet van crimineel handelen. Het betreft onder andere zoekgeraakte usb-sticks, verkeerd verstuurde mailtjes, niet-afgesloten bureauladen en documenten die in de prullenbak belandden in plaats van vernietigd te worden.

Verstoring, vernieling, sabotage

In dit tekstblok gaat het om de gevallen waarin het daadwerkelijk de intentie is om ICT te verstoren of te vernielen en niet om partijen af te persen voor geld. Afpersing is hierboven afzonderlijk behandeld.
Er kunnen diverse motieven zijn om de ICT te willen verstoren of vernielen en een ander zo schade toe te brengen: baldadigheid, wraak, concurrentie of ideologische motieven. De daders (en motieven) van dergelijke aanvallen blijven meestal onbekend.
De meest voorkomende vormen zijn DDoS-aanvallen en *defacements*. DDoS staat voor 'distributed denial-of-service' en houdt in dat een computerserver of website van een bedrijf of instelling wordt aangevallen door meerdere besmette computers (oftewel een botnet), waardoor de website of server plat komt te liggen en klanten en gebruikers er niets meer mee kunnen.

DDoS-aanvallen zijn een wijdverspreid probleem en worden wel de meest gedemocratiseerde vorm van cybercrime genoemd. Voor een geringe prijs kunnen DDoS-aanvallen worden ingekocht via zogenoemde *booter services.* De meeste aanvallen vinden plaats tussen jongeren onderling, maar ook volwassenen en bedrijven maken zich er schuldig aan. *Defacement* of *defacen* is het aanpassen van webpagina's, vaak met als doel een politieke of ideologische boodschap achter te laten. In sommige gevallen zijn er ernstiger vormen van sabotage, waarbij gegevens worden gewist en er informatie verloren gaat.

2.2.2 Hightechcrime

Aanvallen op vitale infrastructuren

Een infrastructuur is vitaal als producten, diensten en de onderliggende processen van essentieel belang zijn voor het dagelijkse leven van de meeste mensen. De vitale producten waar het om gaat, zijn onder meer olievoorziening, productie, transport en distributie van gas en elektriciteit, drinkwatervoorziening, waterbeheer en toegang tot internet en datadiensten. Verstoring van deze producten en processen kan (zeer) ernstige economische, fysieke en sociaal-maatschappelijke gevolgen hebben die leiden tot maatschappelijke ontwrichting. In Nederland is dat tot op heden niet gebeurd. Wel zijn er voorbeelden in het buitenland, zoals een cyberaanval op het Oekraïense elektriciteitsnet in 2015 waarbij 225.000 huishoudens enkele uren zonder stroom kwamen te zitten.

Organisaties in Nederland die verantwoordelijk zijn voor vitale processen en producten hebben evenals andere organisaties last van cyberaanvallen. De meeste aanvallen blijken niet specifiek gericht te zijn tegen de vitale processen. De meestgebruikte digitale instrumenten bij deze aanvallen zijn malware, phishing en ransomware. De vitale processen zijn kwetsbaar voor aanvallen, doordat vaak verouderde procescontrolesystemen worden gebruikt die niet geüpdatet worden maar wel van buitenaf, via internet, toegankelijk zijn. Hiervoor is de laatste jaren meer aandacht en dat heeft geleid tot extra beveiligingsmaatregelen. Daardoor zullen eenvoudige hacks waarschijnlijk minder vaak voorkomen. Desalniettemin blijven vitale processen kwetsbaar voor geavanceerde aanvallen. Er zijn actoren die over de middelen en vaardigheden beschikken om dergelijke aanvallen op vitale infrastructuren uit te voeren. In hoeverre die actoren ook motieven hebben om dit de komende jaren in Nederland te doen, is afhankelijk van internationale politieke en andere ontwikkelingen.

Aanvallen op banken

Bij aanvallen op banken spelen verschillende motieven een rol: het verkrijgen van informatie, ontwrichting van het financiële stelsel en financieel gewin. Zowel criminelen als statelijke actoren kunnen aanvallen (laten) uitvoeren om informatie te verkrijgen. Het doel van statelijke actoren kan bijvoorbeeld zijn invloed uit te kunnen oefenen op of wanorde te kweken in het financiële stelsel van andere landen. Criminelen vallen banken vooral aan om veel geld te verdienen.

Er zijn wereldwijd diverse aanvallen op banken geweest waarbij grote hoeveelheden geld zijn buitgemaakt. Het meest tot de verbeelding sprekende voorbeeld is dat van de criminele groep die in 2014-2015 met behulp van de zogenoemde *Carnabak malware* over de hele wereld meer dan honderd banken heeft aangevallen en tussen de 500 miljoen en 1 miljard US dollar heeft buitgemaakt. De aanvallen waren goed voorbereid en social engineering speelde een belangrijke rol. De aanvallers gebruikten ook de Society for Worldwide Interbank Financial Telecommunication (SWIFT) om grote geldbedragen over te schrijven naar hun eigen rekeningen. SWIFT is een internationaal communicatiesysteem waar wereldwijd ruim negenduizend banken en andere financiële spelers gebruik van maken. In 2015 en 2016 zijn twee banken aangevallen met gebruikmaking van SWIFT. Daarbij werden grote geldbedragen gestolen. Slachtoffers waren de centrale bank van Bangladesh en een commerciële bank in Vietnam.
Er zijn voor zover bekend geen Nederlandse banken slachtoffer geworden van dergelijke grote aanvallen. Maar door deze aanvallen werden zij zich er wel van bewust dat deze ook in Nederland zouden kunnen plaatsvinden. Het is een serieus risico, waarmee banken nu meer rekening houden dan voorheen in de scenario's die ze ontwikkelen om voorbereid te zijn op aanvallen van criminelen.

In Nederland is vooralsnog alleen sprake van pogingen om banksystemen binnen te dringen. Daarbij lijkt het deels te gaan om schijnaanvallen om de beveiliging te testen. De toegenomen maatregelen aan de kant van de banken vragen om grotere investeringen van cybercriminelen. Deze criminelen gaan zich daarom steeds beter organiseren en zich steeds beter voorbereiden om de aanvallen op banken zo effectief mogelijk uit te kunnen voeren. De verwachting is dat daardoor de opbrengst (en dus het verlies voor de banken) per aanval groter wordt. Wat het risico vergroot, is het feit dat de financiële keten als gevolg van de invoering van de nieuwe EU-richtlijn Payment Service Directive2 uit steeds meer partijen bestaat die een deel van het betalingsverkeer overnemen, alle met hun eigen systemen en kwetsbaarheden. Daardoor hebben banken steeds minder controle over de verschillende onderdelen in de keten.

Bedrijfsspionage

Staten, bedrijven en criminelen houden zich bezig met bedrijfsspionage. In de praktijk is het soms lastig onderscheid te maken tussen de verschillende actoren. Zowel statelijke actoren als bedrijven maken voor bedrijfsspionage gebruik van de diensten van beroepscriminelen en criminele middelen (malware).

Spionage door bedrijven bij andere bedrijven of wetenschappelijke instituten heeft doorgaans als doel het verbeteren van de eigen concurrentie- en kennispositie. Bij multinationals gaat het vaak om diefstal van intellectueel eigendom. Dergelijke aanvallen worden zelden openbaar gemaakt. Er zijn enkele Amerikaanse gevallen van vooral bedrijfsmatige spionage bekend geworden. Zo heeft een Amerikaanse aanbieder van linnengoed toegegeven een server van een concurrent te hebben gehackt om zicht te krijgen op diens klanten

en die vervolgens te benaderen. Ook bekende een scout van een Amerikaans baseballteam dat hij een database (met onder andere contract-informatie) van een rivaliserend team had gehackt. Uit gelekte documenten van de gecompromitteerde datingsite Ashley Madison bleek dat de leiding daarvan zich in het verleden toegang had verschaft tot de klantendatabase van een concurrerende datingsite. In 2015 meldden de Nederlandse media dat Chinese hackers chipfabrikant ASML gehackt hadden en informatie hadden gestolen.

Er is nauwelijks zicht op bedrijfsspionage en eventuele ontwikkelingen op dit terrein. Wel kan worden gesteld dat de belangen en potentiële opbrengsten van bedrijfsspionage groot zijn en dat deze vorm van spionage in Nederland voorkomt. Bewustwording en maatregelen blijven achter op de dreiging die volgens experts van dit fenomeen uitgaat. Als dat niet verandert, is de verwachting dat bedrijfsspionage zich de komende jaren ook in Nederland vaker zal voordoen, met nadelige gevolgen voor de concurrentiepositie van ons land.

Hacktivisme

De term *hacktivisme* is een samentrekking van de woorden 'hacking' en (politiek) 'activisme'. Hacktivisme onderscheidt zich van reguliere cybercrime in het motief. Hacktivisten acteren vanuit een politieke of anderszins idealistische overtuiging en ze gebruiken daarvoor drie methoden: (1) verstoren en ontoegankelijk maken van websites, bijvoorbeeld door DDoS-aanvallen, (2) verspreiden van een (ideologische) boodschap, bijvoorbeeld door defacements, en (3) informatie stelen en openbaar maken, bijvoorbeeld door hacking.

De meerderheid van de aanvallen is klein en heeft een beperkte impact. Een DDoS-aanval of defacement kan relatief snel worden opgelost. Er mogen dan weinig grote hacktivistische aanvallen zijn, één enkele aanval kan een grote impact hebben. Voorbeelden hiervan zijn de NSA-*databreach* van Edward Snowden in 2013 en de Panamapapers-hack in 2016. Deze *highprofile*-aanvallen hebben consequenties die jaren kunnen voortduren. Ze zijn eenvoudig uit te voeren, en het lage beveiligingsniveau van de ICT bij veel bedrijven voedt de verwachting dat dergelijke aanvallen steeds meer gemeengoed zullen worden.

2.2.3 Gedigitaliseerde criminaliteit

Bij gedigitaliseerde criminaliteit is ICT een middel om (traditionele vormen van) criminaliteit te plegen. ICT kan een rol spelen in alle fasen van het criminele proces: bij de voorbereiding, de uitvoering en de afronding.

Bij de productie van en handel in cannabis en synthetische drugs speelt internet een rol in de voorbereiding. Het gaat hierbij vooral om het uitwisselen van kennis en informatie over bijvoorbeeld nieuwe productiemethoden of recepten voor nieuwe synthetische drugs. Wat betreft vermogensmisdrijven is er anekdotische informatie dat Google Earth gebruikt wordt voor doelwitselectie en voorverkenning bij woninginbraken en voertuigdiefstal. Sociale media worden gebruikt om afspraken te maken over straatroven, overvallen of woninginbraken.

Bij verschillende vormen van vermogenscriminaliteit worden digitale technologieën gebruikt bij de uitvoering. De opvallendste ontwikkeling is zichtbaar bij de diefstal van auto's: daarbij worden steeds vaker laptops gebruikt voor het uitlezen van sleutels en het uitschakelen van het alarm en de startonderbreker. Bij winkeldiefstallen worden stoorzenders gebruikt om detectiepoorten buiten werking te stellen. Bij zware overvallen en liquidaties wordt gebruikgemaakt van BlackBerry's met PGP (Pretty Good Privacy), een manier om afgeschermd te communiceren.

Digitalisering in de transportsector en in de Nederlandse havengebieden heeft ertoe geleid dat criminelen hun toevlucht zoeken tot nieuwe methoden om het logistieke proces te manipuleren. Dat is onder andere geconstateerd bij de cocaïnehandel en -smokkel en bij ladingdiefstal. Vroeger werden bijvoorbeeld vrachtbrieven en containerinformatie 'analoog' gestolen uit chauffeurscafés of verkocht door havenmedewerkers. Tegenwoordig is deze informatie steeds vaker alleen digitaal beschikbaar. Dat betekent dat criminelen toegang moeten krijgen tot de digitale systemen, hetzij door hacken hetzij door het omkopen van kantoorpersoneel of opsporingsambtenaren. Social engineering is hierbij een mogelijkheid voor criminelen om contacten te leggen. Langs deze weg kunnen ICT'ers bij havenbedrijven bijvoorbeeld benaderd worden via LinkedIn of Facebook.
Bedrijven in de transportsector maken steeds vaker gebruik van digitale vrachtuitwisselingssystemen. Deze systemen zijn niet altijd goed beveiligd. Er zijn tot nu toe enkele ladingdiefstallen gepleegd waarbij ze zijn misbruikt. Er zijn nog geen gevallen bekend waarbij ze zijn gehackt. Dit alles zal mogelijk veranderen als criminelen hun digitale vaardigheden verder ontwikkelen.

Slachtoffers van mensenhandel, kinderporno en diverse vormen van horizontale fraude (fraude met betaalmiddelen, fraude op online marktplaatsen, voorschotfraude en acquisitiefraude) worden benaderd en gerekruteerd via internet en sociale media. Katvangers worden gerekruteerd via online advertenties en sociale media, soms met een sollicitatiegesprek waaruit niet blijkt dat ze zullen gaan meewerken aan criminele activiteiten.

Identiteitsfraude is vaak een stap bij de uitvoering van andere (fraude)delicten en komt voor bij veel vormen van georganiseerde criminaliteit. Het betreft vooral het gebruik van valse namen, het gebruik van andermans rekeningnummer en de inzet van katvangers bij onder andere gebruikmaking van rechtspersonen. Als gevolg van de digitale ontwikkelingen nemen de mogelijkheden om identiteitsfraude te plegen toe. Veel mensen hebben online meerdere gebruikersprofielen. Al die accounts kunnen worden misbruikt. Dat steeds meer zaken op afstand geregeld worden, zonder dat iemand in persoon hoeft te verschijnen, vergroot de mogelijkheden voor identiteitsfraude eveneens. Identiteitsverificatie wordt hierdoor immers lastiger. Dit speelt bijvoorbeeld bij het aanvragen van financiële producten zoals verzekeringen, hypotheken en betaalrekeningen.

Ook bij de productie van illegale goederen worden digitale technologieën gebruikt. Zo worden met inkjetprinters valse eurobiljetten gemaakt en kunnen 3D-printers producten namaken (merkfraude) en vuurwapens fabriceren. In hoeverre dat de komende jaren daadwerkelijk zal gebeuren, is moeilijk in te schatten. Naar verwachting is er vanwege de lage productiekosten voorlopig voldoende aanbod van regulier geproduceerde namaakproducten.

De handel in illegale goederen en diensten op internet neemt toe, zowel op het darkweb als op het reguliere internet. Het betreft veelal de handel in drugs (voornamelijk synthetische drugs en cannabis), nagemaakte goederen of namaakgoederen, illegale vuurwapens, gestolen waar, vals geld, gestolen creditcardgegevens of kinderporno, mensenhandel of mensensmokkel. Bij deze handel wordt vaak gebruikgemaakt van cryptocurrency's, in het bijzonder van bitcoins. De versleutelingstechniek achter cryptocurrency's wordt blockchaintechnologie genoemd. Deze technologie controleert de echtheid van een virtuele munt en biedt koper en verkoper de mogelijkheid op een vertrouwde manier transacties te verrichten zonder tussenkomst van een derde vertrouwde partij.

De groeiende populariteit van het darkweb bij criminelen is vooral te danken aan de mogelijkheden die het biedt om anoniem te blijven. Het darkweb is onderdeel van het deepweb. Het deepweb is het deel van het internet dat niet door zoekmachines zoals Google geïndexeerd kan worden; hieronder vallen bijvoorbeeld ook intranetsites van reguliere bedrijven. Het darkweb bestaat uit darknets, netwerken waarbij communicatie in vertrouwen plaatsvindt. Het oorspronkelijke doel van het darkweb was het garanderen van vrijheid van meningsuiting voor hen die te maken hebben met censuur. TOR is het bekendste voorbeeld van een darknet. Andere voorbeelden zijn Freenet en Invisible Internet Project (I2P). TOR en andere darknets worden niet alleen gebruikt om censuur te vermijden, er worden ook criminele activiteiten op ontplooid. TOR lijkt daarbij volgens onderzoek van Europol vooralsnog verkozen te worden boven andere ondergrondse platforms en marktplaatsen. Dat wordt bevestigd in onderzoek van Van Remunt en Van Wilsem uit 2016. Volgens dat onderzoek groeit de populariteit van het TOR-netwerk nog steeds evenals de omvang van de geldtransacties die er plaatsvinden. Het gaat daarbij vooral om drugshandel. De mogelijkheid bestaat dat de drugshandel zich verplaatst van de fysieke wereld naar het digitale domein. Experts zijn het niet eens over de vraag in hoeverre en op welke termijn dat daadwerkelijk zal gebeuren. Aan de ene kant werkt het darkweb drempelverlagend en kan daar op een veilige en afgeschermde manier worden gehandeld, aan de andere kant wordt aangevoerd dat drugs en ook andere goederen in Nederland ook zonder darkweb gemakkelijk te verkrijgen zijn.

De technologische ontwikkelingen staan ondertussen niet stil. Volgens de rapportage van Trend Micro uit 2015 (Ciancaglini et al.) zullen criminelen meer investeren in het darkweb om nog anoniemer te kunnen communiceren en onvindbaar en ongrijpbaar te blijven voor opsporingsinstanties. Daarnaast worden er nieuwe gedecentraliseerde marktplaatsen verwacht die gebaseerd zijn op de blockchaintechnologie.

Ook bestaat het vermoeden dat er nog geavanceerdere diensten zullen komen die het traceren van cryptocurrency's en met name bitcoins (nog) moeilijker maken.

Het gebruik van cryptocurrency's wordt in toenemende mate gesignaleerd in witwasonderzoeken. Het zijn vooral bitcoins die de afgelopen jaren in beslag zijn genomen. Transacties met bitcoins kunnen relatief anoniem zijn, vooral wanneer gebruik wordt gemaakt van bitcoinmixers en (malafide) bitcoinexchangers om het virtuele geld om te zetten in traditionele betaalmiddelen. De afgelopen jaren is ook gebleken dat *payment service providers* (PSP's) gebruikt of zelfs opgezet worden om geld wit te wassen. Een PSP is een online-betaaldienstverlener die de betalingen bij zowel online als offline winkeliers kan afhandelen. Een PSP spaart vaak verschillende transacties op, waardoor het voor de bank moeilijker is een controle uit te voeren op verdachte transacties. Een PSP zelf blijkt hiertoe vaak ook niet in staat. Zo kan een PSP onbedoeld criminelen helpen bij het verhullen van de herkomst van geld.

Bij veel van de genoemde digitale ontwikkelingen gaat het om de afschermingsmogelijkheden door geavanceerde encryptietechnologieën waarmee financiële transacties, communicatie, identiteit en andere gegevens worden verhuld. Daarvoor worden ook bonafide diensten gebruikt zoals Dropbox, Pinterest, WhatsApp en Google docs. Deze diensten zijn aantrekkelijk, omdat verkeer van en naar deze diensten vaak standaard versleuteld wordt verstuurd en omdat communicatie met deze diensten op zichzelf niet verdacht is.

Jammers en opspoorapparatuur zijn offensieve methoden waarmee opnameapparatuur en bakens kunnen worden verstoord. Met opspoorapparatuur kunnen onder andere voertuigen en goederen worden 'gesweept', gecontroleerd op afluisterapparatuur. In verschillende deelonderzoeken voor dit dreigingsbeeld is dat geconstateerd. Bij kraken op geldautomaten sweepen daders hun voertuigen op bakens en bij heling zoeken ze op deze wijze naar track-and-tracetechnologie in gestolen partijen goederen om deze vervolgens onschadelijk te maken. Hennepplantages en drugslabs worden (tegen de politie en criminelen) beveiligd met behulp van digitale camera's, bewegingsmelders, opnameapparatuur en alarmsystemen.

2.3 Invloed op aard en omvang van criminaliteit

Bij meerdere criminele verschijnselen heeft de digitalisering invloed op de aard van de criminaliteit. Zo lijkt als gevolg van de digitale ontwikkelingen de ernst van enkele delicten toe te nemen, zien we soms nieuwe typen daders of dadergroepen en slachtoffers, en zijn er gevolgen voor de wijze waarop het logistieke proces georganiseerd is. In sommige gevallen leidt de digitalisering tot verandering in de criminele samenwerking. En bij enkele criminaliteitsvormen zien we door de digitale ontwikkelingen een toename in de omvang.

Door de geavanceerde afschermingsmogelijkheden die de digitale ontwikkelingen bieden, is het zicht op verschillende criminele verschijnselen minder geworden. Met een afnemend zicht kan de ernst van deze delicten toenemen. Dit komt sterk naar voren bij kinderpornografie: er lijkt tegenwoordig minder schroom te bestaan om ook de ernstiger vormen van misbruik te delen.
Ook fenomenen als sexting (het digitaal verspreiden of delen van seksueel getinte foto's) en *livestreaming* of 'live distant child abuse' nemen toe door deze digitale ontwikkelingen. Hierdoor worden meer – soms zeer jonge –kinderen slachtoffer van *sextortion* of seksueel misbruik. Sextortion is afpersing op internet met door sexting verkregen afbeeldingen of filmpjes. Vooral door sexting lopen Nederlandse kinderen een verhoogd risico slachtoffer te worden van sextortion of cyberpesten.

Doordat vooral jongeren zeer actief zijn op internet en er weinig moeite mee hebben om gevoelig (beeld)materiaal te delen, wordt een bredere groep jongeren kwetsbaar voor kinderporno en mensenhandel. Niet alleen het profiel van (potentiële) slachtoffers is aan veranderingen onderhevig, ook het profiel van afnemers verandert. Bij het aanschaffen van illegale of gestolen goederen of het inhuren van illegale diensten zijn het vooral online handelsplaatsen die drempelverlagend werken. Waren voorheen connecties nodig met criminelen, in de fysieke wereld, nu zijn die niet meer nodig.

Afgaand op (een weliswaar beperkt aantal) opsporingsonderzoeken kunnen we ons een beeld vormen van daders achter cybercrime. Afhankelijk van het type delict zien we verschillende soorten daders. Bij delicten waar financieel gewin centraal staat, zoals bij afpersing, verschillende fraudevormen en criminele activiteiten op de illegale markten, zijn het overwegend beroepscriminelen die de dienst uitmaken. Beroepscriminelen zijn agressiever en gaan sneller de directe confrontatie met slachtoffers aan dan andere categorieën daders, die met andere vormen van cybercrime geassocieerd worden, zoals hacktivisten, statelijke actoren en cybervandalen.
Over de wijze waarop daders met elkaar samenwerken, is weinig empirisch materiaal beschikbaar. In de samenwerking worden verschillende rollen onderscheiden: kernleden die het proces aansturen, facilitatoren, moneymules, programmeurs, techneuten, hackers, fraudeurs, (criminele) hosters en financieel ondersteuners. Soms wordt door dadergroepen samengewerkt langs hiërarchische lijnen en soms wordt samengewerkt in losse, tijdelijke, internationaal opererende samenwerkingsverbanden.

Bij sommige delicten verandert de criminele samenwerking als gevolg van de digitale ontwikkelingen. Dit is bijvoorbeeld het geval bij autodiefstal. De gebruikte digitale beveiligingsmethoden vereisen specialistische kennis en materiaal. De investering in kennis en materiaal is voor individuele daders te kostbaar; dadergroepen hebben meer financiële armslag. Bij kinderpornografie is er als gevolg van de groei van het internet en de toegenomen geavanceerde mogelijkheden meer dan voorheen sprake van clustering van gebruikers

in internationale kinderpornonetwerken. Deze clusters houden zich bezig met livestreaming van kindermisbruik of met chantage met seksueel beeldmateriaal.
In een aantal gevallen is gebleken dat er nieuwe daders en dadergroepen actief zijn geworden. Er zijn bijvoorbeeld particuliere, zelfstandig werkende producenten van synthetische drugs aangetroffen die hun producten uitsluitend via het darkweb verkopen. Overigens zijn er op het darkweb naast nieuwkomers ook veel oudgedienden te vinden: veel verkopers van drugs op het darkweb waren voorheen straatdealer.

De verplaatsing van de handel naar het darkweb kan gevolgen hebben voor de wijze waarop het logistieke proces georganiseerd is. Zo zou in veel gevallen de tussenhandel kunnen verdwijnen, omdat directe handel tussen producent en gebruiker makkelijker is geworden. Bij drugshandel waarbij een beroep moet worden gedaan op grootschalige internationale netwerken, zoals bij de handel in cocaïne en heroïne, ligt dit volgens de onderzoekers minder voor de hand. De kopers op het darkweb lijken in dit geval juist vaker de tussenhandelaars te zijn.

Aansluitend heeft de handel op het darkweb gevolgen voor de wijze waarop de illegale goederen worden vervoerd. Hoewel de smokkelwaar nog grotendeels in grotere partijen via de lucht, het water en de weg wordt getransporteerd, is er door de handel op *darkmarkets* een toename van het vervoer van kleinere partijen via post-, pakket- of koeriersdiensten.

De verplaatsing van handel naar internet betekent een sterkere marktwerking, waarin de klant een sterkere positie heeft. Daardoor krijgt hij betere waar voor zijn geld en verminderen de schadelijke gevolgen van drugs die via internet zijn aangeschaft. Drugsgebruikers wisselen op internet meer informatie uit over de kwaliteit van geleverde drugs en verantwoord drugsgebruik. Ook worden er drugstests aangeboden.
Uit het deelproject over mensensmokkel blijkt dat er door communicatie via sociale media een meer open markt ontstaat. Zo is er een betere informatie-uitwisseling over de geleverde diensten van mensensmokkelaars. Ook zijn irreguliere migranten door de informatie-uitwisseling in toenemende mate in staat zelfstandig te reizen. Wellicht wordt de rol van mensensmokkelaars daardoor minder groot. Een mogelijke keerzijde van de genoemde ontwikkeling is dat irreguliere migratie laagdrempeliger wordt.

Het is niet bekend in hoeverre de omvang van de georganiseerde criminaliteit stijgt door de toegenomen digitale mogelijkheden om illegale goederen en diensten af te zetten en criminele handelingen af te schermen. Of en in welke mate er sprake is van ‘slechts’ een verschuiving van criminele handel van het fysieke domein naar het digitale domein, is evenmin bekend. Dit komt doordat er weinig zicht is op de omvang van de illegale handel op internet en in het bijzonder op het darkweb.

In een aantal gevallen is de criminaliteit ten gevolge van de digitalisering in omvang toegenomen. Dat zien we vooral bij sterk gedigitaliseerde criminaliteitsvormen als kinderporno-

grafie en online gokken. Internet en de geavanceerde afschermingsmogelijkheden werken bij kinderpornografie drempelverlagend. Steeds meer mensen krijgen toegang tot internet, en dat geldt dus ook voor verspreiders van kinderpornografie en misbruikers. De digitale ontwikkeling vergroot ook het risico van online gokken, vooral doordat deze ontwikkeling het mogelijk heeft gemaakt wereldwijd te gokken. Door de opkomst van mobiele platforms zijn goksites bovendien makkelijk bereikbaar. Ook de opkomst van *e-sports*, het in competitieverband spelen van computergames, vergroot het risico: ook op deze competities kan gewed worden.

Bij horizontale en verticale fraude is weliswaar sprake van een relatief hoge mate van digitalisering, maar voor de komende jaren wordt bij meerdere vormen hiervan geen grote verschuiving in aard en omvang verwacht. Zo is fraude met online handel een gedigitaliseerde vorm van fraude die al jaren veelvuldig voorkomt en is voorschotfraude een gedigitaliseerde vorm die al jaren wat minder voorkomt. Er zijn binnen het digitale domein ook remmende factoren waardoor er geen grote verschuivingen optreden, zoals naar voren komt bij fraude met betaalmiddelen, acquisitiefraude en hypotheekfraude. Er is software ontwikkeld om (deze) fraudes te herkennen, onder meer door het mogelijk te maken verschillende systemen aan elkaar te koppelen (big data).
Bij merkfraude wordt echter een toename verwacht. Door het internet is de drempel verlaagd om namaakartikelen aan te bieden. Bovendien lijkt het normbesef bij burgers, vooral binnen het digitale domein, af te nemen en zijn deze goederen dus makkelijker af te zetten. Handhavingscapaciteit schiet al snel tekort om alle (illegale) transacties via internet te volgen.

Er wordt een toename verwacht van het aanbod van synthetische drugs op het darkweb, waardoor het makkelijker wordt deze aan te schaffen. Heling – en daarmee (deels) ook de daaraan voorafgaande vormen van diefstal – gedijt door de digitalisering: door het internet groeit de afzetmarkt, consumenten vragen zich niet altijd af wat de herkomst van een goed is. Ten aanzien van mensenhandel wordt verwacht dat het rekruteringsproces door digitale ontwikkelingen een groter bereik heeft en dat het gebruik van online diensten om mensenhandel te faciliteren verder zal toenemen.

Tot slot nog enkele opmerkingen over de dienstverleners. Zij faciliteren het gebruik van digitale technologie op verschillende manieren. De belangrijkste actoren zijn *hostingproviders.* Nagenoeg elke vorm van digitale criminaliteit heeft hosting nodig, en Nederland heeft een goede digitale infrastructuur en veel grote hostingproviders. Malafide onderaannemers faciliteren bewust criminele activiteiten door voor relatief hoge prijzen volledig *bulletproof*, dat wil zeggen anonieme, hosting aan te bieden. Daardoor hebben hostingproviders geen zicht op de daadwerkelijke gebruikers van hun infrastructuur. Dit komt niet vaak meer voor, omdat de onderaannemer hierdoor zelf strafbaar wordt. Wel bieden malafide hostingproviders hosting aan waarbij het toezicht door de overheid op subtielere manieren wordt tegengewerkt.

Een bijzondere vorm van dienstverlening wordt *Crime-as-a-Service* (CaaS) genoemd. Dankzij deze dienstverlening kunnen criminelen, zonder over bijzondere digitale vaardigheden of grondige technische kennis te beschikken, gebruikmaken van digitale instrumenten om cybercrime te plegen en anoniem te opereren op het darkweb en internet: met CaaS kunnen ze DDoS-aanvallen uitvoeren, ransomware verspreiden en gebruikmaken van Remote Access Tools (RAT's), waarmee ze op afstand computers kunnen beheren. Er zijn kant-en-klare softwarepakketten te koop waarmee het mogelijk is diverse vormen van cybercrime te plegen. Een voorbeeld zijn de zogenoemde *exploit kits* die kwetsbaarheden in computerprogramma's detecteren en vervolgens malware installeren.

2.4 Verwachtingen en gevolgen

2.4.1 Verwachtingen

De belangrijkste verwachtingen omtrent de toekomstige ontwikkelingen van cybercrime en gedigitaliseerde criminaliteit zijn gerelateerd aan het toenemende belang van internet in de samenleving. Internet speelt een steeds grotere rol in de wijze waarop delen van de samenleving op allerlei terreinen met elkaar verbonden zijn, bijvoorbeeld in maatschappelijk, economisch en technologisch opzicht. Huidige trends zoals het *Internet of Things* (IoT), *cloudcomputing* en de snelle opmars van mobiele internettechnologie zullen de komende jaren doorzetten, en daarmee zal internet nog belangrijker worden.

Met IoT wordt bedoeld dat steeds meer 'dingen', zoals apparaten, infrastructuur en voertuigen, via het internet worden verbonden en gegevens met elkaar kunnen uitwisselen. De verwachting is dat het in 2020 om bijna 21 miljard 'dingen' gaat: koelkasten, thermostaten, auto's, medische apparaten et cetera. De beveiliging van deze apparaten is vaak niet in orde, doordat deze niet geüpdatet wordt. Dat biedt mogelijkheden om de apparaten te hacken.
Meerdere malen is het security-onderzoekers en hackers gelukt verschillende merken auto's te hacken. Dat stelde hen er onder andere toe in staat het stuur en de remmen over te nemen. Ook is in het recente verleden een groot botnet van apparaten die 'deel uitmaken' van het IoT, gebruikt voor grootschalige DDoS-aanvallen. Daarbij werd een bedrijf getroffen dat belangrijk is voor toegang tot onder andere Twitter, Netflix en Spotify, met als gevolg dat velen tijdelijk geen gebruik konden maken van deze populaire diensten.
In hoeverre voertuigen en andere 'dingen' die verbonden zijn met het internet gehackt en gebruikt zullen worden door criminelen hangt af van de mate waarin er een economisch verdienmodel van gemaakt kan worden. Hierbij kan gedacht worden aan 'dingen' waaraan financiële transacties gekoppeld zijn en/of 'dingen' met een hoog afbreukrisico, waarbij blokkering van de ICT fatale gevolgen heeft. Bij een hoog afbreukrisico is het doelwit wellicht vatbaar voor afpersing. Doelwit kunnen eigenaren en producenten van gehackte voertuigen zijn, maar ook bijvoorbeeld ziekenhuizen, zoals al in paragraaf 2.2.1 is aangestipt.

Naast het IoT ontstaat de komende jaren ook een tendens waarbij mensen met het internet worden verbonden, bijvoorbeeld via implantaten. In dat verband wordt wel gesproken van het *Internet of People* (IoP). Een voorbeeld van zo'n 'menselijke connectie' met het internet is de pacemaker. In het IoP-tijdperk ontstaan in toenemende mate toepassingen die onze werkelijke wereld vermengen met een virtuele wereld en digitale informatie aan de werkelijke wereld toevoegen (*augmented* of *mixed reality*). Deze extra informatie kan worden getoond via een smartphone, tablet, *smart glasses* of *head-updisplay*. Volgens Europol kan dit het onderscheid tussen cyberaanvallen en fysieke aanvallen doen vervagen – met als gevolg fysiek letsel, maar mogelijk ook meer psychische schade.

De ontwikkelingen in de mobiele internettechnologie zijn de laatste jaren snel gegaan. Het smartphonebezit is toegenomen van 45 procent in 2011 naar 80 procent in 2015. Het merendeel van de smartphonefabrikanten gebruikt als besturingssysteem een eigen variant van Android; in 2016 had 80 procent van de verkochte smartphones Android als besturingssysteem. Omdat gebruikersgemak nogal eens de voorkeur krijgt boven beveiliging, actualiseren fabrikanten de besturingssystemen onvoldoende. Daardoor ontstaan beveiligingsrisico's. Criminelen spelen hierop in door in toenemende mate malafide apps te ontwikkelen, vooral op het vlak van *banking malware*. In 2015 maakte een grootschalig internationaal opsporingsonderzoek naar *mobile banking malware* duidelijk welke gelegenheid mobiele platforms bieden voor cybercrime. Bij dit onderzoek werd een belangrijk netwerk van cybercriminelen opgerold. Doordat ze de malware voortdurend aanpasten, wisten ze de beveiliging van de banken een aantal keren te omzeilen en een schade van minstens 2 miljoen euro te veroorzaken. Ze wasten het geld wit door middel van geldezels, die hun bankrekening tegen geringe betaling ter beschikking van de criminelen stelden. Minimaal 150 Nederlandse bedrijven en particulieren werden slachtoffer. Wereldwijd werden in totaal 60 verdachten aangehouden, van wie ongeveer 40 in Nederland. Ook een deel van de gebruikte infrastructuur stond in Nederland en werd ontmanteld.

Ondanks de toename van het smartphonebezit is het risico op malware op mobiele platforms relatief beperkt. Het verspreiden van malware op smartphones kost verhoudingsgewijs meer moeite en geld dan het verspreiden van malware op computers. Op traditionele computersystemen gebruiken mensen vaak één browser waarmee ze alle diensten raadplegen. Bij mobiele platforms gebeurt dit via afzonderlijke apps die allemaal verschillen qua ontwerp, protocollen en technieken. Om deze apps aan te vallen moet gerichte en dus dure malware worden ontwikkeld. Ook richt ransomware op smartphones waarschijnlijk minder schade aan dan op computers door de betere (automatische) back-upfuncties. Het aantal malafide apps zal door de toename van het smartphonebezit ongetwijfeld groeien, maar verwacht wordt dat computers voorlopig het belangrijkste doelwit blijven van cybercriminelen.

Een andere belangrijke ontwikkeling is cloudcomputing. De essentie hiervan is dat ICT-infrastructuren, platforms, softwarediensten en data niet langer lokaal op een eigen pc of server staan, maar via het internet worden gebruikt. Het beheer van de gegevens en de applicaties is uitbesteed aan een dienstverlener, en gegevens worden veelal verspreid over verschillende servers opgeslagen. Het werken in de cloud is een trend en zal naar verwachting de komende jaren toenemen. De cloud kent over het algemeen een goede beveiliging; in veel gevallen is hij beter beveiligd dan lokaal gebruikte computers van bijvoorbeeld kleine en middelgrote bedrijven. De toegangsbeveiliging is de laatste jaren verbeterd. Veel diensten in de cloud zijn overgegaan op een extra beveiligingslaag, de zogenoemde tweefactor-authenticatie. De komende jaren zullen meer diensten volgen. Desalniettemin blijven de toegang tot en de opslag van data bij clouddiensten risicovol, doordat deze beheerd worden door mensen. Die kunnen bedoeld of onbedoeld fouten maken in hun bedrijfsvoering, waardoor grote hoeveelheden data gestolen kunnen worden en in handen kunnen vallen van criminelen. Ook kan de cloud als instrument worden misbruikt bij het uitvoeren van cyberaanvallen. Bij misbruik van de cloud als instrument wordt de opslag- en rekencapaciteit ervan gebruikt voor het maken van botnets of voor het uitvoeren van grootschalige DDoS-aanvallen. Daarnaast kunnen clouddiensten een krachtig middel zijn voor de verspreiding van malware.
Als de cloud doelwit is van criminelen vanwege de schat aan informatie die hij herbergt, is het hun vaak te doen om het verkrijgen van financiële gegevens en identiteitsgegevens. Ze kunnen uit zijn op handel in data of op hacktivisme, maar ook op vernieling of verstoring door middel van DDoS-aanvallen of op afpersing door middel van ransomware en het dreigen met lekken van informatie.
Natuurlijk biedt de goede beveiliging van de cloud criminelen ook mogelijkheden om anoniem en niet-traceerbaar te communiceren. Daardoor is er steeds vaker geen aanwijsbare locatie waar de data zich bevinden – een uitdaging voor de opsporing, omdat de locatie zich dikwijls in het buitenland bevindt.
Transacties met cryptocurrency's (bitcoins) zijn openbaar en transparant, doordat ze direct tussen koper en verkoper plaatsvinden. Zoals eerder vermeld, is de technologie achter cryptocurrency's de blockchaintechnologie. Kort gezegd is een blockchain een openbaar en online register van transacties. Zo kan via de blockchain van de bitcoin nagegaan worden wie de eigenaar is en of de bitcoin niet twee keer wordt uitgegeven. Door het gebruik van geraffineerde online *mixtools* proberen criminelen de herkomst van bitcoins te verhullen. Vermoedelijk wordt het de komende jaren daardoor mogelijk bitcoins ontraceerbaar wit te wassen.

CaaS zal zich de komende jaren volgens het *Cybersecuritybeeld Nederland 2016* verder blijven ontwikkelen en professionaliseren. Cybercrime wordt niet alleen gefaciliteerd door aangeboden software en tools, er komen ook steeds meer handleidingen en zelfs helpdesks die criminelen kunnen raadplegen. Deze ontwikkelingen dragen bij aan een bredere beschikbaarheid van deze dienstverlening en dat zal het de komende jaren naar verwachting voor criminelen eenvoudiger maken om cybercrime en gedigitaliseerde criminaliteit te plegen.

Op het terrein van de cybersecurity werken veel publieke en private partijen samen om cybercrime tegen te gaan. Hun streven is de handen ineen te slaan en de Nederlandse samenleving weerbaarder te maken. Het Nationaal Cyber Security Centrum speelt daarin nu en de komende jaren een belangrijke rol. Digitale ontwikkelingen bieden ook kansen voor de opsporing, zoals slimme digitale camera's en digitale fraudedetectiesystemen, onder andere met de mogelijkheid verschillende systemen te koppelen (big data). Het gebruik van digitale technologieën door criminelen laat bovendien digitale sporen na die naar de daders kunnen leiden. De snelle opeenvolgende digitale ontwikkelingen maken het voor de opsporing noodzakelijk deze op de voet en adequaat te volgen.

2.4.2 Gevolgen

Het is niet bekend wat de totale omvang is van cybercriminaliteit in Nederland. Dat maakt het lastig om het geheel aan gevolgen voor de Nederlandse samenleving te beschrijven. Twee commerciële bedrijven, namelijk McAfee en Deloitte, hebben een poging gedaan en daaruit blijkt dat het (vermoedelijk) om aanzienlijke gevolgen gaat. De totale schade van cybercriminaliteit voor de Nederlandse economie schatten McAfee en Deloitte op respectievelijk 8,8 en 10 miljard euro, dat is om en nabij 1,5 procent van het bruto binnenlands product (bbp). In beide onderzoeken is gekeken naar zowel de directe als de indirecte kosten die het gevolg zijn van cybercriminaliteit. Directe kosten komen voort uit onder andere verlies van geld, verlies van waardevolle bedrijfsinformatie en onderbreking van de operationele continuïteit. Indirecte kosten komen voort uit de beveiligingsmaatregelen die getroffen worden tegen cybercriminaliteit en uit inbreuk op intellectueeleigendomsrechten.

Nederland heeft een relatief hoog geschat schadebedrag in vergelijking met andere landen. In het onderzoek van Deloitte wordt dat gerelativeerd: Nederland registreert in vergelijking met andere landen goed. De schade wordt door Deloitte verder genuanceerd als 'cost of doing business'. De digitalisering van onze samenleving brengt ook veel welvaart. In 2013 was het aandeel van de ICT-sector ruim 4 procent van het bbp. En de sector wordt steeds belangrijker voor de Nederlandse economie, met bovengemiddelde groeicijfers.

Cybercrime is een wijdverbreid probleem, dat qua aantallen slachtoffers volgens het Centraal Bureau voor de Statistiek (CBS) niet onderdoet voor vermogenscriminaliteit: in 2015 werden bij beide criminaliteitsvormen negentien slachtoffers geteld op elke honderd inwoners. De financiële schade voor burgers is in vergelijking met andere vormen van criminaliteit over het algemeen beperkt en wordt in veel gevallen (zoals bij fraude met internetbankieren en creditcardfraude) door de bank vergoed. De meeste schade komt volgens McAfee en Deloitte voor rekening van bedrijven en overheidsorganisaties. Slachtoffers kunnen ook last krijgen van psychische problemen, met soms fatale persoonlijke gevolgen, bijvoorbeeld als een slachtoffer zelfmoord pleegt. De ernst zal verschillen per type cybercrime. Bij een delict als afpersing is het risico op ernstige psychische schade groter dan bij fraude met internetbankieren.

Organisaties worden steeds vaker slachtoffer van cybercrime en het lijkt daarbij vaker te gaan om gerichte aanvallen. Volgens onderzoek van PwC uit 2014 is een op de vijf bedrijven in Nederland slachtoffer van cybercrime. Dat is minder dan bij andere vormen van economische criminaliteit, waar drie van de vier bedrijven slachtoffer worden. In dat onderzoek schatten respondenten ook de schade van cybercrime beduidend lager in dan die van andere vormen van economische criminaliteit. Recenter onderzoek van PwC uit 2016 in het Verenigd Koninkrijk heeft uitgewezen dat daar in vergelijking met 2014 een stijging is van het aantal bedrijven dat slachtoffer is geworden van cybercrime.[40] In Nederland is dat waarschijnlijk ook het geval.

Ook onderzoek van Veenstra, Zuurveen en Stol uit 2016 naar cybercrime bij bedrijven in het midden- en kleinbedrijf en bij zzp'ers geeft een wat genuanceerder beeld. Hoewel uit dit onderzoek naar voren komt dat bijna 30 procent van de onderzochte bedrijven en zzp'ers slachtoffer is geworden van een of meer vormen van cybercrime, rapporteert twee vijfde van de getroffenen dat zij geen schade hebben geleden. Bij de overige bedrijven is tijdverlies de meestgenoemde schadepost, gevolgd door financiële schade.

Hoewel middelgrote en kleine bedrijven volgens deskundigen kwetsbaar zijn, vanwege een relatief laag beveiligingsniveau in vergelijking met grotere bedrijven, blijkt dat niet direct uit eerdergenoemd onderzoek van PwC uit 2014. Uit dat onderzoek kwam naar voren dat de grootte van een organisatie niet van invloed is op de mate van slachtofferschap. Wel wordt vermoed dat middelgrote en kleine bedrijven en zzp'ers minder vaak aangifte doen dan grotere bedrijven.
Bij de overheid zijn vooral onderwijsinstellingen en zorginstellingen kwetsbaar vanwege de relatief zwakke ICT-voorzieningen. Scholen zijn vaak het doelwit van DDoS-aanvallen die door jongeren worden gepleegd; de schade van deze aanvallen bedraagt volgens berichten in de media miljoenen euro's. Ziekenhuizen zijn kwetsbaar vanwege het hoge afbreukrisico, mocht gedreigd worden het ziekenhuissysteem plat te leggen.

2.5 Conclusie

Internet en de bijbehorende digitale ontwikkelingen spelen een steeds grotere rol in de wijze waarop delen van de samenleving op allerlei terreinen met elkaar verbonden zijn. De afgelopen jaren volgden de ontwikkelingen elkaar snel op en de verwachting is dat dit de komende jaren niet anders zal zijn. De verbondenheid met internet in het dagelijks leven neemt de komende jaren verder toe. Bijna iedereen is in het bezit van een smartphone en maakt steeds meer gebruik van goed beveiligde diensten in de cloud en communiceert steeds anoniemer door sterk verbeterde encryptietechnieken. Deze diensten en technieken zijn voor iedereen toegankelijk en dragen bij aan een betere cybersecurity en een grotere weerbaarheid tegen cybercrime.

40 PwC (2016). *Global Economic Crime Survey 2016. Adjusting the lens on economic crime. Preparation brings opportunity back into focus*. Geraadpleegd op: http://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Dat heeft ook een andere kant: ook binnen het criminele domein zijn deze diensten en technieken laagdrempelig toegankelijk. Ze bieden criminelen goede afschermingsmogelijkheden, waarmee gegevens, identiteit, communicatie en financiële transacties succesvol kunnen worden verhuld voor opsporing en vervolging. Bovendien volgen veel personen en bedrijven de snelle digitale ontwikkelingen niet op de voet. Daardoor zijn ze kwetsbaar voor cybercrime en gedigitaliseerde criminaliteit. Dat biedt gelegenheden voor criminelen.

De digitale instrumenten en technieken die gebruikt worden bij cybercrime, worden in toenemende mate toegepast bij de traditionele vormen van georganiseerde criminaliteit die beschreven zijn in deel 2. De verweving tussen cybercrime en gedigitaliseerde criminaliteit wordt steeds sterker. Als deze ontwikkeling doorzet, zal er in de toekomst nauwelijks of geen onderscheid zijn tussen cybercrime en gedigitaliseerde criminaliteit. Het is dan een amalgaam van digitale middelen en vormen van criminaliteit om onder meer diefstal en fraude te plegen, mensen af te persen, te smokkelen en te rekruteren, en drugs en wapens te verkopen.

Op alle criminele markten hebben de digitale ontwikkelingen invloed op de aard van de criminaliteit. Dat is te zien aan de manier waarop tegenwoordig wordt samengewerkt: bij internationale kinderpornonetwerken bijvoorbeeld ontstaan clusters, en er is meer samenwerking bij autodiefstal. Via internet wordt het voor criminelen makkelijker om (internationaal) samen te werken, in veel gevallen anoniem. De invloed van de digitale ontwikkelingen manifesteert zich ook in de toename van individuele producenten van synthetische drugs die als zzp'er hun producten via het darkweb verkopen. Ook de logistiek verandert als gevolg van de digitale ontwikkelingen. Zo neemt door het darkweb de straathandel af en krijgt wie op het web drugs heeft gekocht, ze met de (pakket)post toegestuurd. In enkele gevallen hebben de ontwikkelingen een stimulerend effect op het criminele verschijnsel. Dat is vooral het geval bij sterk gedigitaliseerde criminaliteitsvormen zoals kinderporno en online gokken.

Hoewel een strikt onderscheid tussen de gevolgen van cybercrime en gedigitaliseerde criminaliteit niet te maken is, staat wel vast dat de gevolgen van cybercrime een wijdverbreid probleem vormen, waarvan burgers, bedrijven en overheidsorganisaties slachtoffer worden. De totale schade voor de Nederlandse economie die uit cybercriminaliteit voortvloeit, wordt door McAfee en Deloitte geschat op 8 à 10 miljard euro en dat bedrag zal naar verwachting hoger worden. De ICT-sector en digitale ontwikkelingen, vooral die op het internet, worden volgens het CBS van steeds groter belang voor de Nederlandse economie. Niet alleen economisch, ook persoonlijk en maatschappelijk worden we steeds afhankelijker van het internet. Door deze grotere afhankelijkheid wordt ook de impact van cybercrime op de samenleving groter. De meeste schade komt volgens McAfee en Deloitte voor rekening van bedrijven en overheidsorganisaties. De financiële schade voor burgers is vooralsnog relatief beperkt. Psychische schade kan in individuele gevallen ernstige en soms fatale persoonlijke gevolgen hebben. Alleen al door de groter wordende verbinding met internet in

het dagelijks leven neemt het risico op slachtofferschap toe. Daarnaast worden de persoonlijke gevolgen mogelijk ernstiger, doordat meer (beroeps)criminelen laagdrempelig gebruik kunnen maken van digitale technologieën. Deze criminelen gaan eerder de directe confrontatie met slachtoffers aan dan hacktivisten en cybervandalen.

Kortom, binnen het domein van georganiseerde criminaliteit zijn cybercrime en gedigitaliseerde criminaliteit vooral thema-overstijgende werkwijzen die van invloed zijn op de aard en omvang van meerdere criminele verschijnselen en een grote (financiële) impact hebben op de Nederlandse samenleving, nu en in de komende jaren. De wijdverspreide en groeiende invloed van de digitale ontwikkelingen op de georganiseerde criminaliteit vergroot de reikwijdte van criminelen en draagt bij aan de dreiging van georganiseerde criminaliteit in haar totaliteit.

3 Milieucriminaliteit

3.1 Inleiding

De basis voor dit hoofdstuk vormt het rapport *Dreigingsbeeld Milieucriminaliteit 2016*. In dat rapport wordt verslag gedaan van onderzoek naar milieucriminaliteit dat in de eerste helft van 2016 is uitgevoerd voor de Strategische Milieukamer (SMK). De SMK is een strategisch overleg waarin het openbaar bestuur, het Openbaar Ministerie, landelijke inspecties en de politie vertegenwoordigd zijn en waarin het strategisch beleid bepaald wordt ten aanzien van de aanpak van milieucriminaliteit.
De auteurs van het *Dreigingsbeeld Milieucriminaliteit 2016* zijn Rudie Neve, Monique van Doorn, Debbie Mac Gillavry, Nanina van Zanden (politie), Bart Fortuin (NVWA-IOD), Michiel In 't Veld (Politieacademie) en Armand Stokman (ILT-IOD). De bronnen die zij bij hun onderzoek hebben gebruikt, staan vermeld in het digitale *Bronnenboek NDB2017.*

Zoals in de algemene inleiding op dit deel is toegelicht, is bij het onderzoek naar milieucriminaliteit gekozen voor een andere benadering dan bij de criminele verschijnselen die in deel 2 besproken zijn en is afgezien van het toewerken naar een kwalificatie van dreiging. In plaats daarvan is het onderzoek vooral gericht op het achterhalen van de gelegenheden voor criminaliteit in een select aantal milieudomeinen. Het gaat om gelegenheden voor criminaliteit (in branches die actief zijn) in de volgende domeinen: (1) de afval- en reststromen, (2) de bodemketen en het oppervlaktewater en (3) de gevaarlijke stoffen. Deze domeinen zijn niet willekeurig gekozen. Ze zijn gekozen omdat de Strategische Milieukamer en de instanties die bij het toezicht op de naleving van milieuwetgeving betrokken zijn, de gedeelde perceptie hebben dat zich hier qua milieucriminaliteit of gevolgen belangwekkende ontwikkelingen voordoen of zullen gaan voordoen. De keuze voor onderzoek binnen deze drie domeinen betekent dat een beperkt deel van de milieucriminaliteit in beeld wordt gebracht. Andere domeinen, waar andere vormen van milieucriminaliteit voorkomen, zoals de illegale handel in beschermde dier- en plantensoorten, blijven hier buiten beschouwing.

Binnen de drie aangemerkte domeinen zijn acht vormen van milieucriminaliteit onderscheiden die aan nader onderzoek zijn onderworpen.

In het domein van de *afval- en reststromen* gaat het om onderzoek naar criminaliteit of gelegenheden daarvoor bij:

1. de export van afvalstoffen;
2. de sloop, het transport en het storten van asbest;
3. het *blenden* van stookolie;
4. de verwerking van reststromen.

In het domein van de *bodemketen en het oppervlaktewater* gaat het om onderzoek naar criminaliteit of gelegenheden daarvoor bij:

5. activiteiten in de grondstromen;
6. de mestverwerking.

In het domein van de omgang met *gevaarlijke stoffen* gaat het om onderzoek naar criminaliteit of gelegenheden daarvoor bij:

7. het transport van gevaarlijke stoffen in het binnenlands wegvervoer;
8. het werken met gevaarlijke stoffen door risicobedrijven.

De voornaamste bevindingen over deze acht vormen van milieucriminaliteit worden in dit hoofdstuk besproken.
Kort samengevat vinden we gelegenheden voor criminaliteit die volop worden benut, onder andere in de manier waarop bedrijven en ketens in het milieudomein georganiseerd zijn en de manier waarop zij 'gewend' zijn te werken. Gelegenheden zijn er ook door de manier waarop (specialistische) handhavings- en opsporingsdiensten georganiseerd zijn, samenwerken, omgaan met (complexe) wet- en regelgeving en hun taken uitvoeren.
Niet alleen gelegenheden voor criminaliteit komen in dit hoofdstuk aan de orde, ook schenken we aandacht aan de aard en omvang van milieucriminaliteit. Informatie daarover beperkt zich echter vaak tot casuïstiek op basis van een paar opsporingsonderzoeken of enkele incidentregistraties. Al met al is er weinig concreets bekend. In het bijzonder geldt dat voor de gevolgen van milieucriminaliteit. Die worden vaak beschreven in termen van 'wat zou kunnen gebeuren'. De daadwerkelijke schade die milieucriminaliteit aanricht, is meestal onbekend, doordat deze vaak pas na vele jaren of na talrijke geconstateerde incidenten zichtbaar wordt. In dit hoofdstuk worden de mogelijke gevolgen en eventuele schade daarom kort besproken voor het hele domein van milieucriminaliteit en niet voor de acht onderzochte criminaliteitsvormen afzonderlijk.
Met het onderzoek naar de acht genoemde vormen van milieucriminaliteit wordt beoogd een bijdrage te leveren aan de onderbouwing van de beleidskeuzes van de SMK.

3.2 Afval- en reststromen

Export van afvalstoffen

Afval is materiaal waarvan de houder zich 'ontdoet, wil ontdoen of moet ontdoen', volgens de definitie in de Wet milieubeheer. Het is het residu van een groot aantal verschillende productie- en consumptieketens. De laatste jaren is het beleid erop gericht om uit afvalstoffen zo veel mogelijk grondstoffen terug te winnen die gebruikt kunnen worden bij het fabriceren van nieuwe producten. Die ontwikkeling wordt ook wel aangeduid als de 'circulaire economie'. Er zijn de afgelopen jaren internationale afvalstromen ontstaan door de grote behoefte aan grondstoffen voor zich ontwikkelende economieën, zoals China, en onder invloed van internationale verschillen in wet- en regelgeving omtrent de verwerking van afval. Afval is een exportproduct geworden. Als verantwoorde verwerking van afval in Nederland duur of ingewikkeld is, wordt er in het buitenland gezocht naar goedkopere of laagdrempeliger verwerkingsmogelijkheden.
Het verwerken van afval voor hergebruik en het verwerken van niet-herbruikbaar afval kost 'ontdoeners' geld. Ontdoeners zijn bedrijven waar het afval ontstaat en die er mede voor moeten zorgen dat afvalverwerking op verantwoorde wijze plaatsvindt. Andere partijen kunnen weer verdienen aan het afvoeren van afval: afvalinzamelaars, handelaars, inkopers, transporteurs, exporteurs, expediteurs en dienstverleners.

Soms gebruiken de partijen in de afvalketen illegale methoden om kosten voor afvalverwerking te drukken of er geld aan te verdienen. Daarbij kan bijvoorbeeld gedacht worden aan lekkage van afval uit legale afval- of recyclingketens naar het illegale circuit door ontdoeners van *e-waste* en kunststof- en metaalafval. Ontdoeners sparen de kosten voor juiste afvalverwerking uit, en afvalstoffen worden op onverantwoorde wijze verwerkt.
In alle schakels van de afvalketen zien we handelaars, inkopers, transporteurs, exporteurs, expediteurs en andere dienstverleners die op illegale wijze geld verdienen aan afval. Uit casuïstiek blijkt dat deze partijen miljoenen kunnen verdienen: in 10 van 23 onderzochte casussen bedraagt het wederrechtelijk verkregen voordeel meer dan een miljoen euro.
Enkele activiteiten waarmee de partijen in de afvalketen illegaal geld verdienen, sommen we hier summier op; ze zijn al in eerdere rapportages (onder andere die ten behoeve van het NDB2008 en het NDB2012) aan bod gekomen, maar zijn nog steeds actueel. Exporterende handelaars mengen kleine partijen e-waste van (kleine) inzamelaars om verontreinigde partijen te verhullen en plegen daarbij valsheid in geschrifte. Inkopers uit Afrika en China versturen vanuit Nederland containers met afval naar opdrachtgevers in het bestemmingsland, terwijl de papieren niet in orde zijn of de lading niet correspondeert met de vrachtbrieven. Transporteurs van illegale afvalzendingen stellen geen vragen over de lading, omdat ze eraan verdienen. Exporteurs maken illegaal transport van verontreinigde afvalstoffen naar China mogelijk door Hongkong als bestemming op de ladingsdocumenten in te vullen, terwijl de werkelijke eindbestemming ergens anders in China is.
Bij de illegale export van afvalstoffen valt vooral de rol van expediteurs op. Vaak zijn zij gecertificeerd en worden ze daarom niet meer door de douane gecontroleerd.

Malafide expediteurs zorgen ervoor dat de vrachtdocumenten en douaneaangiften 'kloppen' en verschuilen zich achter de opdrachtgever die verantwoordelijk is voor het aanleveren van de juiste informatie.
Dienstverleners, zoals advies- en analysebureaus, maken soms 'meetfouten' in het voordeel van de klant. Belangenverstrengeling doet zich voor als deze bureaus ingehuurd worden zowel voor de aanvraag van vergunningen als voor het voorbereiden van de toekenning daarvan door het bevoegd gezag.

Bij de export van goederen in tal van afvalstromen rijst steeds vaker de vraag of het om afvalstoffen dan wel om herbruikbare of tweedehands goederen gaat. Is een partij afgedankte huishoudelijke apparaten nu een partij afvalstof of een partij tweedehands apparaten? Daardoor kan het voorkomen dat stoffen die het milieu schaden uiteindelijk toch als niet-afvalstof geëxporteerd worden; verwerkers in de afvalbranche maken gebruik van de onduidelijkheden in de complexe wet- en regelgeving door goederen te exporteren waarvan niet meteen duidelijk is of ze zijn aan te merken als afvalstoffen of als tweedehands goederen.

Over de omvang van de illegale export van afvalstoffen is weinig bekend. Vanuit Nederlandse havens wordt ongeveer 12,5 miljoen ton aan afvalstoffen verscheept naar bestemmingen in vooral Afrika en Zuidoost-Azië. Daar is de vraag naar afvalstoffen groot, de verwerking van afval relatief goedkoop en de regelgeving omtrent afvalverwerking minder streng dan in Europa. Een onbekend deel van de export van afval is illegaal: het gaat naar landen waar het niet heen mag of het is gevaarlijker dan wordt voorgewend. Door de douane, en in mindere mate de politie, worden jaarlijks enige duizenden controles uitgevoerd op een fractie van alle containers die vanuit of via Nederland de grens van de Europese Unie overgaan. Het percentage waarbij overtredingen worden geconstateerd verschilt per afvalstroom, maar ligt gemiddeld op ongeveer 10 procent. Bij een klein deel van de overtredingen wordt strafrechtelijk onderzoek ingesteld. Sinds 2012 zijn negentien gevallen bekend waar overtreding van de Europese Verordening Overbrenging Afvalstoffen (EVOA) het hoofdbestanddeel vormt, tegenover vijftien gevallen in de periode 2008-2011.

Sloop, transport en storten van asbest

Tot aan 1994 zijn gedurende enkele decennia asbesthoudende materialen gebruikt in de bouw. Toen bekend werd dat asbest kan leiden tot verschillende vormen van kanker, is het gebruik ervan verboden. In de huidige asbestketen mogen alleen gecertificeerde bedrijven zich bezighouden met de inventarisatie, sloop en verwijdering ervan. De asbestbranche kent verschillende wetten en regels die nageleefd moeten worden. In de praktijk blijkt dat in de hele branche regelovertredend gedrag plaatsvindt, zoals het niet juist verwijderen van asbest of het illegaal storten ervan. Vaak is het juridisch lastig aan te tonen dat iemand met opzet op illegale wijze asbest heeft verwerkt; tegen de tijd dat er een strafrechtelijk onderzoek kan worden gestart, is het asbest vaak verdwenen.

De afgelopen jaren zijn er minder strafrechtelijke onderzoeken gedaan naar illegale asbestverwerking. Er is meer nadruk komen te liggen op bestuurlijk handhaven.

Binnen de asbestbranche is een onbekend aantal malafide asbestverwijderaars actief, ook wel aangeduid als *free riders.* Dat zijn bedrijven of personen die asbest verwijderen zonder te voldoen aan de wettelijke meldingsplicht en zonder gecertificeerd te zijn. Een aantal van hen bieden zich aan via sites zoals Marktplaats.nl. Ook zien we bedrijven die meerdere schakels in de asbestketen in handen hebben, wat het toezicht bemoeilijkt. Het gaat onder andere om grote aannemers- en sloopbedrijven en om asbestinventarisatiebureaus en laboratoria.
Bedrijven die meerdere schakels in de asbestketen in handen hebben, werken soms met 'ontwijkconstructies'. Anticiperend op ontdekking van hun illegale praktijken door inspecties en handhavingsdiensten richten zij meerdere rechtspersonen op en werken ze met dubbele certificaten. Als het certificaat van het ene bedrijf wordt ingetrokken, werken ze verder vanuit een ander bedrijf. Ook blijkt dat bedrijven soms elkaars certificaten voor asbestsaneringen gebruiken als het certificaat van een van de bedrijven is ingetrokken. De saneringen worden dan uitgevoerd onder de naam van een ander, wel gecertificeerd asbestsaneringsbedrijf.
Soms sjoemelen asbestverwijderaars met de classificering van het risico van asbestverwijdering. Hoe hoger de risicoklasse, des te meer maatregelen getroffen moeten worden en des te duurder het is om asbest te verwijderen. Door de classificering te hoog in te schatten kan een saneerder de klant te veel laten betalen. Omgekeerd blijkt uit casuïstiek dat sommige asbestverwijderaars bij de aanbesteding zeggen dat het om een lagere klasse gaat, die vervolgens op basis van 'nieuwe inzichten' wordt verhoogd als de werkzaamheden zijn begonnen, zodat de opdrachtgever extra moet betalen.
Manieren om het asbestprotocol in zijn geheel te vermijden zijn er ook. Uit casuïstiek blijkt dat sommige sloopbedrijven die met asbest mogen werken, valse monsters bij laboratoria aanleveren om ervoor te zorgen dat slooplocaties asbestvrij worden verklaard. Zo kan de sloop zonder vergunning – en dus goedkoper – worden uitgevoerd.
Ook kunnen laboratoria of adviesbureaus, in opdracht van asbestsaneerders, op allerlei manieren monsteruitslagen of adviezen manipuleren, waardoor het op papier lijkt alsof de saneerder zich aan de regels houdt. Door dergelijke malversaties worden medewerkers van asbestsaneerders soms onwetend en onbeschermd ingezet bij asbestverwijdering.
Verwijderde asbest wordt regelmatig illegaal gestort om kosten en moeite voor juiste verwerking uit te sparen. Uit diverse signalen blijkt dat het illegaal wordt gestort op dezelfde (bedrijfs)terreinen als waar het verwijderd is en op terreinen van asbestverwijderaars.

Sinds 1993 is de asbestbranche geprivatiseerd. In Nederland geven zes certificerende en keurende instellingen certificaten af voor het uitvoeren van asbestsanering door bedrijven in deze branche. Op deze instellingen wordt toegezien door de Inspectie Sociale Zaken en Werkgelegenheid (ISZW). Er bestaat bij inspecties zorg over deze vorm van zelfregulering in de asbestbranche. De certificerende en keurende instellingen moeten met elkaar concurreren om de gunst van de asbestsaneerders, hun 'klanten'. Ze staan dus onder druk om certificaten uit te geven onder eenvoudige condities en zijn weinig geneigd om een certificaat in te trekken als de saneerder zich niet aan de voorwaarden houdt. Dan raken ze immers klanten en dus inkomsten kwijt. Ook is vastgesteld dat de condities in de certificering niet altijd overeenstemmen met de wet- en regelgeving. Aangescherpte regelgeving in 2014 is slechts ten dele in de certificeringsvoorwaarden opgenomen. Deze gang van zaken bij de certificering creëert dus eveneens gelegenheden voor asbestcriminaliteit.

Over de omvang van de malversaties met asbest is weinig bekend. Enig inzicht verkrijgen we als we afgaan op cijfers van saneringsmeldingen (die wettelijk verplicht zijn) en de inspecties die naar aanleiding daarvan zijn uitgevoerd. In 2014 werden op 64.000 saneringsmeldingen 240 inspecties uitgevoerd op locaties waar een verhoogd risico was ingeschat. Daaruit blijkt dat 46 procent van de saneringslocaties niet in orde was. Dat betekent een verbetering ten opzichte van 2012, toen 70 procent niet in orde was. Uiteraard zeggen deze cijfers niet alles over de regelnaleving in de hele branche, maar ze laten wel zien dat overtredingen geregeld voorkomen. De meest voorkomende (asbestgerelateerde) overtredingen zijn het niet nemen van doeltreffende en noodzakelijke maatregelen bij verwachte overschrijding van grenswaarden en het ontbreken van een correct werkplan, een doelmatige wasgelegenheid en doucheruimten. Bij de politie komen jaarlijks enkele tientallen asbestgerelateerde signalen binnen van valsheid in geschrifte, dumpingen en illegale saneringen.

Vanaf 2024 mogen er in Nederland geen asbestdaken meer zijn. Omdat er op dit moment te weinig gecertificeerde asbestverwijderingsbedrijven zijn om alle asbestdaken voor die tijd te slopen, wordt een toename in het aantal free riders verwacht, die gepaard zal gaan met een toename in het aantal illegale saneringen. Ook wordt misbruik verwacht van subsidieregelingen van de overheid om asbest op een juiste manier af te voeren. De plafonds aan de subsidie en de deadlines die in het landelijk asbestbeleid gesteld worden, zullen de druk op particulieren, bedrijven en (overheids)instellingen om zich van asbest te ontdoen, verhogen. Dat werkt malversaties bij de verwerking van asbest in de hand. Begin 2012 is de vergunningsplicht voor het slopen van een gebouw met asbest gewijzigd in een meldingsplicht. Daardoor hebben gemeenten minder opbrengsten uit leges. Dat betekent minder geld voor toezicht en handhaving en ook dat kan zijn weerslag hebben op de ontwikkeling van asbestgerelateerde criminaliteit.

Blenden van stookolie

Recente opsporingsonderzoeken laten zien dat voor de illegale productie van stookolie niet alleen oliehoudend afval wordt gebruikt: ook chemisch afval wordt illegaal aangeleverd, ingezameld en geblend. Op die manier ontlopen ontdoeners de kosten die aan de verwerking van chemisch afval verbonden zijn en kunnen inzamelaars of bewerkers dit afval te gelde maken onder het motto 'mengen is verdienen'. Chemisch afval verdwijnt dus niet van de markt maar wordt als 'product' verhandeld en uiteindelijk opgestookt. Waarschijnlijk veroorzaakt niet (geheel) verbrand chemisch afval gevaarlijke emissies en brengt het schade toe aan de volksgezondheid en het milieu. Onbekend is in welke mate de uitstoot van stookolie met oliehoudend en chemisch afval vervuilender is dan de reguliere uitstoot van stookolie.

Ook is onbekend op welke schaal het illegaal blenden van stookolie plaatsvindt. In de Rotterdamse haven bunkeren jaarlijks 20.000 schepen tezamen ongeveer 11 miljoen kubieke meter stookolie. Daarmee staat Rotterdam mondiaal in de top 3 van bunkerhavens. Geraffineerde aardolieproducten (waaronder stookolie) vormen voor Nederland met afstand de grootste groep 'uitgevoerde goederen', met een geschatte exportwaarde van 38 miljard euro. Door het illegaal gebruik van oliehoudend en chemisch afval als bewerkingsmiddel voor stookolie wordt in Nederland per geproduceerde ton naar schatting tussen de 180 en 470 euro winst gemaakt. Volgens experts wordt minstens 10 procent van de stookolie op deze manier geproduceerd. Uitgaande van dit percentage kunnen we berekenen dat er op jaarbasis een illegale winst van tussen de 225 en 610 miljoen euro wordt gemaakt. Dat is exclusief de 'winst' die het resultaat is van het uitsparen van afvalverwerkingskosten. Met het illegaal blenden van stookolie wordt dus veel geld verdiend.

Opgemerkt zij dat chemisch afval niet alleen bij het blenden van stookolie wordt gebruikt: er zijn aanwijzingen dat het onbewerkt ook in andere brandstofcomponenten wordt weggemengd, zoals in benzine en diesels. Op welke schaal dat gebeurt, is onbekend. De gemengde benzine en diesel zijn veelal bestemd voor Afrika en Azië. Experts hebben de indruk dat er vanuit Afrika en Azië sprake is van toenemende vraag naar brandstoffen. Daardoor kunnen illegale wegmengingen zich verder uitbreiden.

De criminele activiteiten die met de handel in stookolie gepaard gaan, betreffen niet alleen het rechtstreeks wegmengen van afvalstoffen, maar onder andere ook het frauderen met productregistraties van chemische stoffen in administraties en vervoersdocumenten en het sjoemelen met de meldingsplicht voor afvaltransport.

Ook de organisatie en bedrijfsvoering van de stookoliebranche bieden gelegenheden voor criminaliteit. Zulke gelegenheden zien we bijvoorbeeld in de manier waarop de partijen in de stookoliebranche gewend zijn te werken. Olieafvalinzamelaars krijgen doorgaans betaald voordat zij het afval verwerken. Dit nodigt uit tot onverantwoorde verwerking.

Bovendien percipieert een deel van de branche het illegaal wegwerken van afvalstoffen niet als 'zwaar crimineel gedrag'. Het wordt meer gezien als snel en slim inspelen op de wens van ontdoeners en voldoen aan de vraag naar stookolie door bunkersuppliers.
De verschillende schakels, zoals ontdoeners, inzamelaars en transportbedrijven, zijn steeds vaker internationaal actief. Het zicht op die internationale activiteiten wordt belemmerd doordat internationale afvalstromen in de stookolieketen complexe en tijdrovende controles vergen. Ook door schaalvergroting in de branche is toezicht lastig. Er zijn grote olieconcerns die zich in verschillende Europese landen vestigen. Deze bedrijven beslaan nagenoeg de gehele stookolieketen en zijn tegelijkertijd inzamelaar, bewerker, opslag- en distributiepunt en bunkersupplier.
De brancheonderdelen zijn onderling sterk verweven. Veel inzamelaars, bewerkers en verwerkers van afvalolie zijn jarenlang actief en administratief of bestuurlijk met elkaar verbonden. Dat kan resulteren in een collectief wegkijken bij malversaties in de bedrijfsvoering.

Aan de kant van toezichthouders en handhavers zien we dat vergunningverleners, zoals provincies en gemeenten, soms de kennis ontberen om een vergunningsaanvraag goed te beoordelen. Daardoor kunnen bijvoorbeeld malafide inzamelaars en bewerkers van afvalstoffen en oliën in de stookolieketen werken. Bij politie en douane is te weinig chemische kennis aanwezig om alle daarvoor in aanmerking komende weg- en zeetransporten als verdacht aan te merken. Illegale transporten vinden daardoor ongehinderd doorgang. Inspecteurs en bijzondere opsporingsambtenaren komen soms kennis en expertise tekort om afvalsoorten te beoordelen. Daardoor blijven bepaalde illegale mengingen plaatsvinden. Het toezicht op de stookolieketen en het toezicht op de naleving van milieuvergunningen, bijvoorbeeld van inzamelaars en bewerkers, is sterk gefragmenteerd. Het is verdeeld over verschillende omgevingsdiensten en de Inspectie Leefomgeving en Transport (ILT). Omgevingsdiensten zijn regionale uitvoeringsdiensten die vaak in opdracht van en namens (lokale) overheden toezien op de naleving van wet- en regelgeving in het milieudomein. Deze diensten zijn voor een adequaat toezicht en slagvaardige handhaving afhankelijk van de politie, bijvoorbeeld bij wegcontroles van (tank)transporten, en van de douane, bij controles op de import en export van goederen. Het ontbreekt deze diensten dikwijls aan voldoende kennis en apparatuur om de meer gecompliceerde controles uit te voeren. De omvang van de stromen leidt ertoe dat handhavings- en opsporingsdiensten onmogelijk alle vervoersstromen van de stookolieketen kunnen controleren. De wet- en regelgeving is complex en wordt in de praktijk niet altijd juist of adequaat toegepast.
Ten slotte onttrekt een deel van de stookolieketen zich letterlijk aan het zicht van overheidsdiensten: voor 90 procent van het zeeoppervlak bestaat geen regelgeving. Daar wordt niet gecontroleerd. Dat biedt ruime mogelijkheden om ongezien scheepsafval te lozen en stookolie te gebruiken die ernstig vervuild is. Dat houdt de illegale markt voor het verwerken van afvalstoffen in stookolie in stand.

Al met al bestaan er veel gelegenheden voor het plegen van criminele activiteiten door de manier waarop het toezicht op de stookolieketen georganiseerd is en functioneert, terwijl de strafrechtelijke aanpak van het illegaal blenden van stookolie, die zich niet zelden over meerdere landen uitstrekt, complex is.

Verwerking van reststromen

In elke industrie ontstaan naast de beoogde eindproducten ook bijproducten. Het gaat bijvoorbeeld om botten en huiden uit slachterijen, bietenpulp en schadepartijen levensmiddelen. Heeft het bijproduct nog dusdanige kwaliteit dat het kan worden hergebruikt, dan is het een reststroom, anders is het afval. Reststromen zijn economisch interessant, er kan geld aan worden verdiend. Afvalstromen daarentegen kosten alleen maar geld.
Ontdoeners en handelaars hebben er baat bij een partij restgoederen voor een zo hoog mogelijke prijs te verkopen. Reststromen die hergebruikt kunnen worden in voedingsmiddelen (*food*) leveren het meeste op, gevolgd door diervoeders (*feed*), energietoepassingen (zoals covergisting) en technische toepassingen (bijvoorbeeld verwerking in plastic). Dit verdienmodel voor reststromen brengt met zich mee dat er ook wordt gefraudeerd met de identiteit ervan. Reststromen worden dan bewust opgewaardeerd: een reststroom die 'slechts' gebruikt mag worden voor covergisting, bietenpulp bijvoorbeeld, wordt verkocht als bruikbaar voor de productie van diervoeder. Op deze manier wordt er meer geld verdiend. Deze fraude kan schade toebrengen aan de volksgezondheid, de gezondheid van dieren en het milieu.

De markt voor reststromen kan worden aangemerkt als een criminogene markt. Dat komt, kort gezegd, door de complexe (verschillen in) wet- en regelgeving, de grote diversiteit aan reststromen, het internationale karakter van de markt en het feit dat het toezicht belegd is bij meerdere overheidsdiensten. Hierdoor ontstaat ruimte voor gesjoemel. We bespreken een aantal van deze factoren.

Door globalisering van voedselketens groeit ook de internationale handel in reststromen. Handelaars kunnen steeds eenvoudiger ergens ter wereld een gaatje vinden voor de afzet van hun reststromen. Doordat internationale wet- en regelgeving moeite heeft de globale markt bij te benen, blijft fraude bij de afzet vaak onopgemerkt en onbestraft.
Op het speelveld van internationale rest- en afvalstromen is toezicht en handhaving niet eenvoudig. Elke rest- en afvalstroom kent eigen complexe wet- en regelgeving. Die is niet altijd eenduidig, waardoor verschillende interpretaties mogelijk zijn.
Bij bedrijven die in meerdere rest- en afvalstromen handelen, verloopt de toepassing en handhaving van (internationale) wet- en regelgeving soms moeizaam. Dat komt doordat toezicht- en handhavingsdiensten, afhankelijk van de reststroom, ieder een deel van het toezicht op zich nemen en weinig informatie uitwisselen. Daardoor ontbreekt een totaalzicht op de handel en wandel van een bedrijf.

De omvang van de reststromen, het relatief beperkte toezicht – overwegend in de vorm van documentcontroles – en de vele schakels in de internationale reststroomketen bemoeilijken de traceerbaarheid van malversaties in de reststroomketen. Daarnaast zijn er relatief veel momenten waarop reststromen kunnen worden opgewaardeerd. Dit maakt de controle van bedrijven in de reststroomketen lastig. Vaak vindt controle risicogericht plaats.

De keten van reststromen bestaat uit producenten (van reststromen), handelaars, opslagbedrijven, inzamelaars, transporteurs, afnemers, laboratoria (die de bestemming van de reststroom kunnen vaststellen) en schoningsbedrijven (die reststromen kunnen opknappen). In deze keten manifesteert criminaliteit zich op een aantal manieren. Zo kan er sprake zijn van fysiek en administratief opwaarderen.
Van fysiek opwaarderen is sprake als een partij met een te hoog gehalte ongewenste stof wordt vermengd met een schone partij, waarbij het gehalte van de totale gemengde partij net onder de norm blijft. Dit gebeurt vooral bij bedrijven waar meerdere rest- en afvalstromen bij elkaar komen. Deze bedrijven maken gebruik van hiaten in de wetgeving om financieel voordeel te behalen. Zo ontvangt de Nederlandse Voedsel- en Warenautoriteit (NVWA) signalen dat soms partijen dierlijke vetten en oliën (als bijproduct uit de vleesindustrie) worden opgewaardeerd. Op welke schaal dit gebeurt, is onbekend. In eerdere zaken kwamen opgewaardeerde afvalstromen in diervoeder terecht die antibiotica en de kankerverwekkende stof aflatoxine bevatten.
Ook schoningsbedrijven vormen een risico als het gaat om het fysiek opwaarderen van reststromen. Het is niet altijd duidelijk of partijen daadwerkelijk vernietigd of geschoond worden dan wel zonder behandeling weer op de markt worden gebracht. Verder zijn er aanwijzingen dat de covergistingsbranche vatbaar is voor het illegaal wegwerken van afval.
Van administratief opwaarderen is sprake als een reststroom op papier een andere identiteit krijgt (omkatten). Dit kan onder andere door officiële documenten (zoals facturen of certificaten) te vervalsen of door te frauderen met laboratoriummonsters. Volgens de NVWA komt fraude met laboratoriummonsters inderdaad voor, al is onbekend op welke schaal. Er zijn bedrijven met vestigingen in meerdere landen die afval naar een buitenlandse vestiging sturen en daarna dezelfde partij onbewerkt terugontvangen als grondstof voor bijvoorbeeld diervoeders. Deze voorbeelden maken duidelijk dat frauderen met administraties loont. Regulier toezicht bestaat vaak alleen uit controles op de administratie (documentcontroles bijvoorbeeld) en daardoor komen fraudes met reststromen niet aan het licht.

Tot slot zijn er bedrijven die zich moedwillig niet registreren bij de NVWA, terwijl ze levensmiddelen en diervoeders produceren, verwerken of distribueren. Op die manier omzeilen ze de hygiëne-eisen en controles. Het gaat om een onbekend aantal kleine handelaars en importeurs.

Er is weinig bekend over de omvang van de fraude met reststromen.

3.3 Bodemketen en oppervlaktewater

Bij criminaliteit in het domein van de bodemketen en het oppervlaktewater gaat het vooral om criminele activiteiten in de grondstromen (zie ook NDB2008, p. 115-122) en de verwerking van mest.

Activiteiten in de grondstromen

In Nederland vinden veel handelingen met grond plaats. Bij grote bouwwerkzaamheden en infrastructurele werken worden vaak grote hoeveelheden grond af- en aangevoerd. Een gedeelte van de bodem is vervuild en moet worden gesaneerd, waardoor vervuilde grond in omloop raakt. Naar schatting vinden er in Nederland dagelijks 1400 graafbewegingen plaats, waarbij in 350 gevallen sprake is van verontreinigde locaties. Het afgraven, hergebruiken, opslaan, vervoeren, reinigen en storten van grond kost geld. Dat leidt ertoe dat verschillende bedrijven in de grondketen illegale manieren zoeken om kosten uit te sparen. Ook ontdoeners van vervuilde grond zijn gebaat bij zo laag mogelijke kosten. Zij knijpen soms een oogje toe als het aankomt op de naleving van wet- en regelgeving die betrekking heeft op henzelf, in hun rol als opdrachtgever, of op hun opdrachtnemers. Aan opdrachtgeverszijde zien we gemeentelijke afdelingen die niet zo gauw protesteren als opdrachtnemers creatief omspringen met de regelgeving. Aan de kant van opdrachtnemers zien we onder andere adviseurs, laboratoria, aannemers, uitvoerders, transporteurs en grondbanken die wet- en regelgeving niet naleven.

Criminaliteit met grondstromen is er vaak op gericht verontreinigde bodem of grond door te laten gaan voor schone grond. Dit gebeurt door analyseresultaten te manipuleren, papieren te vervalsen en vervuilde partijen grond zodanig te mengen met schone grond dat de hele partij uiteindelijk net onder de vervuilingsnorm blijft. De partijen die hierbij in beeld komen, zijn bijvoorbeeld adviesbureaus die geen of net te weinig onderzoek doen, laboratoria die frauderen met bodemmonsters, niet-erkende onderaannemers die aannemers uit de brand helpen door het afvoeren van een partij vervuilde grond en grondbanken die vervuilde grond mengen met grotere partijen schone grond. Over de omvang van dit soort activiteiten valt weinig met zekerheid te zeggen.

Wel is het zeker dat de pakkans vrij gering is en dat er binnen de keten veel gelegenheden bestaan voor illegale praktijken. Dat hangt samen met de manier waarop het toezicht op de branche georganiseerd en ingericht is, hoe het wordt uitgevoerd en hoe de branche zelf functioneert.

Als we kijken naar het toezicht, zien we dat de overheid, net als bij de asbestbranche, in toenemende mate nadruk legt op privatisering daarvan, onder andere door certificering en accreditatie. Op die manier poogt de overheid de toezichtsdruk bij inspecties te verminderen. Certificering in de bodemketen houdt in dat bodemintermediairs, zoals grondsaneerders, adviesbureaus, grondbanken, aanleggers van bodembeschermende voorzieningen en tanksaneerders, door een certificerende instelling worden voorzien van een certificaat als ze

aan bepaalde eisen voldoen. De certificerende instellingen staan op hun beurt onder toezicht van de Raad van Accreditatie (RvA), die erop moet toezien dat certificaten op correcte wijze worden verstrekt. Net als in de asbestbranche blijkt certificering in de bodemketen geen garantie voor regelnaleving. Om redenen die ook al bij de bespreking van de asbestbranche aan de orde kwamen, verschaffen certificerende instellingen onder soepele condities certificaten en nemen ze niet altijd maatregelen als bedrijven zich niet aan de regels blijken te houden. De certificerende instellingen concurreren met elkaar om de gunst van de bodemintermediairs, hun 'klanten'. Als bedrijven voor weinig geld en onder soepele condities certificaten krijgen, terwijl op regelnaleving mondjesmaat wordt toegezien, kunnen bedrijven de toegekende certificaten als *window dressing* gebruiken, om op papier de indruk te wekken dat alles in orde is.
Onafhankelijkheid van adviezen en metingen door gecertificeerde adviesbureaus en laboratoria is niet altijd gewaarborgd. In de praktijk zijn er grote bedrijven waarbinnen zowel de laboratoriumanalyse als de verdere verwerking van grondstromen plaatsvindt.

Een andere factor van betekenis is dat het toezicht op de grondstromen voor een deel wordt beïnvloed door de grondstromensector zelf, onder meer doordat deze sector beoordelingsrichtlijnen opstelt die bij voldoende draagvlak in wetgeving worden opgenomen. Daardoor wordt soms wet- of regelgeving geformuleerd die ruimte laat voor interpretatie.
Wat eveneens criminaliteit in de bodemketen in de hand kan werken, is het matige zelfreinigende vermogen van de sector. Bij grondstromen worden opdrachten tussen bedrijven doorgeschoven. Daardoor is de neiging om melding te maken van malversaties door concurrerende bedrijven uit dezelfde branche niet erg groot.

Het toezicht op de bodemketen is versnipperd. Er zijn meerdere afdelingen van verschillende gezagsinstanties bij betrokken (Rijkswaterstaat, waterschappen, gemeenten en provincies, omgevingsdiensten, certificerende instellingen en inspecties) en hun informatiesystemen sluiten niet goed op elkaar aan en kunnen niet door iedereen worden ingezien.
Controle op grondhandelingen die onder het toezicht vallen, vindt vaak pas plaats als de werkzaamheden al zijn afgerond. Dan is niet meer na te gaan wat er precies is gebeurd en kan de administratie inmiddels bijgewerkt zijn.
De kans op inspectie en op de ontdekking van malversaties is niet groot. Op meer dan een half miljoen graafbewegingen per jaar, waarbij in vermoedelijk een kwart van de gevallen sprake is van verontreinigde grond, vinden een paar honderd objectinspecties en een krappe vijfhonderd administratieve controles plaats. Generieke toezichthouders zoals gemeenten houden vaak weinig indringende controles, waarbij relevante documenten veelal niet worden gecontroleerd.

Op basis van de inspecties wordt geschat dat meer dan 70 procent van de bodemintermediairs gecertificeerd werkzaamheden verricht. Ruim 50 procent van de bodemintermediairs houdt zich aan de wettelijke eisen voor de kwaliteit van werkzaamheden, zoals neergelegd in normdocumenten. Bij het uitgeven van certificaten baseert ongeveer de helft van de certi-

ficerende instellingen zich op corresponderende normdocumenten. Uit deze cijfers blijkt dat een aanzienlijk deel van de branche die met grondstromen werkt , zich niet aan de regels houdt. Pas als een bedrijf moedwillig en min of meer stelselmatig de regels overtreedt om zo extra economisch voordeel te behalen, is er sprake van criminaliteit. Cijfers daaromtrent zijn er niet. In de jaren 2012 tot en met 2015 vonden in totaal 28 strafrechtelijke opsporingsonderzoeken plaats op het terrein van bodem en grondstromen, waarbij het aantal onderzoeken sterk verschilde over de jaren heen (één in 2012, elf in 2013, dertien in 2014, drie in 2015).

Verwacht wordt dat er de komende jaren een toename van de stroom van vervuilde grond zal optreden. Dat komt door de landelijke doelstelling om in 2018 alle zogenoemde spoedlocaties, dat wil zeggen locaties met directe risico's voor de mens, gesaneerd te hebben. Het aantal criminele activiteiten in de bodemketen zal naar verwachting gelijke tred houden met de toename van handelingen met vervuilde grond.

Mestverwerking

In Nederland is al jaren sprake van een mestoverschot. De afschaffing van het melkquotum in 2015 heeft dat overschot vergroot. Er is te weinig grond waar mest gebruikt mag worden zonder schade voor het milieu. Daarom zijn er strenge regels voor de productie, het gebruik en de verhandeling van mest. Mestproducenten zijn wettelijk verplicht een overschot op verantwoorde wijze af te zetten. Hieraan zijn flinke kosten verbonden. Om die te drukken wordt er met mest gefraudeerd. Volgens de NVWA vindt er fraude plaats met het ophalen, transporteren, afleveren, bemonsteren, wegen en verantwoorden van mest. Voor een varkensbedrijf kan het frauderen met mest een kostenbesparing opleveren die oploopt tot meerdere tonnen per jaar. De totale kosten voor de mestafzet in Nederland worden voor 2015 geraamd op 500 miljoen euro. De financiële belangen in de mestsector zijn groot. Dat komt door de stijging van het mestoverschot en mestafzetkosten en door de lage afzetprijzen van producten uit de veehouderij. Dat maakt de hele keten van de mestverwerking gevoelig voor het plegen van mestfraude.

Het is relatief eenvoudig om fraude te plegen. Er zijn voldoende gelegenheden voor en dienstverleners zijn bereid de fraude mogelijk te maken. Daarentegen is het lastig en arbeidsintensief om mestfraude te ontdekken en aan te tonen. Er is sprake van uitgesteld heterdaad: de administratieve verantwoording van mestafzet vindt pas na een afgesloten jaar plaats, als de mest allang is afgevoerd of uitgereden. Daardoor kunnen hoeveelheden mest en gehalten mineralen niet meer gecontroleerd worden. Bij controle van mesttransporten is controle van de boeken vaak niet voldoende. Op papier klopt het meestal. Om mestfraude in beeld te krijgen is diepgaander onderzoek naar de meststromen nodig. Verschillende data (monstermetingen, rittenlijsten, tachograafgegevens, gps-gegevens) moeten gecombineerd worden om fictieve en daadwerkelijke meststromen inzichtelijk te krijgen. Dergelijke onderzoeken zijn gecompliceerd en tijdrovend.

Wetgeving op het gebied van meststoffen is niet zelden 'gestapeld': verschillende wetten zijn op dezelfde handeling van toepassing. Zowel naleving als handhaving is daardoor complex. Controle en handhaving zijn belegd bij verschillende organisaties, waaronder de Rijksdienst voor Ondernemend Nederland, omgevingsdiensten, de politie, de waterschappen en de NVWA. Handhaving wordt ook bemoeilijkt doordat het delen van informatie en samenwerking tussen de instanties moeizaam verlopen.

In de bodemsector zijn dienstverleners actief, zoals intermediairs, diervoederhandelaars en administratie- en adviesbureaus, die faciliteren bij het opmaken van de mestadministratie of het achteraf kloppend maken van administraties. Onder de ruim duizend mestintermediairs in deze sector bestaat veel concurrentie. Dat leidt ertoe dat intermediairs de kosten voor veehouders zo laag mogelijk houden, onder andere door het bewust niet naleven van regels, soms zonder medeweten van, soms juist in samenwerking met de producent of afnemer van mest.
Ook voor mestafnemers, zoals akkerbouwers en telers van groente en fruit, is het vrij verleidelijk om minder mineralen in hun administraties te verantwoorden dan zij feitelijk uit een partij mest hebben afgenomen, aangezien het toezicht op hun handelen beperkt is.
De mogelijkheid voor vervoerders om zelf vaste mesttransporten te bemonsteren laat ruimte voor fraude. Gezien het grote aantal mesttransporten is het niet mogelijk elk transport te controleren: de NVWA controleert jaarlijks ongeveer 1200 van de ruim 900.000 mesttransporten. Dit is bekend in de branche en dat maakt het illegaal vervoeren en uitrijden van mest aanlokkelijk.

Hoewel de omvang van mestfraude niet in getallen valt uit te drukken, schatten drie verschillende bronnen (mestverwerkers, de Land- en Tuinbouw Organisatie Nederland en de brancheorganisatie van loonwerkers en mestdistributeurs) dat 25 tot 40 procent van de mest in Nederland illegaal wordt verhandeld of gedumpt. Er zijn sinds 2014 drie omvangrijke opsporingsonderzoeken naar mestfraude uitgevoerd. In een van deze zaken werd meer dan een miljoen euro illegale winst behaald.

Uit casuïstiek met betrekking tot mestfraude komen de volgende criminele activiteiten naar voren:
- Er wordt gefraudeerd met mestmonsters.
- Mest wordt fictief verplaatst of opgeslagen en daarna zwart afgezet of op het eigen bedrijf of elders illegaal uitgereden. Administratief lijkt alles keurig in orde. In de administratie staat bijvoorbeeld dat de mest is geëxporteerd naar het buitenland, door intermediairs is afgevoerd of door intermediairs is opgeslagen in silo's of mestkelders.
- Er wordt gefraudeerd met plaatsingsruimte. Veehouders laten meer grond registreren dan ze feitelijk bezitten. Daardoor kunnen ze, op papier althans, meer mest uitrijden. Malafide dienstverleners zijn hun daarbij behulpzaam. De frauderende veehouders rijden de mest gewoon op eigen grond uit.
- Mestintermediairs maken gebruik van ingewikkelde bedrijfsstructuren en katvangers om

de werkelijke eigenaar van de bedrijven en meststromen te verhullen. Veel intermediairs hebben meerdere bv's. Als ze worden gepakt, laten ze de oude bv klappen en gaan ze verder met een andere. Soms maken ze gebruik van tientallen rechtspersonen, zowel Nederlandse als buitenlandse, om mest van A naar B te vervoeren. Fraudeurs die tegen de lamp gelopen zijn, kunnen door het inzetten van katvangers nieuwe rechtspersonen oprichten. Voor opsporingsdiensten wordt het op die manier moeilijk om de juiste rechtspersoon aan te pakken.

3.4 Omgang met gevaarlijke stoffen

Transport van gevaarlijke stoffen in het binnenlands wegvervoer

Op vervoer via buisleidingen en de binnenvaart na vindt het meeste vervoer van gevaarlijke stoffen plaats over de weg. Jaarlijks wordt ongeveer 13 miljoen ton over de weg vervoerd. Bijna 10.000 van de 12.000 transportbedrijven in Nederland houden zich in mindere of meerdere mate bezig met het transport van (containers met) gevaarlijke stoffen; 300 transportbedrijven zijn gespecialiseerd in het vervoer van gevaarlijke stoffen. Criminaliteit in deze branche bestaat vooral in het bewust nalaten van vereiste veiligheidsmaatregelen, waardoor kosten kunnen worden bespaard. Kostenbesparing is aantrekkelijk vanwege onder andere de lage winstmarges in de transportbranche en de hoge concurrentiedruk vanuit Oost-Europa.

Veel transporteurs voelen zich in de praktijk niet erg verantwoordelijk voor de lading die zij vervoeren, vaak omdat zij geen eigenaar zijn van de (afval)stoffen. Dat geeft malafide opdrachtgevers de ruimte om gevaarlijker stoffen te laten transporteren dan in de begeleidende vervoersdocumenten vermeld staat. Daarnaast is er een categorie transporteurs die hun kennis van regels voor gevaarclassificatie en afvalcodering gebruiken om opdrachtgevers juist te adviseren over wat ze in vervoersdocumenten kunnen opnemen om controles te ontwijken. Ook afnemers, zoals afvalverwerkers, hebben er soms belang bij dat de ware aard van partijen wordt verhuld. Met een algemene of aangepaste stofaanduiding bijvoorbeeld kunnen restricties op vervoer worden omzeild en kostbare analyses worden vermeden. Het foutief labelen van stoffen is gemakkelijk, doordat veel gevaarlijke (afval)stoffen onzichtbaar in afgesloten tanks vervoerd worden. Voor handhavers is het lastig om vast te stellen wat er werkelijk in de tank zit en of de wet- en regelgeving wordt nageleefd.

In de sectoren transport en verwerking van gevaarlijke afvalstoffen vindt in toenemende mate concernvorming plaats. Een kleine groep van steeds groter wordende afvalverwerkers verstevigt zijn greep op een groter deel van de afvalverwerkingsketen, waaronder het (internationale) transport van gevaarlijke afvalstoffen. Een aanzienlijk aantal handelingen vindt hierdoor plaats binnen één concern en komt daardoor buiten beeld van het toezicht, dat zich vooral richt op specifieke actoren in de keten.

Evenals in andere milieudomeinen is de capaciteit van het toezicht en bijgevolg het aantal controles gering in verhouding tot de omvang van stromen gevaarlijke (afval)stoffen en het aantal bedrijven dat zich bezighoudt met transport en verwerking ervan. De pakkans is dus gering. Als een bedrijf toch betrapt wordt, is de sanctie dikwijls licht. Frauderen bij het vervoer van gevaarlijke stoffen is al met al lucratief en relatief eenvoudig.

Werken met gevaarlijke stoffen door risicobedrijven

In Nederland vallen zo'n vierhonderd bedrijven die met grote hoeveelheden gevaarlijke stoffen werken onder het Besluit risico's zware ongevallen (Brzo). Dit zijn voor een groot deel chemische bedrijven, maar ook energiebedrijven en afvalverwerkers vallen eronder. Er is ook een onbekend aantal bedrijven dat (net) niet Brzo-plichtig is, maar waar vanwege handelingen met bepaalde gevaarlijke stoffen ook risico's bestaan. Het gaat bijvoorbeeld om grote chemiebedrijven (RIE-4-bedrijven), afvalbedrijven en transportbedrijven. Die bedrijven vallen onder een minder strikt handhavingsregime dan Brzo-bedrijven.

Een deel van de incidenten ontstaat doordat bedrijven onvoldoende maatregelen nemen om deze te voorkomen, een overtreding van het hoofdartikel van het Brzo. Als dat met opzet gebeurt, is het motief hiervoor veelal kostenbesparing. De meldingsplicht van alle ongebruikelijke voorvallen (onderdeel van het Brzo) wordt soms ontdoken om imagoschade te voorkomen. Uit een aantal onderzoeken van de Onderzoeksraad voor Veiligheid blijkt dat een minder goede 'veiligheidscultuur' bij bedrijven vaak een rol speelt in de totstandkoming van onveilige situaties en strafbare feiten.

Tabel 21 laat zien bij hoeveel geïnspecteerde bedrijven in de afgelopen jaren overtredingen van de veiligheidsregelgeving zijn geconstateerd en om hoeveel overtredingen het in totaal ging.

Tabel 21. Inspecties en overtredingen

Jaar	Geïnspecteerde bedrijven	Bedrijven met overtredingen	Geconstateerde overtredingen
2012	365	208	871
2013	363	236	1097
2014	362	191	850
2015	352	215	615

In 2015 werden bij ruim tweehonderd bedrijven in totaal meer dan zeshonderd overtredingen geconstateerd. In tien gevallen was er sprake van een 'onmiddellijke dreiging zwaar ongeval'. Om deze overtredingen aan te kunnen merken als een misdrijf moet opzet aangetoond kunnen worden door een strafrechtelijk onderzoek. In de jaren 2012-2015 hebben dertien strafrechtelijke onderzoeken plaatsgevonden, naast een onbekend aantal onderzoeken van andere diensten, zoals de ISZW en omgevingsdiensten.

De dertien onderzoeken hadden onder andere betrekking op emissies van giftige stoffen, explosies, een lekkage van blauwzuurgas en het vrijkomen van gevaarlijke afvalstoffen.

Binnen Brzo-bedrijven bestaan verschillende gelegenheden voor het plegen van overtredingen. We noemen hier de gelegenheden waarvan uit casuïstiek is gebleken dat die daadwerkelijk misbruikt worden. Bedrijven passen hun historische stofgegevens aan, waardoor bij inspecties niet bekend wordt hoeveel er van een bepaalde stof in het bedrijf aanwezig is geweest. Bedrijven melden zich niet bij de veiligheidsregio als ze onderhoud gaan uitvoeren, terwijl dat wel moet. Kleine tot middelgrote bedrijven wenden zich tot adviesbureaus voor het ontwikkelen van wettelijk verplichte veiligheidsbeheerssystemen (VBS'en) die vervolgens niet volledig worden geïmplementeerd. Sommige adviesbureaus kopiëren eerder ontwikkelde VBS'en, terwijl in alle gevallen maatwerk nodig is. Brzo-bedrijven voeren op eigen terrein laad- en losbewegingen met gevaarlijke stoffen uit, waar deze acties niet onder de vervoerswetgeving gevaarlijke stoffen vallen en ook niet zijn afgedekt in vergunningen die concrete veiligheidsvoorschriften vragen. Er vindt onvergunde (tijdelijke) opslag van gevaarlijke stoffen plaats buiten de inrichting van Brzo-bedrijven, al dan niet in transportmiddelen.

Diverse indicatoren zijn bepalend voor de waarschijnlijkheid dat zich bij Brzo-bedrijven overtredingen voordoen of dat er strafbare feiten worden gepleegd. Gebrekkig onderhoud en beperkte investeringen is zo'n indicator. Er zijn 'calculerende' bedrijven die uitsluitend aanpassingen doen als de inspectie dat verlangt. Of ze werken volgens het 'breakdownprincipe': pas als iets kapot gaat, wordt het vervangen. Dit soort bedrijven meldt ongewone voorvallen niet of bagatelliseert ze. Het risico dat er strafbare feiten worden gepleegd, bestaat ook bij bedrijven die eigen werkprocedures veronachtzamen, een onduidelijke vergunning hebben of een slechte relatie met de overheid onderhouden.

Bij omgevingsdiensten bestaat de indruk dat er bedrijven zijn die hun bedrijfsvoering zo inrichten dat zij niet Brzo-plichtig worden of zelfs bedrijfsactiviteiten splitsen om hieraan te ontkomen. Op die manier ontduiken ze de strenge Brzo-controles, terwijl ze wel activiteiten uitvoeren die feitelijk onder het Brzo-regime zouden moeten vallen. RIE-4-bedrijven en afvalbedrijven worden in dit opzicht aangemerkt als risicobedrijven. Transportbedrijven worden ook genoemd, omdat deze niet altijd beschikken over voldoende kennis van stoffen en de daaraan verbonden risico's.

Een andere criminogene factor die ertoe leidt dat overtredingen bij Brzo-bedrijven onopgemerkt kunnen blijven, is de belangrijke inbreng die de branche heeft bij de totstandkoming van wet- en regelgeving. De lobby bedingt uitzonderingen en nuances, waardoor regelgeving ontstaat die moeilijk te handhaven is. Er kan bijvoorbeeld sprake zijn van te ruime vergunningsvoorschriften, die maken dat risicovolle situaties bij bedrijven kunnen voortbestaan.

3.5 Gevolgen van milieucriminaliteit

Als gezegd in de inleiding van dit deel, geven de gevolgen van milieucriminaliteit in de incidentele gevallen die aan het licht komen reden tot bezorgdheid. Het gaat hierbij echter om casuïstiek, het ontbreekt aan cijfers waarmee gevolgen kunnen worden gekwantificeerd. Bij gebrek aan meer concrete informatie blijft het bij veel verschijningsvormen van milieucriminaliteit bij beschrijvingen van 'wat zou kunnen gebeuren en de mogelijke gevolgen die dat zou hebben'.
Hoewel de mogelijke gevolgen van de verschillende criminaliteitsvormen in de diverse milieudomeinen zeer uiteenlopen, zijn er wel enkele algemene tendensen te beschrijven voor milieucriminaliteit in brede zin.

Aantasting van de fysieke of psychische gezondheid - Bij illegale praktijken met ongezonde materialen, zoals asbest en vervuilde grond, lopen directbetrokkenen, zoals medewerkers, het risico gezondheidsklachten te ontwikkelen. Omwonenden, soms in de verre omgeving, lopen gezondheidsrisico's door incidenten bij bedrijven die de veiligheidsregelgeving niet naleven. Wanneer reststromen op frauduleuze wijze in omloop worden gebracht in de voedselketen, kan dat ernstige gevolgen hebben voor de volksgezondheid. Illegale praktijken bij het blenden van stookolie raken de hele bevolking, doordat schadelijke stoffen bij het gebruik van stookolie in de lucht terechtkomen. Boven op de duizenden doden die jaarlijks wereldwijd het gevolg zijn van reguliere emissies door de scheepvaart dragen de illegale blends vermoedelijk onevenredig bij aan nog meer doden door de uitstoot van gevaarlijk fijnstof en onverbrande stoffen.

Aantasting van het milieu - Ernstige emissies van gevaarlijke stoffen in chemische fabrieken die het gevolg zijn van overtreding van de regelgeving, hebben vermoedelijk ernstige gevolgen voor het milieu. Door illegale overbemesting of door het illegaal wegmengen van vervuilde grond in grondstromen kan de kwaliteit van het grondwater waaruit drinkwater wordt gewonnen nadelig worden beïnvloed. Door overbemesting bijvoorbeeld maken drinkwaterbedrijven veel extra kosten om drinkwater binnen de kwaliteitsnormen te houden.

Angst, hinder en onbehagen - Deze categorie gevolgen doet zich vooral voor als zich grotere incidenten voordoen ten gevolge van malversaties in het milieudomein. In sommige branches voelen toezicht en handhaving zich onder druk gezet door belanghebbenden. Als de hand wordt gelicht met wet- en regelgeving en dit een directe impact heeft op consumentenproducten, bijvoorbeeld bij reststromen, kan dit het vertrouwen van de consument in de voedselvoorziening schaden. Het vertrouwen van de consument of medewerkers van bedrijven kan eveneens in het geding zijn bij bijvoorbeeld asbestverwijdering of de activiteiten van risicobedrijven. Dat vertrouwen wordt geschaad als bekend wordt dat asbestsaneerders locaties vrijgeven, terwijl ze feitelijk onveilig zijn of dat risicobedrijven werken met veiligheidsbeleid waarvan ze de regels met voeten treden.

Financiële schade - Bedrijven die in het milieudomein verschillende vormen van milieucriminaliteit plegen, zadelen de overheid en de samenleving op met kosten. Deze bedrijven vergoeden de kosten dikwijls niet zelf of doen dat in beperkte mate. De kosten kunnen flink oplopen: een brand bij een bedrijf dat tot 2011 chemicaliën mengde en verpakte, kostte de samenleving ruim 65 miljoen euro, en voor de sanering van een zwaar vervuild terrein van een fosforfabriek bleek een budget van 41 miljoen euro niet toereikend.
Ook mestfraude kan aanzienlijke financiële consequenties hebben. Als Nederland door mestfraude meer fosfaten produceert dan in Europa toegestaan is, kan dat leiden tot sancties op het gebied van derogatie en een verdere inperking van het gebruik van dierlijke mest in Nederland. Dat brengt de agrarische sector ernstige economische schade toe, omdat deze sector dan minder kan produceren.

Ondermijning - Van ondermijning in het milieudomein is veelvuldig sprake, omdat in hoofdzaak legale bedrijfsstructuren worden misbruikt voor illegaal gewin. Bedrijven die zich wel aan de regels houden, worden benadeeld door oneerlijke concurrentie van bedrijven die dit niet doen. Dat levert besmettingsgevaar op, omdat in het milieudomein veel verschillende ketenpartners voor inkomsten van elkaar afhankelijk zijn en bovendien nauw met elkaar samenwerken. Bedrijven die niet uit de markt willen worden gedrukt, staan onder druk om ook de regels te overtreden. Het normbesef van bedrijven kan negatief worden beïnvloed. Dat kan uiteindelijk als gevolg hebben dat branches in het milieudomein als geheel corrumperen.
Alhoewel er weinig bekend is over illegale beïnvloeding van rechtspleging, politiek, openbaar bestuur en economie, zijn toezichthouders in het milieudomein wel kritisch over de aanzienlijke rol die branchevereningingen en lobby's spelen bij de ontwikkeling van wet- en regelgeving in dit domein.
Van ondermijning op het gebied van de vitale infrastructuur kan sprake zijn, als vervuiling van het grondwater door milieucriminaliteit de drinkwatervoorziening bedreigt.

3.6 Conclusie

Aan de economische activiteiten binnen het milieudomein worden eisen en regels gesteld om het milieu, de fysieke veiligheid, de voedselveiligheid en de volksgezondheid te beschermen. Die eisen en regels brengen kosten met zich mee voor degenen die de regels moeten naleven, meestal bedrijven. Sommigen gaan op zoek naar illegale mogelijkheden om die kosten te drukken. In het milieudomein kan ook illegaal worden verdiend aan activiteiten die bij een rechtmatige uitvoering alleen maar geld zouden kosten.
Uit de voorgaande bespreking van de acht criminaliteitsvormen in het milieudomein blijkt dat gelegenheden voor criminaliteit in ruime mate voorhanden zijn, evenals de financiële prikkel om de gelegenheid te baat te nemen. Deze kenmerken brengen milieucriminaliteit als het ware voort. Bovendien heeft handhaving van de wet- en regelgeving vanuit overheidsinstanties beperkte impact: de instanties kampen met een gebrek aan capaciteit.

Evenals in eerdere rapportages is gedaan (zie ook het NDB2012), kunnen we uit het onderzoek naar de acht vormen van milieucriminaliteit concluderen dat het milieudomein kan worden omschreven als criminogeen. De factoren die daarin vooral bepalend zijn, sommen we hier nog eens op.

Bedrijven in het milieudomein, met name bedrijven die zich bezighouden met vormen van afvalverwerking, krijgen veelal betaald voordat zij hun werkzaamheden hebben afgerond. Concernvorming leidt tot bedrijven met controle over diverse schakels in de ketens van het milieudomein, waardoor transacties minder transparant worden en toezicht wordt bemoeilijkt. Globalisering van handelsstromen biedt de mogelijkheid te kiezen voor bestemmingslanden met andere verwerkingstechnieken, minder wet- en regelgeving of minder toezicht.
Ook in Nederland zelf is de wetgeving moeilijk te handhaven, doordat op eenzelfde situatie verschillende wetten van toepassing zijn en doordat wetgeving ingewikkeld is en diverse uitzonderingen kent. Binnen een branche zijn bedrijven niet zelden afhankelijk van elkaar, bijvoorbeeld doordat ze opdrachten naar elkaar doorsluizen. Dat heeft tot gevolg dat de neiging om melding te maken van illegale praktijken van andere bedrijven niet groot is.
De grote landelijke inspecties hebben hun zorg uitgesproken over de gedeeltelijke privatisering van het toezicht door certificerende instellingen. Het is gebleken dat gecertificeerde bedrijven ernstige overtredingen plegen, maar dat dit niet gauw leidt tot het intrekken van het certificaat. In Brzo-bedrijven heerst in sommige gevallen een cultuur waarin de veiligheid van medewerkers en omwonenden geringe aandacht heeft.
In combinatie met de economische druk die sommige bedrijven voelen, dragen deze factoren ertoe bij dat wet- en regelgeving overtreden wordt.

Ongewenste effecten van horizontaal toezicht zien we ook bij de toezichtstaken die (lokale) overheden gedelegeerd hebben aan omgevingsdiensten die in opdracht van deze overheden toezien op de naleving van milieuwet- en -regelgeving. Zij kampen met efficiencydruk die door hun opdrachtgevers wordt opgelegd. Vooralsnog ontwikkelen veel omgevingsdiensten zich moeizaam. Dat komt onder meer doordat er geen gemeenschappelijke kwaliteitscriteria zijn voor een adequaat functioneren van deze diensten. Door deze problemen schiet het toezicht van omgevingsdiensten tekort en ontspringen malverserende bedrijven in het milieudomein de dans.
In de nieuwe Omgevingswet, die in 2019 van kracht wordt, zet de tendens van horizontaal toezicht zich voort. Bedrijven die de regels serieus en consequent naleven, krijgen het vertrouwen van de overheid om zelf toezichthouder te zijn, al dan niet met inschakeling van andere private partijen. Hoe dergelijke regelgeving uitwerkt in de praktijk zal moeten blijken.
Het eerdergeschetste beeld van de wijze waarop bedrijven in het milieudomein georganiseerd zijn en gewend zijn (met elkaar) te werken, nodigt er niettemin toe uit deze vorm van privatisering en de effecten daarvan kritisch in het oog te houden. Daarbij speelt mee dat veel branches in het milieudomein door hun uitgebreide kennis en expertise op het terrein van ingewikkelde (internationale) wet- en regelgeving aanzienlijke invloed hebben op het vaststellen van nieuwe wet- en regelgeving en beleid.

Een van de gedachten achter de privatisering van het toezicht in het milieudomein is dat de toezichtsdruk daardoor kan afnemen: het aantal (medewerkers bij) toezichthouders zou gereduceerd kunnen worden. Dat is ook wat er feitelijk gebeurt.
Dat laat onverlet dat er knelpunten zijn in de handhaving en het toezicht op het milieudomein, en dat biedt ook gelegenheden voor criminaliteit. In verhouding tot de omvangrijke stromen die in het milieudomein rondgaan, is de capaciteit van veel handhavings- en opsporingsdiensten gering, zowel in termen van het aantal medewerkers als wat betreft de noodzakelijke kennis en expertise om controles adequaat te kunnen uitvoeren. Het gebrek aan deskundigheid manifesteert zich in het bijzonder bij de interpretatie van de 'einde-afvalcriteria'; niet zelden ontstaat er discussie tussen toezichthouders en bedrijven over de vraag of iets nu als afval moet worden gezien of niet. Die ontwikkeling zet zich voort nu er mondiaal een tendens is steeds meer (afval)stoffen te hergebruiken. Bij die trend hoort ook het afschaffen van steeds meer vereiste vergunningsverleningen in het milieudomein. Toezicht vindt hoe langer hoe vaker pas achteraf plaats.
Door al deze ontwikkelingen kunnen sommige illegale activiteiten in het milieudomein ongehinderd doorgang vinden en worden geen strafbare feiten geconstateerd, terwijl daar feitelijk wel sprake van is.
Bedrijven in het milieudomein die strafbare feiten willen plegen, weten hoe de inspecties en opsporingsdiensten georganiseerd zijn en werken. Ze kennen de leemten in wet- en regelgeving en kennen de valkuilen van handhavings- en opsporingsdiensten. Dat inzicht buiten ze uit bij het plegen van strafbare feiten. De pakkans voor gepleegde illegale activiteiten is klein door de beperkte capaciteit, de versnippering van het toezicht en het tekort aan kennis en deskundigheid in relatie tot de complexe wet- en regelgeving.

Deel 4

Signaleringen en nabeschouwing

1 Signaleringen

1.1 Inleiding

De doelstelling van het Nationaal dreigingsbeeld is tweeledig: het moet een rationele basis bieden voor de keuze van de criminele hoofdactiviteiten die bij de aanpak prioriteit zullen krijgen, en het moet nieuwe ontwikkelingen en andere opmerkelijke zaken signaleren waarmee bij de bestrijding van de georganiseerde criminaliteit rekening moet worden gehouden. We putten voor deze signaleringen uit de deelrapporten die aan dit NDB ten grondslag liggen. Het gaat om aspecten van georganiseerde criminaliteit die opvallen zonder dat er in de meeste gevallen speciaal onderzoek naar gedaan is en waarvan we denken dat ze in de (nabije) toekomst een belangrijke rol gaan spelen. Soms gaat het om gelegenheden, soms gaat het om (technologische) ontwikkelingen en in andere gevallen om veranderingen in de criminele praktijk. Zo zijn elf signaleringen geselecteerd, die in een viertal clusters zijn ondergebracht:

- *De rol van de overheid*
  Horizontaal toezicht
  Wet- en regelgeving in de milieusector
- *Digitale technologie*
  Internet of Things
  Cloudcomputing
  Crowdfunding
  Blockchain, bitcoin en payment service provider
- *De criminele praktijk*
  Do-it-Yourself
  Crime-as-a-Service
  Criminele uitbesteding en professionalisering
  Criminele veelzijdigheid
- *Georganiseerde criminaliteit in de wijken: onaantastbaarheid en normvervaging*

Aan elk van deze clusters is in dit hoofdstuk een paragraaf gewijd.

1.2 De rol van de overheid

In deze paragraaf wordt de rol van de overheid vanuit twee invalshoeken belicht. De ene betreft de verschuiving van toezicht en controle van de overheid naar private partijen. We zien deze verschuiving vooral in de milieusector en bij de belasting- en accijnsinning. De andere heeft betrekking op de complexiteit van wet- en regelgeving op het terrein van milieuhandhaving.

Horizontaal toezicht

Sinds 2003 zet de overheid in op certificering en accreditatie bij de naleving van wet- en regelgeving.

Zo bestaat er inmiddels binnen het milieudomein een scala aan certificerende instellingen (CI's), die op hun beurt onder toezicht staan van de Raad van Accreditatie (RvA). Certificerende instellingen geven – na een initiële audit – certificaten uit waaruit blijkt dat een bedrijf aan bepaalde eisen voldoet. Ook adviseren zij bedrijven over de wijze waarop deze ervoor kunnen zorgen dat ze aan de eisen voldoen. Bedrijven met zo'n certificaat worden minder gecontroleerd dan andere bedrijven. De CI's worden betaald door de ondernemingen die zij moeten certificeren, het zijn commerciële bedrijven. De Raad van Accreditatie is er om erop toe te zien dat de certificaten op correcte wijze worden verstrekt. Het 'verticale' toezicht (door de overheid op bedrijven) is goeddeels vervangen door 'horizontaal' toezicht (HT).

De inspecties die actief zijn op de milieumarkt (de Voedsel- en Warenautoriteit, de Inspectie Leefomgeving en Transport en de Inspectie Sociale Zaken en Werkgelegenheid) wijzen erop dat de controles van de CI's vaak tekortschieten en niet goed genoeg geregistreerd worden. Ook blijkt dat CI's veelal zeer terughoudend zijn bij het nemen van maatregelen. Zo behouden bedrijven hun certificaat, ook bij herhaalde overtreding. De inspecties verklaren deze bevindingen onder andere uit de marktsituatie bij de certificatie. De CI's zijn commerciële bedrijven die moeten concurreren om opdrachten van bedrijven binnen te halen. De bedrijven zoeken en contracteren CI's die tegen de laagste kosten de ruimste certificaten afgeven. Dit leidt ertoe dat de eerste audit op basis waarvan een certificaat wordt afgegeven niet altijd even streng wordt uitgevoerd. Ook bij vervolgaudits moet de CI er rekening mee houden dat de klant altijd naar een andere CI kan overstappen als deze naar verwachting soepeler zal omspringen met de condities. Wanneer er financiële afhankelijkheid bestaat, is de vereiste onafhankelijkheid van de CI's in het geding.

Vormen van horizontaal toezicht beperken zich niet tot de milieusector, ook bij de belastingheffing en douaneprocedures zien we vormen van horizontaal toezicht. Zo sluit de Belastingdienst HT-convenanten met individuele ondernemingen waarin vastgelegd wordt wat ieders verantwoordelijkheden zijn en welke verwachtingen ieder mag koesteren. Bij horizontaal toezicht werkt de Belastingdienst samen met externe partijen en verschuift het toezichtproces van controle achteraf naar afstemming vooraf. Bij horizontaal toezicht met fiscaal dienstverleners steunt de Belastingdienst op het werk dat de fiscaal dienstverlener voor zijn klant (de ondernemer) doet. De controle wordt in feite uitbesteed aan deze dienstverlener.

Bij de douane krijgt het horizontale toezicht gestalte in de zogenoemde Authorized Economic Operator (AEO). Een AEO is een import- of exportbedrijf dat als veilig en betrouwbaar te boek staat en dat, nadat het op bepaalde criteria is getoetst, als zodanig door de douane gecertificeerd wordt. Deze bedrijven worden minder vaak fysiek en/of administratief gecontroleerd en hebben daardoor minder oponthoud bij het passeren van grenzen. Een AEO-certificaat is in de gehele Europese Unie geldig. Nederland moet dus certificaten van andere lidstaten accepteren en deze bedrijven als veilig en betrouwbaar behandelen, en andere lidstaten moeten op dezelfde manier omgaan met door Nederland gecertificeerde bedrijven. De douane hoeft zich bij deze bedrijven niet meer af te vragen of zij (of hun goederen) diepgaand gecontroleerd moeten worden.
Het is evident dat bij dergelijke vormen van toezicht het risico van misbruik bestaat. In het milieuveld wordt melding gemaakt van fraude bij certificerende instellingen. Ook lijken fiscaal dienstverleners op malafide wijze in te spelen op de toezichtsstrategie van de Belastingdienst. Verder vermoeden experts een verband tussen het aantal teruglopende douaneonderzoeken in Rotterdam en de toepassing van horizontaal toezicht. Door de verminderde controle zouden ook minder overtredingen worden geconstateerd. Ten slotte wordt in het deelrapport over arbeidsuitbuiting gewezen op het gevaar dat een terugtredende overheid en de daarmee gepaard gaande afname van toezicht kunnen leiden tot een toename van de gelegenheden voor arbeidsuitbuiting.

Wet- en regelgeving in de milieusector

Bij milieucriminaliteit gaat het om overtreding van gecompliceerde wet- en regelgeving. Op de inhoud en handhaving hiervan hebben diverse overheden invloed: de landelijke overheid, de provincies en de gemeenten. Daar komt bij dat veel Nederlandse regelgeving voortkomt uit de implementatie van Europese regelgeving. Vanuit de branches wordt niet zelden succesvol gelobbyd voor meer uitzonderingen en nuances in de wet- en regelgeving. Dat maakt alles nog ingewikkelder en maakt handhaving nog moeilijker. Soms bestaat het nettoresultaat uit regels die elkaar gedeeltelijk overlappen of zelfs met elkaar in tegenspraak zijn.
De regelgeving voor transport bijvoorbeeld ziet toe op gevaarlijke stoffen en heeft het veilig vervoeren van de lading tot doel, terwijl milieuregelgeving over gevaarlijke *afval*stoffen spreekt en bescherming van mens en milieu tot doel heeft. Doordat bij het transport van gevaarlijke afvalstoffen niet alleen de gevarenclassificatie komt kijken maar ook afvalstoffenwetgeving, zijn er twee manieren waarop stoffen en mengsels worden ingedeeld. Hierdoor ontstaat in de praktijk nogal eens ‘verwarring’ en worden stoffen foutief ingedeeld, met alle veiligheids- en milieurisico’s van dien.
Het indelen van gevaarlijke (afval)stoffen is bijzonder lastig en kan gemakkelijk fout gaan. Bestanddelen en fysische en chemische eigenschappen van stoffen kunnen doorgaans niet eenvoudig worden bepaald, terwijl een correcte identificatie essentieel is voor de juiste indeling en voor de regels die van toepassing zijn. Bedrijven kunnen economisch voordeel behalen door die indeling te kiezen waarvoor minder eisen zijn gesteld aan transport en verwerking van stoffen.

Hiaten, overlap en onduidelijkheid in de toepassing van wet- en regelgeving bij het transport van gevaarlijke (afval)stoffen vormen een fundamenteel probleem.
De complexe wet- en regelgeving rond milieuproblematiek vormt een niet te onderschatten gelegenheidsstructuur. In combinatie met de verminderde controle ten gevolge van het hierboven beschreven horizontale toezicht, kan deze gelegenheidsstructuur worden beschouwd als een belangrijke criminogene factor. Milieucriminaliteit bestaat immers voor een belangrijk deel uit het nalaten van dingen die volgens de regels hadden moeten gebeuren, en deze regels laten door de invloed van de branches veel ruimte voor interpretatie.

1.3 Digitale technologie

Er zijn relatief veel signaleringen met een digitale component. Dat is niet vreemd in een tijd waarin de samenleving in toenemende mate digitaliseert en ontwikkelingen elkaar razendsnel opvolgen. De impact ervan is waarschijnlijk groot, maar zal pas op langere termijn ten volle duidelijk worden. Ofschoon we deze digitale signaleringen in deze paragraaf individueel behandelen, interacteren ze met elkaar, en daardoor worden de effecten ervan versterkt. De hier genoemde digitale signaleringen voorzien in een legale en legitieme behoefte. Wanneer ze echter gebruikt worden voor criminele doeleinden, gaat er van de gecombineerde en interacterende ontwikkelingen een duidelijke dreiging uit.

Internet of Things

Internet of Things (IoT) verwijst naar de trend om allerlei 'dingen' via wifi of andere draadloze verbindingen aan het internet te koppelen. Het begon allemaal toen naast het internetprotocol versie 4 (IPv4) in 2012 IPv6 werd geïntroduceerd. Dit protocol breidde het aantal mogelijke IP-adressen uit van zo'n 4 miljard tot 50 quadriljard adressen per persoon ($3{,}4 \times 10^{38}$)[41]. Hierdoor werd het aantal toe te wijzen IP-adressen schier onuitputtelijk en ontstond de mogelijkheid om 'alles met alles' te verbinden. En dat heeft dus ook een aanvang genomen. Zo zijn beveiligingscamera's en de daarbij behorende digitale videorecorders aangesloten op het internet, thermostaten laten via een app op de smartphone de verwarming starten, koelkasten geven door welke artikelen over de houdbaarheidsdatum zijn of aanvulling behoeven, hartpatiënten krijgen monitorapparatuur geïmplanteerd die via internet aan de arts laat weten hoe het ermee staat, e-pleisters analyseren de transpiratie en stellen remedies voor, insulinepompen en pacemakers worden via een app bediend, diagnostische robotjes worden door het lichaam gestuurd waarna de gegevens online worden gedeeld met het ziekenhuis, de vuilcontainer geeft aan de gemeente door dat hij geleegd wil worden en bidons maken de eigenaar er met een notificatie op attent dat het tijd is aandacht te besteden aan de vochtbalans. De voorbeelden worden alleen gelimiteerd door onze beperkte fantasie.
Er zijn diverse schattingen van het aantal apparaten dat in de nabije toekomst verbonden zal zijn met het globale IoT. Het consultancy- en adviesbureau Gartner schat dat dit aantal rond

41 Internet Protocol versie 6 (s.d.). In *Wikipedia*. Geraadpleegd op https://nl.wikipedia.org/wiki/Internet_Protocol_versie_6

2020 op 21 miljard zal liggen.[42] Anderen[43] gaan verder en komen uit op 50 tot 100 miljard apparaten. Hoe het ook zij, duidelijk is in ieder geval dat het IoT de komende jaren een enorme groei te zien zal geven.

Met een toename van 'dingen' die met het internet verbonden zijn, neemt het aantal potentiële doelwitten van cyberaanvallen exponentieel toe. Bovendien kunnen deze 'dingen' ook deel gaan uitmaken van botnets die gebruikt worden voor het plegen van cybercrime. Voor de consumenten is vaak niet duidelijk welk apparaat besmet is met malware. De mate waarin cyberaanvallen zullen gaan plaatsvinden, is afhankelijk van de aandacht voor de technische beveiliging en de mate waarin van deze aanvallen een crimineel verdienmodel kan worden gemaakt. Steeds duidelijker wordt echter dat de 'dingen' die met het internet verbonden zijn, een notoir slechte beveiliging kennen. Ze hebben vaak software die niet geüpdatet wordt en er worden van fabriekswege standaardwachtwoorden gebruikt die vaak niet te wijzigen maar wel eenvoudig te kraken zijn. In oktober 2016 heeft een hackersgroep hiervan gebruikgemaakt door grote aantallen beveiligingscamera's en digitale videorecorders (van een bepaald merk) te hacken en ze in een botnet te plaatsen waarmee een DDoS-aanval gepleegd werd op belangrijke servers aan de oostkust van de Verenigde Staten. Dit resulteerde in een massieve interruptie van populaire internetdiensten zoals Twitter, Amazon, Reddit, Spotify, PayPal, Airbnb, Pinterest en Vox Media. Nu valt te verdedigen dat dit vooral vandalisme is en voor een beperkte tijd wat overlast heeft gegeven bij diensten die niet bepaald tot de cruciale onderdelen van de vitale infrastructuur behoren, maar het maakt wel duidelijk welke (criminele) mogelijkheden het IoT in zich bergt. Zo is het denkbaar – en wat denkbaar is binnen de ICT-wereld gebeurt waarschijnlijk ook – dat op dezelfde manier ransomware verspreid wordt. Dat zal niet alleen financiële consequenties hebben, maar kan ook leiden tot verlies van belangrijke (persoonlijke) gegevens en verstoring van ICT-systemen. Verder bieden de vele apparaten die met internet verbonden zijn, mogelijkheden om via hacking bij de eigenaren van die apparaten mee te kijken en te luisteren naar alles wat zich afspeelt in huis, bedrijfs- of overheidsgebouw. In potentie resulteert dit in een schending van de privacy die haar weerga niet kent.

In het centrum van deze wereldwijde innovatie staan niet zozeer al die apparaten als wel de 'verbonden mens' die al die apparaten gebruikt; er is sprake van een 'Internet of People'. Dit leidt tot dataficatie, een enorme toename van data over menselijk gedrag – al dan niet vrijwillig afgestaan – en registratie, opslag en analyse hiervan door bedrijven en overheden. Er zijn veel toepassingen mogelijk, al dan niet met behulp van bigdata-technieken, voor de analyse van grote hoeveelheden gegevens. Behalve voor deze bedrijven zelf, zijn al deze gegevens om uiteenlopende redenen ook interessant voor 'digitale criminelen'. Ze kunnen bijvoorbeeld gebruikt worden voor identiteitsfraude, ze kunnen gegijzeld worden en alleen

42 Gartner (2015, 10 november). *Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015* (Press release). Geraadpleegd op http://www.gartner.com/newsroom/id/3165317

43 Ch. Adams jr. (2014, 15 december). The Internet of Things and the connected person (Blogpost). Geraadpleegd op http://insights.wired.com/profiles/blogs/the-internet-of-things-iot-and-the-connected-person

tegen betaling vrijgegeven, de data kunnen gevoelige persoonlijke of financiële gegevens en wachtwoorden bevatten die tot afpersing of diefstal kunnen leiden. Hoewel militaire spionage en bedrijfsspionage niet tot het NDB-domein gerekend worden, willen we er wel op wijzen dat het IoT ook op deze terreinen talloze gelegenheden biedt.

Cloudcomputing

Een belangrijke ontwikkeling binnen het internetlandschap is *cloudcomputing*. Er is geen vastomlijnde definitie van cloudcomputing, maar de essentie ervan is dat ICT-infrastructuren, platforms, softwarediensten en data niet langer lokaal (op de eigen pc of server) maar via het internet worden opgeslagen, benaderd en gebruikt. Daarbij is van belang dat het gegevensbeheer of de computerapplicaties aan een dienstverlener worden uitbesteed, en dat gegevens verspreid over verschillende servers worden opgeslagen – meestal zonder dat de gebruiker de regie heeft over de precieze locatie.

Cloudcomputing gaat met diverse veiligheidsrisico's gepaard. Zo kan de cloud zowel doelwit van als middel voor cybercriminaliteit zijn. Als doelwit is de cloud interessant, omdat clouddiensten over een schat aan informatie beschikken. Vooral financiële gegevens en identiteitsgegevens zijn interessant voor criminelen. Zij kunnen ze gebruiken voor afpersing maar ook voor identiteitsfraude. Vooral clouddiensten die vanaf eenzelfde fysieke locatie worden gefaciliteerd, zijn kwetsbaar. Met één enkele aanval kunnen direct veel gebruikers worden getroffen.

De opslag- en rekencapaciteit van de cloud kan verder worden misbruikt in botnets of voor het uitvoeren van grootschalige DDoS-aanvallen. Daarnaast kunnen clouddiensten een krachtig middel voor de verspreiding van malware zijn. Verder kunnen criminelen de cloud gebruiken om anoniem en niet-traceerbaar te communiceren.

De hoeveelheid mogelijkheden die de cloud aan criminelen biedt, hangt samen met het beveiligingsniveau. Na enkele incidenten is de toegangsbeveiliging verbeterd. Veel diensten zijn inmiddels overgegaan op tweefactor-authenticatie, waardoor de cloud relatief veilig is. Een verschuiving van activiteiten naar de cloud zou gunstig kunnen zijn voor bijvoorbeeld het midden- en kleinbedrijf (MKB). Momenteel is het MKB door de hoge kosten van goede beveiliging en de gefragmenteerde ICT-infrastructuur kwetsbaar voor cybercrime. De cloud is beter beveiligd dan de ICT-voorzieningen die nu over het algemeen gebruikt worden.

Crowdfunding

Crowdfunding is een fenomeen dat sterk in opkomst is. Op allerlei terreinen worden crowdfundingacties opgezet: van het bekostigen van een dure operatie tot het financieren van commerciële start-ups, van kleine sympathieke private projecten zoals een kattencafé in Amersfoort tot de deelname van het vrouwensquashteam aan het WK.

De bedragen waarmee deelgenomen kan worden, variëren sterk. Soms wordt de hoogte van het bedrag aan de investeerder overgelaten, soms wordt een minimumbedrag aangehouden, soms gaat het om een donatie zonder dat een tegenprestatie wordt gevraagd en is

crowdfunding een digitale vorm van collecteren. In 2015 werd hiermee in Nederland een totaalbedrag van 125 miljoen euro opgehaald.
De Autoriteit Financiële Markten (AFM) waarschuwt tegen crowdfunding, omdat de risico's vaak veel groter zijn dan bij 'gewone' beleggingen. Crowdfunding wordt immers gebruikt voor het financieren van projecten waar gewone banken geen brood in zien vanwege de te grote risico's. Er worden schuchtere pogingen ondernomen om de markt te reguleren. Zo mag een consument per crowdfundingplatform niet meer investeren dan 80.000 euro en moeten mensen die voor het eerst investeren en meer dan 500 euro willen inleggen een investeringstoets afleggen. In hoeverre dit de risico's beperkt, moeten we nog afwachten.
Uit diverse deelrapporten blijkt dat crowdfunding ook op minder eerzame manieren gebruikt wordt. In het rapport over horizontale fraude is melding gemaakt van misbruik van crowdfunding als vorm van voorschotfraude. Ook kan crowdfunding gebruikt worden voor witwassen: een witwasser kan een crowdfundingactie opstarten waarbij hij de inleggers zelf van de inleg voorziet. Het geld dat hij daarmee binnenhaalt, heeft door die truc een verklaarbare en schijnbaar legale herkomst.
Al staan de signalen in Nederland op dit moment niet op rood, in het buitenland zijn meerdere meldingen van dergelijk misbruik gedaan. Wanneer de groei echter doorzet – en het heeft er alle schijn van dat dit zal gebeuren – wordt crowdfunding ook voor Nederlandse criminelen een aantrekkelijke mogelijkheid voor frauduleus gebruik.

Blockchain, bitcoin en payment service provider

Hoewel zich de afgelopen jaren al grote veranderingen hebben voltrokken, staat de financiele dienstverlening aan de vooravond van wellicht nog grotere veranderingen. Enkele exponenten van die veranderingen zijn de *blockchaintechnologie*, met als bekendste manifestatie de bitcoin, en nieuwe manieren van betalen, waaronder de *payment service provider* (PSP).

De blockchaintechnologie is de technologie achter de bitcoin en andere cryptocurrency's. Tot voor kort was dit een wat duister fenomeen, dat vooral bekendheid kreeg door de aanvankelijk sterk stijgende koers van de bitcoin, de snel daarop volgende koersval en het gebruik van de bitcoin voor dubieuze zaken zoals het betalen van de losprijs bij gijzeling van computers. Recent heeft een internationaal consortium van veertig banken de blockchaintechnologie echter omarmd, omdat deze voor meerdere doeleinden inzetbaar is. Kort gezegd is een blockchain een openbaar, online register van transacties. Via de blockchain van de bitcoin kan nagegaan worden wie de eigenaar is en of de bitcoin niet twee keer wordt uitgegeven. De toepassingen zijn legio. Zo is voorstelbaar dat deze techniek ook bij de huizenverkoop, aandelentransacties, het opmaken van aktes en autoverhuur zal worden gebruikt.
Er valt veel meer over te zeggen, maar de essentie van de blockchaintechnologie is dat er geen tussenpersoon meer nodig is bij transacties. Doordat het register openbaar is en wereldwijd gedistribueerd wordt, kunnen partijen rechtstreeks met elkaar zakendoen.

Hierdoor worden notarissen, financieel dienstverleners, makelaars en andere intermediairs in beginsel overbodig. Het verdienmodel van banken zou bij algemene toepassing van de blockchaintechnologie een grondige herziening behoeven. Dit verklaart ook de interesse van de banken. Hoewel er veel vragen bestaan over de veiligheid van de blockchains, de softwareontwikkeling en de bereidheid van partijen om de vertrouwde omgangsvormen bij transacties los te laten, zien veel betrokkenen hierin de volgende digitale revolutie.
Ongetwijfeld vinden innovatieve criminele samenwerkingsverbanden of individuele *whizzkids* een manier om misbruik te maken van de mogelijkheden die de blockchaintechnologie biedt. De kernvraag is in hoeverre dit fenomeen in de komende vier jaar al zijn stempel zal drukken op het betalingsverkeer. De deskundigen zijn het daarover niet eens. Er zijn weliswaar voorbeelden te geven van technologische ontwikkelingen die veel sneller gingen dan aanvankelijk gedacht (bijvoorbeeld de toepassingen van internet, smartphones, sociale media en tablets), maar de blockchaintechnologie verkeert nog in een pril stadium. Dat maakt het lastig verwachtingen uit te spreken. Op dit moment zijn de cryptocurrency's bijvoorbeeld nog geen wettig betaalmiddel, terwijl dat wel een voorwaarde is om breed ingang te vinden bij alledaagse betalingen. Hoe het ook zij, het lijkt een buitengewoon relevant fenomeen dat het volgen waard is. Alleen zo kunnen we tijdig het hoofd bieden aan eventuele criminele toepassingen.

Recent is in opsporingsonderzoeken naar witwassen de *payment service provider* (PSP) opgevallen. Een PSP is een online betaaldienst die de betalingen aan winkeliers afhandelt. Het voert hier te ver om alle technische varianten ervan te behandelen. Relevant is dat uit opsporingsonderzoeken is gebleken dat het gebruik van een PSP de crimineel kan helpen bij het verhullen van de herkomst van zijn omzet. Dat komt doordat een PSP vaak verschillende transacties opspaart om deze in één keer bij de bank aan te leveren. Doordat de transacties dan niet meer op consumentenniveau uitgesplitst zijn, kan de bank niet controleren wie de transacties hebben verricht en of de regels zijn nageleefd (*compliance*). De compliance ligt daarom bij de PSP, maar deze is vaak in het buitenland gevestigd en ziet te weinig details. Een nieuwe ontwikkeling op dit gebied is dat verdachten zelf de beschikking over een PSP hebben en dus de compliance volledig in eigen beheer hebben. Daarmee ontstaat voor criminelen een goede mogelijkheid hun cliënten of omzet te verhullen. De drempel om een PSP te beginnen is relatief laag. Iemand met enige technologische *knowhow* kan er al een opstarten en anders kan hij de expertise wel inhuren. De rol van PSP's zal in de nabije toekomst belangrijker worden. Het is een vorm van uitbesteding die tot grote besparingen leidt.

1.4 De criminele praktijk

In deel 2 zijn, per afzonderlijk thema, uiteenlopende aspecten van de criminele praktijk besproken. Hier worden enkele meer algemene ontwikkelingen belicht waarvoor geldt dat de relevantie niet beperkt blijft tot de criminele praktijk binnen een enkel thema, maar bredere toepassing kent binnen het terrein van de georganiseerde criminaliteit.

Allereerst zijn dat drie ontwikkelingen die iets zeggen over de mate waarin criminelen hun omgeving inschakelen bij hun criminele activiteiten: *Do-it-Yourself, Crime-as-a-Service* (CaaS) en criminele uitbesteding. Do-it-Yourself kenmerkt zich door zelfstandigheid. Zo gebruikt men bestaande technieken en informatie om zelf producten te vervaardigen. Dat zijn in dit verband producten die kunnen worden misbruikt of die van zichzelf al illegaal zijn. Bij CaaS worden instrumenten gebruikt die anderen hebben ontwikkeld en aangeboden om criminaliteit te faciliteren. En in het geval van criminele uitbesteding worden anderen ingehuurd om een deel van de criminele activiteiten uit te voeren. We besteden bij de bespreking hiervan ook aandacht aan de vraag of ontwikkelingen in de afgelopen jaren iets zeggen over de mate waarin criminele samenwerkingsverbanden (csv's) op een professionele manier werken (al dan niet professionalisering[44]).
Ten slotte bespreken we de criminele veelzijdigheid van daders. Worden criminelen veelzijdiger dan ze voorheen waren?

Do-it-Yourself

Do-it-Yourself (DIY) is een maatschappelijke ontwikkeling die al enige tijd gaande is. Het is een ontwikkeling waarbij individuen hun wensen trachten te realiseren door daaraan, zo veel als mogelijk, zelf invulling te geven, zonder de hulp van experts of professionals. Manifestaties van DIY zijn bijvoorbeeld bands en artiesten die hun muziek uitbrengen op platenlabels die zij zelf financieren of door hun fans laten financieren via crowdfunding, reizigers die hun accommodatie zelf online regelen via Airbnb, en wijkbewoners die elkaar informeren over duurzame energie en gezamenlijk zonnepanelen inkopen en installeren.
Technologie wordt steeds compacter en goedkoper, informatie wordt overal en voor iedereen toegankelijk. De bredere beschikbaarheid van veel technieken en informatie zal steeds meer mogelijkheden creëren voor individuen. DIY zal daarom de komende jaren alleen maar toenemen. En dit sluit aan bij de groeiende behoefte van consumenten aan producten op maat en de wens om minder afhankelijk te zijn van anderen om in de eigen behoefte te voorzien.
Naar verwachting zullen binnen DIY ook steeds meer criminele toepassingen te zien zijn. Zelfvervaardigde producten kunnen illegaal zijn of misbruikt worden. Zo circuleren er handleidingen en filmpjes op internet met behulp waarvan explosieven gemaakt kunnen worden en maken biotechnologische ontwikkelingen het binnenkort mogelijk opiaten te kweken op een manier die vergelijkbaar is met het bierbrouwproces. Met het oog op een toekomstig tekort aan pijnstillers startten synthetisch biologen in 2004 met het maken van morfineproducerende gist. Daarvoor zijn meerdere stappen nodig. Binnenkort kunnen met één soort gist alle zeventien reacties naar morfine in één keer efficiënt worden uitgevoerd met suiker als grondstof. Passend in de DIY-trend zou eenieder daarmee in principe in de eigen kelder opiaten kunnen kweken.

44 Een professionele manier van werken betekent hier het vakkundig, effectief en efficiënt organiseren van de criminele bedrijvigheid. Professionalisering houdt in dat een professionele manier van werken vaker voorkomt dan voorheen.

Een andere recente manifestatie van DIY op het terrein van drugs is de particuliere drugsproducent. Deze werkt geheel zelfstandig, zonder link met georganiseerde misdaad. Hij beschikt wel over kennis van IT, die hij aanwendt om via internet grondstoffen en hardware aan te schaffen en de synthetische drugs, na productie in eigen beheer, aan te bieden.

Een technologische ontwikkeling die naadloos in deze trend past, is het driedimensionaal printen (3D-printen). Met een 3D-printer kunnen aan de hand van digitale instructies in een CAD-bestand (*Computer Aided Drawing*) exacte driedimensionale kopieën gemaakt worden. De kosten van 3D-printers gaan in sneltempo omlaag (in enkele jaren van 50.000 euro naar 1000 euro in de loop van 2016) waardoor de technologie snel bredere toepassing zal krijgen. In de toekomst zal de vervanging van onderdelen van apparaten door middel van een CAD-bestand plaatsvinden. De producent stuurt het bestand per mail naar de aanvrager en die print het benodigde onderdeel zelf uit; nooit meer naar Ikea voor een kapot onderdeeltje. Distributie van ontwerpen gebeurt via internet, alleen de grondstoffen worden nog fysiek vervoerd. Er zullen websites komen die CAD-bestanden van talloze producten verkopen. Dit botst met het intellectueeleigendomsrecht.
Artikelen die tot dusver gebrekkig werden nagemaakt, zullen in de nabije toekomst worden geperfectioneerd met behulp van *ultrahigh resolution* 3D-scanning en -printing, zodat het resultaat niet meer van echt te onderscheiden is. Door middel van CAD-bestanden en 3D-printing kunnen belastingen en importheffingen worden ontdoken. Vindingrijke criminelen zullen steeds meer toepassingen van de 3D-printer ontdekken waarmee zij hun activiteiten kunnen faciliteren. Bij het plegen van ladingdiefstallen is al gebruikgemaakt van veiligheidsverzegelingen die met een 3D-printer vervaardigd zijn.

De Do-it-Yourselftrend en de voortschrijdende digitalisering hebben consequenties voor de criminele samenwerking. Personen zijn zelfstandig tot veel meer in staat dan voorheen. Het zwaartepunt in daderschap verschuift daardoor van groepen naar individuen. Voor zover individuen anderen nog nodig hebben, vinden de contacten niet meer *face to face* plaats, maar via internet. Het contact is niet meer plaatsgebonden; de criminele samenwerking internationaliseert. Dit alles heeft consequenties voor de opsporing. De verschuiving van het werkterrein van de opsporing naar het digitale domein vereist andere expertise dan de traditionele opsporingskennis en -vaardigheden. Verder zullen daders steeds vaker vanuit of via het buitenland opereren. Daardoor wordt de opsporing in Nederland steeds meer afhankelijk van toestemming en medewerking van buitenlandse instanties.

Een ontwikkeling die in belangrijke mate bijdraagt aan de mogelijkheden voor individuen om zelfstandig criminele activiteiten te ontplooien, is Crime-as-a-Service. Hieraan besteden we aandacht in het volgende tekstblok.

Crime-as-a-Service

In de ondergrondse economie is een vorm van dienstverlening ontstaan die wordt aangeduid als Crime-as-a-Service (CaaS): het aanbieden van kant-en-klare, eenvoudig te gebruiken softwarepakketten waarin de functionaliteiten om diverse vormen van cybercrime te plegen zijn voorgeprogrammeerd. CaaS maakt het mogelijk om bijvoorbeeld DDoS-aanvallen uit te voeren, ransomware te verspreiden en *Remote Access Tools* (RAT's) te gebruiken zonder te beschikken over bijzondere digitale vaardigheden. Het vereiste softwarepakket om bijvoorbeeld een DDoS-aanval uit te voeren is relatief gemakkelijk toegankelijk via marktplaatsen op het darkweb. De drempel om cybercrime te plegen wordt hierdoor verlaagd, wat het aantal potentiële aanvallers vergroot. Door CaaS zijn het niet alleen beroepscriminelen en statelijke actoren die cybercrime plegen, maar ook individuen zonder bijzondere technische kennis. Het risico bestaat dat jongeren via games of anderszins in aanraking komen met tools voor cyberaanvallen. Voor sommige van deze jongeren kan dit de start betekenen van een geheel andere dan een gamecarrière.

De dienstverlening wordt professioneler. Niet alleen wordt cybercrime gefaciliteerd door het aanbieden van software en tools, er komen ook steeds meer handleidingen en zelfs helpdesks voor de toepassing ervan en voor het regelen van de uitgaande kasstromen. Er zijn kant-en-klare moneymule-netwerken te koop. Zoals eerder in dit NDB werd beschreven, stellen moneymules hun bankrekening ter beschikking om daarop inkomsten te ontvangen die uit criminele activiteiten afkomstig zijn. Vaak betreft het individuele overeenkomsten tussen dader en moneymule of katvanger. In het geval van omvangrijker cybercriminaliteit is het belangrijk dat de inkomsten gespreid worden over buitenlandse moneymules, zodat de herkomst moeilijk te achterhalen is en het risico gespreid wordt.

Het Nationaal Cyber Security Centrum geeft aan dat het aantal dienstverleners toeneemt en de aangeboden diensten talrijk zijn geworden. De concurrentie die hierdoor ontstaat, zorgt ervoor dat de dienstverleners steeds betrouwbaarder en goedkoper worden en een steeds completer 'dienstenpakket' aanbieden.

Criminele uitbesteding en professionalisering

Voor veel criminele samenwerkingsverbanden is het moeilijk om alle essentiële deeltaken van een crimineel bedrijfsproces (zoals productie, transport, afzet, communicatie, afscherming, witwassen) te realiseren met uitsluitend inzet van eigen mensen en middelen. Het kan een csv bij het uitvoeren van deeltaken ontbreken aan benodigde kennis en vaardigheden, vereiste papieren, ruimtelijke voorzieningen, menskracht, materieel en materiaal.[45] Voor sommige deeltaken is het dan, vanwege een gemis of tekort, noodgedwongen aangewezen op uitbesteding. Ook overwegingen van risicobeperking kunnen een csv ertoe doen besluiten bepaalde onderdelen van het criminele bedrijfsproces uit te besteden.[46] Door het inschakelen van anderen die bijvoorbeeld risicovolle smokkeltrajecten voor hun rekening nemen, kunnen csv's zelf buiten schot proberen te blijven.

45 H. Moerland & F. Boerman (1999). *Georganiseerde misdaad en betrokkenheid van bedrijven* (Politiestudies nr. 25). Deventer: Gouda Quint.

46 E.W. Kruisbergen, H.G. van de Bunt & E.R. Kleemans (2012). *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom Lemma.

In de deelstudies die voor dit dreigingsbeeld zijn verricht, treffen we diverse voorbeelden aan van het inhuren van anderen voor het uitvoeren van onderdelen van de criminele bedrijvigheid. De belangrijkste voorbeelden van dergelijke criminele uitbesteding zijn de volgende:

- het verwerven van panden door makelaars, verhuurbemiddelaars en notarissen ten
- behoeve van hennepteelt;
- het inrichten van locaties voor hennepteelt door hokkenbouwers en elektriciens;
- het bouwen van koelers, destillatieapparatuur, drukvaten, reactievaten, kristallisatie-, filtratie- en mengapparatuur door hardware-bouwers ten behoeve van het vervaardigen van synthetische drugs;
- het dumpen van afvalstoffen van synthetischedrugsproductie door specialistische dumpers;
- het uithalen van verdovende middelen in de havens;
- het bieden van serverruimte door malafide *subcontractors* van hostingproviders ten behoeve van criminele activiteiten;
- het beschikbaar stellen van kennis van de beveiliging van nieuwe typen auto's;
- het aanbieden van apparatuur en software voor het manipuleren van beveiligingssystemen van voertuigen;
- het op bestelling leveren van gestolen auto's die zijn geprepareerd voor het uitvoeren van een ramkraak;
- het leveren van valse documenten door criminele specialisten die gebruikmaken van geavanceerde technieken;
- het verzenden van wapens en munitie door tussenkomst van een *parcel forwarding service*;
- het herstellen van onklaar gemaakte vuurwapens door technische experts;
- het wegsluizen en witwassen van criminele opbrengsten door gespecialiseerde csv's;
- het gebruikmaken van de diensten van payment service providers voor witwassen;
- het plannen en uitvoeren van criminele afrekeningen;
- het op bestelling leveren van automatische vuurwapens en vluchtauto's.

Bij criminele uitbesteding schakelen criminelen anderen in vanwege hun criminele specialisme. Deze werkwijze draagt doorgaans bij aan een betere organisatie van de criminele bedrijvigheid en getuigt daarmee van een zekere mate van professionaliteit. De hennepteelt en de synthetischedrugscriminaliteit in ons land kunnen wat dit betreft als professioneel worden beschouwd: zowat elk facet van de criminele bedrijvigheid wordt uitgevoerd door specialisten die meestal zelfstandig hun bijdrage leveren aan het geheel. Dit bemoeilijkt de aanpak van de organisatoren achter de schermen. Een specifieke aanpak gericht op het uit de markt halen van personen met een bepaald specialisme (bijvoorbeeld elektriciens) kan bewerkstelligen dat de criminele bedrijfsketen voor een bepaalde tijd wordt verstoord. In hoeverre dit resulteert in langdurige verstoring hangt af van de flexibiliteit van de criminele gemeenschap.

Hoewel uitbesteding in de hennepteelt en de synthetische drugs zeker niet iets van de laatste jaren is, bestaat wel de indruk dat het is toegenomen. Uit casuïstiek komt in elk geval het

beeld naar voren dat de uitbesteding ten behoeve van de hennepteelt zich wijder heeft verbreid; de branche is verder geprofessionaliseerd.
De uitbesteding van conflictbeslechting is hoofdzakelijk gelieerd aan de drugshandel. Dat opdrachtgevers specialisten inschakelen, is een teken van professionaliteit. Dit neemt niet weg dat het die 'specialisten' bij de uitvoering aan professionaliteit kan ontbreken, gezien de dodelijke persoonsverwisselingen die zich hebben voorgedaan.

Autofabrikanten laten hightech beveiligingssystemen ontwikkelen als preventieve maatregel tegen autodiefstal. In reactie hierop is een crimineel specialisme ontstaan: het analyseren en ontleden van de beveiliging van nieuwe typen auto's. Bestrijding en technologische vooruitgang aan de ene kant leiden tot de noodzaak tot aanpassingen aan de andere kant. Om succesvol te blijven moeten csv's innoveren. De georganiseerde autodiefstal kent niet alleen een complexe logistieke keten, een hoge organisatiegraad en criminele uitbesteding, maar de professionaliteit van deze csv's blijkt ook uit hun vermogen om op onderdelen de werkwijze aan te passen en te vernieuwen.

De mogelijkheden voor beveiliging die de technologie biedt, nopen niet alleen de georganiseerde illegale autobranche tot professionalisering. Ook bij het vervaardigen van valse documenten en vals geld moeten criminelen over steeds meer expertise en steeds geavanceerdere technieken beschikken om succesvol te zijn.
Een bijzonder geval vormt in dit verband de drugssmokkel via de Rotterdamse haven. Steeds meer van de bedrijvigheid in de haven, waaronder de doorgang van containers, gebeurt geautomatiseerd. Door de verregaande automatisering en robotisering is manipulatie van het computersysteem de enige manier waarop criminelen erachter kunnen komen waar een container zich bevindt. Door manipulaties kunnen ze niet alleen zien waar containers staan, ze kunnen deze ook laten verplaatsen, ze 'op groen' zetten zodat de douane ze niet controleert, of pincodes achterhalen die noodzakelijk zijn voor het ophalen van een container. Dat betekent dat criminelen toegang moeten krijgen tot deze systemen, hetzij door hacken (zelf of door het inhuren van hackers) hetzij door het omkopen van kantoorpersoneel of opsporingsambtenaren.
In eerdere dreigingsbeelden is al beargumenteerd dat met de toenemende automatisering en robotisering de mens hoe langer hoe meer de zwakste schakel wordt. Die constatering is juist gebleken en lijkt alleen maar meer van toepassing geworden, gelet op de gevallen van corruptie die de laatste tijd aan het licht zijn gekomen. Door de voortschrijdende automatisering van het havenbedrijf zal het aantal corruptiegevallen vermoedelijk verder groeien. Ook de toename van smokkel in de gemanifesteerde lading draagt hieraan bij, omdat deze methode niet zonder betrokkenheid van de zendende en ontvangende partij kan worden uitgevoerd. De druk op werknemers in de logistieke sector en bij toezichthoudende en controlerende instanties zal naar verwachting alleen maar groter worden.
Het gebruik van corruptie binnen de georganiseerde criminaliteit is in vorige dreigingsbeelden in den brede aan de orde gesteld. In dit dreigingsbeeld is een afzonderlijk onderzoek naar deze criminele werkwijze achterwege gelaten.

Voor meer inzicht in dit fenomeen verwijzen we naar het onderzoek naar corruptie dat aan de Universiteit Maastricht wordt uitgevoerd. Hier beperken we ons tot de signalering dat corruptie bij drugshandel (cocaïne, heroïne, hennep) nog immer een belangrijke rol speelt, en dat er in toenemende mate gebruik wordt gemaakt van corruptie bij drugssmokkel met containervervoer via de havens van Rotterdam en Antwerpen.

Op nog twee terreinen zien we professionalisering: mensensmokkel en cybercrime. Een restrictiever migratiebeleid (bijvoorbeeld ten aanzien van gezinshereniging) en striktere handhaving aan de grenzen van de Europese Unie en in Nederland maken migratie lastiger. Irreguliere migranten raken daardoor (nog) meer afhankelijk van mensensmokkelaars. De smokkelaars moeten professioneler te werk gaan om succesvol te kunnen zijn. Zij moeten immers hogere barrières in de vorm van grenscontroles aan de binnen- en buitengrenzen zien te nemen.
De dienstverlening gericht op het faciliteren van cybercrime (CaaS) is professioneler geworden. Dit blijkt uit de eerder besproken toename en verbreding van het aanbod en de grotere concurrentie onder aanbieders.

Ter afsluiting van dit tekstgedeelte een opmerking over witwassen. Door de vele witwasconstructies die worden gebruikt om de herkomst van crimineel geld te versluieren is het niet eenvoudig om wederrechtelijk verkregen voordeel te ontnemen. Uitbesteding van witwassen compliceert de aanpak van witwassen nog verder. Dat geldt eens te meer als er via die uitbesteding buitenlandse banken betrokken zijn. Sommige van dergelijke instituties zijn voor Nederlandse opsporingsinstanties namelijk moeilijk benaderbaar. Ook in dit verband draagt internationalisering bij aan de uitdaging waarvoor de opsporing zich gesteld ziet. De uitbesteding aan facilitatoren met een geheimhoudingsplicht, zoals advocaten en notarissen, compliceert de aanpak van witwassen eveneens. Dergelijke facilitatoren kunnen door criminelen onder druk worden gezet (corruptie, afpersing) om hun diensten in te zetten voor witwassen. De aanpak van deze facilitatoren wordt bemoeilijkt doordat hun diensten in beginsel onder de wettelijke geheimhoudingsplicht vallen.

Criminele veelzijdigheid

Het algemene beeld dat criminele samenwerkingsverbanden zich bezighouden met een breed scala aan criminele activiteiten, wordt in de deelstudies die ten grondslag liggen aan dit Nationaal dreigingsbeeld meer dan eens bevestigd. De traditionele indeling van csv's naar criminele hoofdactiviteiten lijkt achterhaald. Voorheen waren de csv's vaak samengesteld langs etnische lijnen. Was de etnische achtergrond of de nationaliteit van een csv bekend, dan gold dit vaak tegelijkertijd voor zijn criminele bezigheden. Wat dit betreft, lijken zich veranderingen te hebben voltrokken.

Zo zijn Turkse csv's veelzijdiger geworden: ze zijn niet meer uitsluitend actief in de heroïnehandel. In Brabant houden criminele Turkse familienetwerken zich bezig met hennep, cocaine, synthetische drugs, arbeidsuitbuiting, illegaal gokken en witwassen. Er vindt 'branche-

vervaging' plaats. De voorheen redelijk gescheiden markten zijn vermengd geraakt. Een reden voor de grotere veelzijdigheid zien sommigen in de opkomende markten in Turkije: het gebruik van cocaïne en ecstasy is daar toegenomen en de traditionele Turkse netwerken voorzien in de vraag.
Daarnaast zien we al langere tijd dat de heroïnemarkt in Nederland krimpt en inmiddels bescheiden van omvang is. In Europa is er nog een aanzienlijke markt, maar het aantal gebruikers daalt langzaam. De perspectieven om geld te verdienen met heroïnehandel nemen dus af. Het is goed mogelijk dat de Turkse netwerken gekozen hebben voor diversificatie als bedrijfsstrategie om de teruglopende inkomsten uit de heroïnehandel te compenseren. De genoemde factoren (groeiende vraagmarkt in Turkije en krimpende markt in Nederland) kunnen in combinatie verantwoordelijk zijn voor de geconstateerde diversificatie.

Diversificatie vinden we niet uitsluitend bij de Turkse csv's, het is een bredere trend in het Nederlandse criminele landschap. Uit opsporingsdossiers blijkt dat fraudeurs niet alleen allerlei soorten fraude plegen, maar zich bezighouden met veel verschillende vormen van criminaliteit: het een wordt gepleegd (fraude) om het andere (drugs) te bekostigen, waarna de criminele opbrengsten worden witgewassen (in vastgoed) en de organisatie kan groeien. Ook binnen de georganiseerde vermogenscriminaliteit zien we de specialisaties vervagen. Vaak worden verschillende vermogensdelicten gecombineerd, maar ook andere combinaties zijn mogelijk, zij het dat we die in mindere mate aantreffen. Internationaal opererende dadergroepen maken zich bijvoorbeeld schuldig aan diefstal, overvallen, straatroof, voertuigcriminaliteit, drugshandel, oplichting, mensenhandel en openlijke geweldpleging. Hoe professioneler de dader, des te eerder hij zich met midden- en zware criminaliteit gaat bezighouden. Europol ziet in de veelzijdigheid van deze dadergroepen een belangrijke verklaring voor hun 'succes'.
Vuurwapenhandel is van oudsher een branche die op zichzelf niet buitengewoon winstgevend is, maar 'meelift' met andere vormen van grensoverschrijdende criminaliteit. Dat werd ook al geconstateerd in het NDB2012. Vrijwel alle verdachten van vuurwapensmokkel houden zich ook met andere vormen van criminaliteit bezig, zoals de handel in verdovende middelen en het plegen van liquidaties. Het beeld van de criminele veelzijdigheid van vuurwapenhandelaars dat al jaren bestaat, blijft intact.
Illegale teelt van en handel in hennep levert veel geld op. Dat wordt aangewend om andere criminele activiteiten te financieren. Voorbeelden daarvan zijn de aankoop van grondstoffen voor synthetische drugs en de inkoop van een partij cocaïne. Geconstateerd wordt dat de hennepteelt en -handel eenvoudig toegankelijk is en voorkomt bij veel criminele samenwerkingsverbanden, ook wanneer deze zich primair met een andere vorm van criminaliteit bezighouden. Inherent aan de georganiseerde hennepteelt en -handel zijn de criminele activiteiten met betrekking tot witwassen en fraude. De illegale winsten worden witgewassen via diverse constructies. Fraude wordt dikwijls gepleegd om bepaalde aspecten van de hennepteelt te faciliteren. Voorbeelden daarvan zijn hypotheekfraude, faillissementsfraude en fraude met betrekking tot identiteitsdocumenten en werkgeversverklaringen voor het verwerven van panden.

Zo zijn er legio voorbeelden te geven van de diversificatie in de criminele bedrijfsvoering.

Het belang van deze signalering betreft niet alleen een verandering in het algemene beeld van de georganiseerde criminaliteit, maar ook en misschien wel vooral de consequenties ervan voor de aanpak van criminele netwerken en samenwerkingsverbanden en de daarvoor benodigde expertise.

1.5 Georganiseerde criminaliteit in de wijken: onaantastbaarheid en normvervaging

In 2014 verscheen een rapport van Tops en Van der Torre waarin verslag wordt gedaan van een onderzoek naar de resultaten van de zogenoemde wijkenaanpak.[47] Een belangrijk thema in het rapport is de manier waarop georganiseerde of ondermijnende criminaliteit zich manifesteert in woonwijken en welke gevolgen dat heeft. Dit rapport heeft raakvlakken met het NDB, en wel zodanige raakvlakken dat in de deelprojecten die ten behoeve van het NDB zijn uitgevoerd, speciale aandacht besteed is aan de vraag welke gevolgen 'de' georganiseerde criminaliteit heeft op wijkniveau. Deze gevolgen hebben meegewogen bij de kwalificatie van dreiging van de criminele verschijnselen die in deel 2 van dit NDB zijn behandeld. Ze staan daar verspreid over de tekst, waardoor het belang ervan gemakkelijk aan de aandacht kan ontsnappen. Onder de noemer 'georganiseerde criminaliteit in de wijken' brengen we daarom in deze paragraaf een aantal van die gevolgen bij elkaar.

Tops en Van der Torre concluderen onder andere dat in kwetsbare wijken een cumulatie van problemen bestaat die een voedingsbodem voor criminele activiteiten vormt. Voor een deel bestaan die criminele activiteiten uit 'zichtbare' aangiftecriminaliteit, voor een ander deel uit minder zichtbare deelname aan georganiseerde vormen van criminaliteit zoals hennepteelt, fraude, productie van synthetische drugs, arbeidsuitbuiting en witwassen. Tops en Van der Torre zeggen daarover onder meer: "Er zijn aanwijzingen dat in een dergelijke context een symbiotische verhouding tot vormen van (georganiseerde) criminaliteit kan ontstaan (...). Activiteiten van criminelen (niet zelden ook van criminele families), worden dan met de mantel der liefde bedekt. Vanwege verschillende redenen hebben criminelen een positief imago. Zij weten de autoriteiten uit te dagen. Als ze aan jouw kant staan springen ze bij, wanneer je het nodig hebt. Soms is er ook sprake van intimidatie. Meestal is er sprake van een mix van deze factoren" (p. 8). De georganiseerde criminaliteit biedt een "alternatieve kansenstructuur"; waarom zou je je inzetten voor een lang niet zekere respectabele en productieve carrière, wanneer je buurjongen met betrekkelijk geringe inspanningen over een mooie auto en dito vriendin beschikt? Maar het gaat niet alleen om min of meer actieve deelname aan criminele activiteiten. Het gaat ook om iets wat kan worden aangeduid als 'normvervaging' bij bewoners die niet actief aan criminaliteit deelnemen, maar er in het grijze gebied tussen legaal en illegaal van profiteren en in voorkomende gevallen 'de andere kant op kijken'. Deze conclusie wordt goeddeels bevestigd door observaties in verschillen-

47 P.W. Tops & E. van der Torre (2014). *Wijkenaanpak en ondermijnende criminaliteit.* S.l.: s.n.

de NDB-deelrapportages, zoals die over hennep, afpersing, georganiseerde vermogenscriminaliteit, cocaïne, heroïne en arbeidsuitbuiting. Een greep daaruit bespreken we hier.

De ondermijning van de leefbaarheid in toch al kwetsbare wijken is een zorgpunt. Hennepkwekerijen komen overal voor, zowel in 'goede' als in 'zwakke' wijken. Vooral de kwetsbare en zwakke wijken blijken echter vruchtbare voedingsbodems voor criminele netwerken. Hierdoor ontstaat een samenleving waarin criminaliteit en crimineel geld als 'normaal' worden beschouwd. Mensen zien dat er veel geld wordt verdiend, zonder dat daar belasting over wordt betaald. De morele acceptatie in combinatie met hoge opbrengsten, een lage pakkans en milde straffen maakt dat het toetreden tot de hennepindustrie voor veel mensen aantrekkelijk is.
Een negatief aspect van drugshandel is de (vermeende) onaantastbaarheid van personen die zich daarmee bezighouden. Bij drugshandel is de pakkans relatief gering, terwijl de winsten enorm zijn. De rijkdom en status die met de handel bereikt zijn, vertalen zich vaak in patsergedrag: het bezit van grote hoeveelheden contant geld en de aanschaf van dure sieraden of kleding. Omdat jongeren voldoende bewijs zien dat deze route loont, heeft de drugshandel een aanzuigende werking op hen.
In verschillende sectoren, zoals de haven- en de transportsector, is soms sprake van normvervaging. In deze sectoren heerst (van oudsher) een cultuur die zich kenmerkt door een sterke onderlinge verbondenheid en geslotenheid ten opzichte van de buitenwereld. Mensen of bedrijven kennen elkaar en zijn sterk op elkaar gericht. Een ongeschreven regel is dat er geen informatie wordt gedeeld met buitenstaanders, en er lijkt een taboe te liggen op 'uit de school klappen' en op het melden van misstanden. Hier lijken ook andere normen en waarden te heersen ten aanzien van criminaliteit. Dit schept gelegenheid voor het plegen en afschermen van criminele activiteiten.
Bij een opkoper, bij een autohandelaar of op lokale markten lijken veel afnemers goedkope goederen met een bedenkelijke herkomst inmiddels te appreciëren. Dat blijkt bijvoorbeeld uit de casus van een markthandelaar die daarop inspeelt bij het aanprijzen van zijn waar. Hij ontdoet de goederen in zijn kraam juist niet van diefstalkenmerken: de sticker met prijs en winkelketen. Daardoor verkopen ze beter. Er blijkt immers uit dat het om echte (merk)artikelen gaat. Van enige scrupules of angst om bij het kopen of verkopen van een gestolen goed – een misdrijf – betrapt te worden, lijkt geen sprake. Blijkbaar is het voor zowel verkopers als kopers heel gewoon dat er gestolen waar wordt verkocht. Markten en opkoopbedrijven waar deze praktijken veelvuldig plaatsvinden, zijn aan te merken als locaties die aanleiding geven tot normvervaging. Dat leidt tot meer heling en tot een toename van de criminele activiteiten die daaraan voorafgaan.

Normvervaging die het gevolg is van de criminele activiteiten van malafide autohandelaars hangt vooral samen met het feit dat veel van deze ondernemers al decennialang in dezelfde wijken redelijk ongemoeid kunnen opereren. Veel consumenten en bedrijven zijn al jaren klant en kennen de schimmige praktijken. Er is in de loop der jaren een groot vertrouwd netwerk van afnemers ontstaan bij wie de periode van kritisch vragen stellen over de

herkomst van aangeboden waar allang verstreken is. Een aantal malafide autohandelaars hebben in de voorbije jaren een gezaghebbende positie in de lokale gemeenschap opgebouwd en spreiden dat ook ten toon. Zij vertonen binnen die lokale gemeenschap openlijk patsergedrag, bijvoorbeeld door in dure auto's rond te rijden. De gemeenschap rondom dit soort criminelen is buitengewoon gesloten. Er is een groep burgers die niet durft te getuigen uit angst voor represailles. Anderen trekken profijt van de opbrengsten van deze criminelen omdat zij klant zijn. In een paar gevallen profiteert ook de gemeenschap als geheel van de opbrengsten van deze csv's. In twee opsporingsonderzoeken bleken twee csv's ieder een lokale voetbalclub te sponsoren. Beide voetbalclubs hadden een vermoeden omtrent de herkomst van de sponsorgelden maar stelden geen vragen.
In een aantal steden of regio's zijn er groepen die zich onaantastbaar gedragen of hebben gedragen. Deze groepen hebben zich daarbij ook schuldig gemaakt aan afpersing. Afpersing is vaak een onderdeel van een breder criminaliteitsprobleem, waar andere vormen van georganiseerde en ernstige criminaliteit, zoals financieel-economische fraude, een rol kunnen spelen. Het ultieme risico bestaat dat er illegale economieën en zogenoemde (etnische) monoculturen ontstaan waar de politie en andere opsporingsdiensten nauwelijks een informatiepositie (meer) hebben.

De aanwezigheid van georganiseerde criminaliteit in kwetsbare wijken heeft een heel scala aan (in)directe gevolgen, variërend van gelaten acceptatie tot openlijk strafbaar gedrag. Vooral het patsergedrag, de dure auto en de gepercipieerde onaantastbaarheid komen in verschillende deelrapportages naar voren. Alle manifestaties bij elkaar resulteren in een subcultuur binnen de betreffende wijken waarin georganiseerde criminaliteit een geaccepteerd fenomeen is. Er is sprake van een verschuiving van normen. In deze wijken wordt tegen de meest succesvolle criminelen opgekeken en is de grens tussen 'goed' en 'kwaad' niet duidelijk waarneembaar. Hierdoor kunnen bewoners ook tegen hun wil betrokken raken bij strafbare praktijken.
Juist de veelheid aan symptomen met hun eigen dynamiek maakt duidelijk dat de exclusieve aanpak ervan door politie en Openbaar Ministerie niet tot de gewenste resultaten zal leiden. Dat wordt hier niet voor de eerste keer gesignaleerd. Daarom is in veel gemeenten gekozen voor een integrale aanpak waarbij politie, Openbaar Ministerie, openbaar bestuur, bedrijfsleven, Belastingdienst en welzijnswerk gezamenlijk onderzoek doen en actie ondernemen. Deze samenwerking krijgt onder meer gestalte in de Regionale Informatie en Expertise Centra (RIEC's). Over heel Nederland zijn er daarvan tien actief. De RIEC's brengen op gezette tijden bestuurlijke criminaliteitsbeeldanalyses uit, waarin zij verslag doen van de belangrijkste problematiek in de regio waarin zij actief zijn, en suggesties doen voor de aanpak ervan.

2 Nabeschouwing

2.1 Inleiding

In dit laatste hoofdstuk van het Nationaal dreigingsbeeld 2017 zullen we nagaan hoe dit NDB zich verhoudt tot de eerdere NDB's. Daartoe worden alle kwalificaties over de jaren heen naast elkaar gezet en met elkaar vergeleken: zijn daar patronen in te ontdekken en welke verschuivingen hebben plaatsgevonden? Omdat met het NDB beoogd wordt onderbouwing te bieden voor het vaststellen van beleidsprioriteiten, worden ook de opeenvolgende prioriteiten vergeleken en tegen de resultaten van de NDB's afgezet. Ten slotte besteden we aandacht aan criminele verschijnselen waarvan de gevolgen voor de Nederlandse samenleving zijn toegenomen en waarvan het aannemelijk is dat de ernst ervan blijft toenemen.

2.2 Nabeschouwing

In het NDB2012 werden 36 verschillende criminele verschijnselen voorzien van een kwalificatie van dreiging. Er werd 12 maal tot een 'dreiging' besloten, 12 maal tot 'geen concrete dreiging' en 12 maal tot een 'witte vlek'. Geen enkel crimineel verschijnsel kreeg de kwalificatie 'voorwaardelijke dreiging'. Deze evenwichtige verdeling is voor een gedeelte toeval, want als we deze resultaten met 2017 vergelijken, zien we dat in 17 gevallen sprake is van een dreiging, 4 maal van een witte vlek, 12 maal van geen concrete dreiging en 1 maal van een voorwaardelijke dreiging. De vergelijking gaat niet helemaal op, doordat voor het NDB2017 verschillende categorieën zijn samengevoegd. Zo is de categorie 'cannabis' van drie kwalificaties teruggebracht naar één, en de categorie kinderpornografie van twee naar één. Opvallend is wel dat aanmerkelijk minder vaak tot een 'witte vlek' is besloten. De methode van kwalificeren en de criteria zijn nagenoeg gelijk gebleven. De voorzichtige conclusie luidt dus dat er meer relevante informatie ter beschikking staat op grond waarvan we tot een inschatting van de dreiging van het betrokken criminele verschijnsel kunnen komen.

Als we voor de drie NDB's (2008, 2012 en 2017) die met een vergelijkbare methode gemaakt zijn[48], bezien welke constanten er zijn, zien we het volgende:
Het 'drugscluster' vertoont door de jaren heen een stabiele kwalificatie. Alle jaren zijn de vier onderscheiden categorieën als dreiging gekwalificeerd. Hierbij moet worden aangetekend dat de argumentatie die ertoe leidt dat de handel in en distributie van heroïne als dreiging wordt gekwalificeerd, steeds minder leunt op de directe gevolgen van het gebruik in Nederland en meer en meer op de rol van Nederland als transitland. Dit komt vooral doordat het gebruik van heroïne in Nederland gestaag afneemt, terwijl dat in de grotere Europese landen veel minder het geval is. Er worden in ons land steeds minder opsporingsonderzoeken naar de handel in en distributie van heroïne gestart.

48 Het NDB2004 had een andere invalshoek, namelijk die van de thema's, zoals criminele samenwerking, contrastrategieën, en uitbreiding van de Europese Unie. De schadecategorieën in het NDB2017 zijn uitgebreid met het onderwerp 'ondermijning'. In bijlage 3 wordt vermeld hoe dat is geoperationaliseerd.

Een ander delict dat telkens als dreiging werd gekwalificeerd, is seksuele uitbuiting. Het centrale argument is steeds dat de gevolgen voor de slachtoffers buitengewoon ernstig zijn. Dan zijn er vier categorieën van financieel-economische criminaliteit: witwassen, beleggingsfraude, fiscale fraude en accijnsfraude. Ook deze criminele verschijnselen werden onveranderlijk van de kwalificatie 'dreiging' voorzien. De schade ervan is voornamelijk financieel en loopt in de miljarden.
Ten slotte zijn er twee vermogensmisdrijven die in georganiseerde vorm veel schade veroorzaken: overvallen en woninginbraken. Naast de financiële schade wegen de traumatische ervaringen van de slachtoffers van deze delicten zwaar.
In totaal tellen de drie NDB's elf criminele verschijnselen die permanent een dreiging vormen voor de Nederlandse samenleving (zie tabel 22: de blauwe vlakken).

Van een zestal delicten kunnen we zeggen dat ze in dit NDB als dreiging zijn gekwalificeerd terwijl dat eerder niet telkens het geval was: arbeidsuitbuiting, mensensmokkel, vuurwapens en explosieven, kinderpornografie, verzekeringsfraude en faillissementsfraude (zie tabel 22: de oranje vlakken).

Van dertien criminele verschijnselen kunnen we zeggen dat ze door de jaren heen ofwel geen concrete dreiging voor de Nederlandse samenleving vormden volgens de criteria die voor het NDB gelden, ofwel zodanig afgenomen zijn dat het geen dreigingen meer zijn. Overigens wil dat niet zeggen dat ze geen probleem vormen. Het wil vooral zeggen dat deze soorten georganiseerde criminaliteit in vergelijking met andere soorten relatief minder ernstige gevolgen voor de samenleving hebben. Dit betreft de gevolgen van het verschijnsel in zijn totaliteit en laat onverlet dat in individuele gevallen de gevolgen zwaarwegend kunnen zijn voor de betrokkenen. Het gaat om vals geld, skimmen, diverse vormen van horizontale fraude en diverse vormen van vermogenscriminaliteit (zie tabel 22: de paarse vlakken).

Dan blijven er nog een paar verschijningsvormen over die niet in te delen vallen in een van de bovengenoemde categorieën, omdat ze niet consequent onderzocht zijn: vervalste medicijnen, merkfraude, winkeldiefstal, heling, bedrijfsspionage, orgaanhandel, kunst en antiek, illegale kansspelen en matchfixing. Van winkeldiefstal en heling kan gezegd worden dat telkens gebleken is dat er onvoldoende informatie over beschikbaar is om tot een verantwoorde kwalificatie van dreiging te komen (zie tabel 22: de groene vlakken).

Tabel 22. Kwalificaties door de jaren heen[49]

Criminele verschijnselen	Kwalificatie NDB2008	Kwalificatie NDB2012	Kwalificatie NDB2017
Illegale markten			
Cocaïne	D+	D+	D+
Heroïne	D+	D+	D+
Synthetische drugs	D+	D+	D+
Cannabis	D+	WV/WV/D+	D+
Seksuele uitbuiting	D+	D+	D+
Arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening	WV	WV	D+
Mensensmokkel	WV/D-	D-	D+
Vuurwapens en explosieven	D-	D+	D+
Kinderpornografie	WV/D-	WV/D+	D+
Vals geld	D-	D-	D-
Mensenhandel: orgaanhandel	-	-	D-
Vervalste medicijnen	-	D-	-
Illegale kansspelen	-	-	D-
Matchfixing	-	-	D-
Fraude en witwassen			
Witwassen	D+	D+	D+
Beleggingsfraude	D+	D+	D+
Fiscale fraude	D+	-	D+
Accijnsfraude	D+	-	D+
Verzekeringsfraude	-	WV	D+
Faillissementsfraude	-	WV	D+
Fraude met online handel	-	D-	D-
Fraude met betaalmiddelen	-	D-	D-
Voorschotfraude	D+	D+	D-
Acquisitiefraude	-	WV	D-
Hypotheekfraude	-	WV	D-
Telecomfraude	-	D-	WV
Merkfraude	-	WV	-
Vermogenscriminaliteit			
Woninginbraak	VD	D+	D+
Overvallen	D+	D+	D+
Bedrijfsinbraak	D-	D-	D-
Kraken op automaten	D-	D-	D-
Ladingdiefstal	D+	WV	D-
Georganiseerde autocriminaliteit	D-	D-	VD
Afpersing	-	D-	WV
Skimming	D-	D-	-
Winkeldiefstal	VD	WV	WV
Heling	WV	-	WV
Kunst en antiek	-	D-	-
Bedrijfsspionage	-	WV	-

D+ = dreiging; D- = geen concrete dreiging; WV = witte vlek; VD = voorwaardelijke dreiging

49 Mensensmokkel en kinderpornografie zijn van twee kwalificaties teruggebracht naar één.

Er bestaat door de jaren heen binnen de context van het NDB een betrekkelijk grote consensus over welke vormen van georganiseerde criminaliteit een gevaar vormen, welke dat mogelijk gaan worden en welke relatief minder problematisch zijn. Dat is van belang, omdat de hoofddoelstelling van het NDB is een rationele bijdrage te leveren aan de strategische prioritering in de aanpak van de georganiseerde criminaliteit. Prioritering is noodzakelijk opdat de beperkte mensen en middelen zo doelmatig en doeltreffend mogelijk worden ingezet. Op basis van het NDB formuleert het College van procureurs-generaal een advies daarover aan de minister van Veiligheid en Justitie. Dit advies is de leidraad voor een programma waarin de strategie in de aanpak van georganiseerde criminaliteit uiteen wordt gezet. Dit programma wordt aangeboden aan de Tweede Kamer. Gewoonlijk worden de prioriteiten geput uit de lijst van dreigingen zoals die in het NDB benoemd worden. Dat is echter geen wet van Meden en Perzen, het staat de minister vrij daarvan af te wijken.

Hieronder bezien we voor de jaren 2008 en 2012 welke prioriteiten de minister heeft gesteld en hoe die zich verhouden tot de resultaten van de respectievelijke NDB's.
Voor de periode 2008-2012 werden de volgende "speerpunten van beleid" geformuleerd:[50]

- witwassen (onder andere via investeringen in vastgoed);
- mensenhandel en -smokkel;
- terrorisme en andere extreme vormen van ideologisch gemotiveerde misdaad;
- grootschalige hennepteelt;
- handel in cocaïne;
- handel in heroïne;
- synthetische drugs en met name de productie van en handel in ecstasy en amfetamine.

Zoals we kunnen zien, werden zeven speerpunten benoemd die uit het NDB2008 afkomstig zijn; terrorisme werd in het NDB niet onderzocht. Op één na (mensensmokkel) werden deze allemaal als dreiging gekwalificeerd. Voor het feit dat mensensmokkel toch op de lijst van prioriteiten terecht is gekomen, wordt de volgende reden gegeven: "In de praktijk blijkt dat illegale (im)migratie vaak samengaat of wordt gevolgd door uitbuiting, wat als mensenhandel strafbaar is gesteld. Gezien de nauwe onderlinge samenhang verdient het daarom overweging om mensensmokkel en -handel samen als speerpunt te behouden."
Het zijn criminele verschijnselen die door de jaren heen telkens als dreiging zijn bestempeld. In dat opzicht is het een logisch lijstje. Dat neemt niet weg dat zes dreigingen niet in aanmerking kwamen voor prioritering: beleggingsfraude, fiscale fraude, accijnsfraude, voorschotfraude, overvallen en ladingdiefstal. In de brief aan de Tweede Kamer wordt betrekkelijk weinig gezegd over de motivering daarvoor, behalve: "Het aantal speerpunten bij de aanpak van de georganiseerde criminaliteit dient beperkt te blijven om te voorkomen dat de capaciteit van politie en justitie te zeer wordt versnipperd."

50 Tweede Kamer, vergaderjaar 2008-2009, *Kamerstuk* 29911, nr. 17.

Ook in 2012 werd een lijst met prioriteiten per brief aan de Tweede Kamer[51] voorgesteld. Ditmaal waren het de volgende prioriteiten:

- productie en/of in- en uitvoer van drugs: cocaïne, heroïne, synthetische drugs, cannabis/hennepteelt;
- mensenhandel (inclusief mensensmokkel);
- witwassen van crimineel verkregen vermogen;
- zware of georganiseerde fraude, met speciale aandacht voor horizontale fraude en misbruik van rechtspersonen;
- kinderpornografie, met speciale aandacht voor de productie ervan;
- cybercrime, met name hightechcrime;
- (zware) milieucriminaliteit.

In 2012 zien we dezelfde vormen van georganiseerde criminaliteit terugkomen, aangevuld met horizontale fraude, kinderpornografie, cybercrime en milieucriminaliteit. Ook nu weer komen verschillende verschijnselen die in het NDB als dreiging zijn gekwalificeerd, niet voor in de lijst. Over vermogenscriminaliteit wordt gezegd dat hiervoor speciale aandacht komt bij de aanpak van *highimpactcrime* (confronterende criminaliteit die grote gevolgen heeft voor het slachtoffer). Het gaat daarbij niet alleen om de georganiseerde vorm ervan. Voorbeelden zijn overvallen en woninginbraak. Over de als dreiging gekwalificeerde vuurwapenhandel wordt gezegd dat dit onderwerp meegenomen wordt bij de bestrijding van andere vormen van (georganiseerde) criminaliteit. Twee onderwerpen, cybercrime en milieucriminaliteit, zijn in het NDB niet van een kwalificatie voorzien, omdat de verschijningsvormen ervan zo divers zijn dat een aparte behandeling ervan noodzakelijkerwijs onvolledig is en geen recht doet aan de complexiteit van de categorieën. Wel werd er in het NDB op gewezen dat milieucriminaliteit een vorm van organisatiecriminaliteit is die ernstige gevolgen kan hebben, en van cybercrime werd gezegd dat het gebruik van internet als instrument ter facilitering van het criminele bedrijf “alomtegenwoordig” is. Voldoende reden om het als prioriteit op te nemen.
De eerder als ‘constanten’ benoemde categorieën drugs, mensenhandel en witwassen keerden terug op de prioriteitenlijst, terwijl door de toevoeging van andere onderwerpen een actualisering plaatsvond.

Concluderend kunnen we zeggen dat de uitkomsten van de opeenvolgende NDB’s gereflecteerd worden in de prioriteitstelling van de minister. Dat een aantal van de geïdentificeerde dreigingen niet tot prioriteit benoemd zijn, is het gevolg van schaarste aan mensen en middelen – precies de reden waarom überhaupt tot prioriteren moest worden overgegaan. Grosso modo betekent dit dat met de diverse NDB’s het gestelde doel is bereikt.
Wat opvalt, is dat er weliswaar enkele vernieuwingen plaatsvinden in de prioriteiten, wat verschuivingen in de kwalificaties en aanvullingen op de lijst van te onderzoeken verschijnselen, maar dat door de bank genomen de klassieke vormen van georganiseerde criminaliteit

51 Tweede Kamer, vergaderjaar 2012-2013, *Kamerstuk* 29911, nr. 79.

in de opeenvolgende NDB's telkens terugkeren als dreiging. Er worden betrekkelijk weinig nieuwe criminele markten geëxploiteerd. Dat blijkt ook uit de resultaten van het project Nieuwe criminele verschijnselen dat in 2015 ten behoeve van het NDB werd uitgevoerd. De onderzoekers vonden geen nieuwe vormen van georganiseerde criminaliteit die in aanmerking kwamen voor opname in het NDB. Wel zien we een steeds toenemende invloed van digitale technologie in de criminele bedrijfsvoering. Hieraan hebben we aandacht geschonken in het hoofdstuk over cybercrime en in het hoofdstuk Signaleringen. Deels gaat het om technologische innovaties voor algemeen gebruik die ook een criminele toepassing kunnen krijgen, deels om toepassingen die speciaal voor het bedrijven van criminaliteit worden ontwikkeld: de *exploit kits*, malware en ransomware.
Als we de digitale ontwikkelingen even buiten beschouwing laten, bestaat door de jaren heen de 'ruggengraat' van zowel de NDB-dreigingen als de ministeriële prioriteiten dus uit de meer klassieke vormen van georganiseerde criminaliteit.

In deel 2 van dit NDB zijn de verschillende criminele verschijnselen elk apart voorzien van een kwalificatie van dreiging. Ze zijn, bij wijze van spreken, geïsoleerd behandeld. Wat de kwalificatie betreft, is de gradatie in dreiging beperkt: iets is een 'dreiging' of 'geen dreiging'. De twee overige kwalificaties, 'witte vlek' en 'voorwaardelijke dreiging', zijn een 'uitwijkmogelijkheid' wanneer de andere niet voldoen. Een vraag die zich opdringt, is welke van de dreigingen de afgelopen jaren nu het meest in ernst zijn toegenomen en van welke verwacht wordt dat ze de komende jaren ernstiger worden.
Alles overziend kunnen we concluderen dat van de zeventien geïdentificeerde dreigingen er vier zijn waarvan gezegd kan worden dat ze niet alleen in de afgelopen periode ernstiger zijn geworden, maar ten aanzien waarvan ook verwacht wordt dat de ernst ervan in de komende jaren minstens gelijk zal blijven en misschien zal toenemen. Het is belangrijk zich te realiseren dat het niet per se om de ernstigste bedreigingen gaat; het gaat hier uitsluitend om de *toename* van de ernst van de dreiging.

Als eerste wordt gewezen op *arbeidsuitbuiting*, waartoe in dit verband ook criminele uitbuiting en gedwongen dienstverlening gerekend worden. In de afgelopen jaren is het aantal strafrechtelijke onderzoeken door de Inspectie Sociale Zaken en Werkgelegenheid en de politie ongeveer verzesvoudigd. Nu mag hieruit niet de conclusie getrokken worden dat ook de werkelijke omvang verzesvoudigd is. Omdat dit delict een aantal jaren geleden meer aandacht heeft gekregen, is ook het aantal onderzoeken toegenomen. We mogen echter aannemen dat er aanleiding was om tot intensivering van de handhaving over te gaan. Ook cijfers van het Coördinatiecentrum tegen Mensenhandel (CoMensha) wijzen in de richting van een toename: in 2014 was er sprake van 259 geregistreerde slachtoffers, terwijl dit er in 2010 nog 128 waren.
De slachtoffers van deze vormen van uitbuiting vinden we vooral bij kwetsbare groepen. De verwachting is dat in Nederland de komende jaren de aanwezigheid van dergelijke kwetsbare groepen zal toenemen. Demografische ontwikkelingen, zoals grote migratie- en vluchtelingenstromen, ontwikkelingen op de arbeidsmarkt en economische ontwikkelingen, zoals

verdergaande flexibilisering en globalisering, zullen ertoe bijdragen dat er grote groepen mensen komen die in een (financieel) kwetsbare positie verkeren en daardoor vatbaar zijn voor uitbuiting. Europol en Interpol verwachten hierdoor een toename van arbeidsuitbuiting, criminele uitbuiting en gedwongen dienstverlening. Mensensmokkelorganisaties zullen zich actiever gaan bezighouden met mensenhandel of nauwe(re) samenwerkingsverbanden met mensenhandelaars aangaan. De praktijk wijst uit dat sommige van de uitgeprocedeerde asielzoekers gedurende langere tijd illegaal in Nederland blijven; naar verwachting vormen zij een kwetsbare groep voor uitbuiting.

Ten tweede gaat het om productie van, handel in en smokkel van *cannabis,* en dan vooral de nederwietvariant. Cannabis is verreweg de meestgebruikte illegale drug in Europa. In 2014 gaf 8 procent van de volwassen Nederlandse bevolking aan, het voorgaande jaar cannabis gebruikt te hebben, en 4,6 procent de voorgaande maand. Alleen in Spanje (9,2% en 6,6%) en in Frankrijk (11,1% en 6,6%) is het gebruik hoger dan in Nederland.
De totale binnenlandse consumptie van in Nederland geteelde cannabis wordt in onderzoek van het WODC voor de jaren 2012 en 2013 geschat op een hoeveelheid die ligt tussen de 28 en 119 ton.
Wat problematisch gebruik betreft, laat het Landelijk Alcohol en Drugs Informatie Systeem (LADIS) zien dat de laatste jaren een stijging van aanmeldingen heeft plaatsgevonden: het aantal cliënten dat ingeschreven stond wegens een primair cannabisprobleem is tussen 2005 en 2014 twee keer zo groot geworden. Het aandeel van cannabis in alle hulpverzoeken met betrekking tot drugsgebruik is eveneens toegenomen in de loop der jaren: in 2005 had 17 procent van alle drugsgerelateerde hulpvragen betrekking op cannabis, in 2011 was dit percentage gestegen naar 33. Sindsdien is het vrij stabiel gebleven.
In toenemende mate bereiken ons de laatste jaren berichten dat de teelt van hennep ernstige gevolgen heeft. Vooral in het zuiden van Nederland wordt daarover de noodklok geluid, omdat de problematiek hand over hand toeneemt. Kwekerijen worden niet alleen op het platteland aangetroffen, ook in woningen in stadswijken worden ze ontdekt. Er zijn aanwijzingen (zie ook de paragraaf over georganiseerde criminaliteit in de wijken in het hoofdstuk Signaleringen) dat de kweek van nederwiet in woonwijken onder andere tot gevolg heeft dat de drempel om zich in te laten met criminele activiteiten relatief laag is. Onderzoek heeft uitgewezen dat sommige wijken een vrijplaats lijken te worden waarin tegen criminelen wordt opgekeken en een criminele carrière een ‘normaal’ alternatief wordt gevonden. Bovendien is er sprake van bedreigingen aan het adres van lokale bestuurders en verweving van de onder- met de bovenwereld.
Er zijn politieke initiatieven om hennepteelt verdergaand te reguleren. Of dit leidt tot andere wetgeving en zo ja, welke betekenis die wetgeving dan zal hebben voor de hierboven beschreven problematiek, moet nog blijken.

De derde dreiging waarvan de ernst is toegenomen, betreft *cocaïne*, een onveranderd populaire drug in Europa. Het jaarlijkse aantal cocaïnegebruikers in de Europese Unie wordt geschat op 3,6 miljoen. Zij consumeren ongeveer 91 ton cocaïne met een straatwaarde van 5,7 miljard euro. De Nederlandse consumptie wordt op basis van het aantal gebruikers geschat op ruim 3,6 ton per jaar. Het aanbod van cocaïne is groot: jaarlijks worden duizenden kilo's in de Rotterdamse haven in beslag genomen en die hoeveelheden nemen de laatste tijd toe. De consumentenprijs van cocaïne is in Nederland relatief stabiel. Ondanks inbeslagnames schommelt de prijs in Nederland al sinds 2008 rond de 50 euro per gram, ook nu de zuiverheid van cocaïne de laatste jaren verder lijkt toe te nemen. Dat wijst op ruime beschikbaarheid van deze drug in ons land. Uit het gegeven dat er in Nederland meer cocaine in beslag wordt genomen dan er wordt geconsumeerd, kunnen we concluderen dat ons land als (een van de) distributieland(en) voor Europa fungeert. Zowel het gebruik als de handel in Nederland als de transitfunctie van ons land brengt ernstige gevolgen met zich mee, zoals volksgezondheidsproblemen, corruptie, liquidaties in het openbaar en het witwassen of herinvesteren van grote hoeveelheden crimineel geld.

Ten slotte wordt gewezen op de productie en verspreiding van *kinderpornografie*. Dit is een delict dat door de toenemende digitalisering een steeds internationaler karakter krijgt. Vooral de grotere internetdekking in derdewereldlanden in Azië en Zuid-Amerika zorgt voor een sterke toename van het internetgebruik. Internet, met name de darkwebvariant, is een populair instrument om aan kinderpornografisch materiaal te komen en dit te distribueren. Georganiseerde commerciële distributie ervan vindt bijvoorbeeld plaats via een *pay-per-view*- of *pay-per-premiumservice*-constructie. Zo kunnen beelden van kindermisbruik tegen betaling *live* worden gedeeld.
Het Meldpunt Kinderporno op Internet signaleert een forse stijging van het aantal meldingen: van 20.000 in 2013 naar 70.000 in 2015. 75 procent van deze meldingen betrof strafbaar materiaal.
Hoewel de algemene indruk bestaat dat de productie van kinderpornografie niet of nauwelijks in Nederland plaatsvindt, werden in de periode 2012-2015 bijna 2000 verdachten aangehouden en 850 Nederlandse slachtoffers geïdentificeerd. De verwachting is dat wereldwijd de productie, distributie en consumptie van kinderporno, en daarmee ook de schadelijke gevolgen ervan, zullen toenemen.
De opsporing heeft in toenemende mate te maken met verdachten die in grootschalige internationale kinderpornonetwerken opereren. Verder valt op dat de verdachten in kinderpornozaken steeds jonger worden. Een mogelijke verklaring hiervoor is dat jongeren seksueel getinte foto's en video's van zichzelf en elkaar maken. Zij zijn steeds vaker online en posten daarbij soms ook dit seksueel getinte, wettelijk gezien kinderpornografische, materiaal. Dit kan leiden tot sextortion, dat wil zeggen het afdwingen van seksuele handelingen of afbeeldingen van slachtoffers door te dreigen met de verspreiding van eerder verkregen beeldmateriaal. Europol signaleerde in 2015 een sterk groeiende trend op het gebied van sextortion van jongeren.

2.3 Slotconclusie

Op abstract strategisch niveau hebben zich de afgelopen jaren op het gebied van de georganiseerde criminaliteit betrekkelijk weinig substantiële veranderingen voorgedaan en dat lijkt ook voor de komende vier jaar te zullen gelden. Zodra we daarentegen op tactisch-operationeel niveau naar de materie kijken, zien we dat de georganiseerde criminaliteit in de uitvoering van de activiteiten een dynamisch geheel vormt dat voortdurend in beweging is. Zo worden er nieuwe smokkelroutes gebruikt en steeds omvangrijker partijen drugs gesmokkeld, neemt op sommige terreinen de professionaliteit van samenwerkingsverbanden toe en ontplooien veel samenwerkingsverbanden op meer dan één gebied criminele activiteiten. Over het algemeen zien we echter dezelfde vormen van criminaliteit terug en zijn telkens dezelfde 'klassieke' soorten georganiseerde criminaliteit de grootste dreiging voor de Nederlandse samenleving. Illegale drugs, financieel-economische criminaliteit, uitbuiting en vermogenscriminaliteit veroorzaken miljarden euro's schade en maken veel slachtoffers. De ondermijnende en ontwrichtende effecten van sommige vormen van georganiseerde criminaliteit zijn moeilijk te overschatten, vooral wanneer de criminaliteit zich innestelt in de woonwijken en daar zichtbaar wordt.

We zien een toenemende invloed van digitale technologie op het criminele landschap. Dit geldt voor vrijwel alle vormen van georganiseerde criminaliteit; vrijwel ieder crimineel samenwerkingsverband maakt gebruik van digitale hulpmiddelen. Niet alleen worden legale toepassingen doelwit van cybercriminelen, er wordt ook software ontwikkeld en te koop aangeboden waarvan het doel is er illegale activiteiten mee te ontplooien, zoals ransomware, exploit kits en malware. Individuen zonder veel digitale knowhow kunnen met behulp van deze kant-en-klare softwarepakketten met weinig moeite en zonder geografische beperkingen op grote schaal criminele acties ondernemen. De drempel om cybercrime te plegen wordt lager en daardoor betreedt een nieuw soort dader de criminele markt. Het gaat om individuen die communiceren via internet en crimineel actief zijn zonder de deur uit te hoeven. Door deze ontwikkeling dekken de vertrouwde begrippen 'georganiseerde criminaliteit' en 'criminele samenwerking', die immers samenwerking tussen meerdere personen veronderstellen, de lading in steeds mindere mate. Het is onvermijdelijk dat dit – meer nog dan nu al het geval is – consequenties zal hebben voor de manier waarop handhaving en opsporing gestalte krijgen.

Bijlagen

1 Begeleidingscommissie

Ten behoeve van het NDB2017 is, evenals bij voorgaande gelegenheden, een begeleidingscommissie samengesteld. De bevoegdheden en taken van de commissie werden als volgt vastgelegd:

Bevoegdheden

De bevoegdheden van de begeleidingscommissie bestaan uit het bewaken van de voortgang en het gevraagd en ongevraagd adviseren over de inhoud en de werkwijze van het project. Indien onverhoopt sprake mocht zijn van onoverbrugbare verschillen van inzicht tussen de begeleidingscommissie en de projectleiding, worden deze voorgelegd aan de opdrachtgever.
De commissie vergadert in ieder geval aan het eind van elke fase en zo veel vaker als er volgens de voorzitter aanleiding toe bestaat.

Taken

De begeleidingscommissie heeft tot taak het beoordelen van en adviseren over:
- het projectplan (inclusief inhoud en werkwijze);
- de lijst met onderwerpen (inclusief voorstellen voor aanvullingen en verwijderingen);
- de deelprojectplannen;
- de voortgang;
- de gehanteerde methodiek bij het vaststellen van de kwalificaties;
- de inhoud, structuur en leesbaarheid van het eindrapport.

Binnen elk deelproject is een rapportage samengesteld met onderzoeksbevindingen. Deze rapportages vormen de bouwstenen voor dit eindrapport. Elk deelproject is afgesloten met een korte schriftelijke evaluatie door een klankbordcommissie. De deelrapportages en de schriftelijke evaluaties zijn voorgelegd aan de begeleidingscommissie.

Leden

De heer P.J. Aalbersberg	Politiechef Eenheid Amsterdam, tevens voorzitter.
De heer G.W. van der Burg	Procureur-generaal. Namens de opdrachtgever het College van procureurs-generaal. Gemandateerde: de heer P.P.H.M. Klerks, raadadviseur.
De heer T.G. van der Plas	Hoofd Operatiën, plaatsvervangend politiechef Landelijke Eenheid. Namens de opdrachtnemer de politie.
De heer H.R. Bril	Sectorhoofd DLIO. Namens de uitvoerder de DLIO.
De heer F.K.G. Westerbeke	Hoofdofficier van justitie van het Landelijk Parket, plaatsvervangend voorzitter.
De heer V.S.Th. Leenders	Plaatsvervangend hoofdofficier van justitie van het Functioneel Parket.
De heer A. IJzerman	Directeur Rechtshandhaving en Criminaliteitsbestrijding, Ministerie van Veiligheid en Justitie. Gemandateerde: de heer J. Dobbelaar, sr. beleidsadviseur.
De heer W.J.A. Paulissen	Sectorhoofd DLR.
De heer J. van der Vlist	Directeur FIOD, voorzitter Platform BOD's.
De heer K.C. Schuurman	Hoofd Landelijk Informatie en Expertise Centrum. Vervangen door de heer H. Schilders, plaatsvervangend hoofd LIEC.
De heer C.G. Hermans	Programmadirecteur Taskforce Brabant-Zeeland.
De heer E.R. Kleemans	Hoogleraar Zware criminaliteit en rechtshandhaving, Vrije Universiteit Amsterdam.
Mevrouw N. Kop	Lector Criminaliteitsbeheersing en recherchekunde, Politieacademie.

Vaste genodigde

Mevrouw C.G.L. Kuijper	DLIO, Landelijke Eenheid.

Projectleiding

De heer F.A. Boerman	DLIO, Landelijke Eenheid.
De heer M. Grapendaal	DLIO, Landelijke Eenheid.
De heer F.J. Nieuwenhuis	DLIO, Landelijke Eenheid.

2 Samenstelling consensusgroep

Voorzitter:

Dr. J.B. Lammers	Wetenschappelijk onderzoeker, DLOS, Landelijke Eenheid.

Leden:

Dr. F.A. Boerman	Senior onderzoeker, DLIO, Landelijke Eenheid.
Drs. M. Gieling	Docent en onderzoeker, Politieacademie.
Drs. M. Grapendaal	Senior onderzoeker, DLIO, Landelijke Eenheid.
Drs. F.J. Nieuwenhuis	Onderzoeker, DLIO, Landelijke Eenheid.
Drs. H. Sollie	Onderzoeker en adviseur, Organisatieadviesbureau Twynstra Gudde.

3 Gevolgeninstrument

Bij het bepalen van de ernst van de maatschappelijke gevolgen van georganiseerde criminaliteit hanteren we de soorten gevolgen en categorieën van slachtoffers die hieronder in een overzicht zijn gezet.

Slachtoffer / soort gevolg	A. Gezondheid		B. Milieu	C. Overlast	D. Financieel	E. Ondermijning					
	A1. fysiek	A2. psychisch				E1. Rechtspleging en rechtsorde	E2. Politiek/openbaar bestuur	E3. Economie	E4. Infrastructuur	E5. Verweving	E6. Normbesef
1 Individu			nvt			nvt	nvt	nvt	nvt	nvt	nvt
2 Bedrijfsleven	nvt	nvt	nvt			nvt	nvt	nvt	nvt	nvt	nvt
3 Overheid	nvt	nvt	nvt	nvt		nvt	nvt	nvt	nvt	nvt	nvt
4 Systeem	nvt	nvt	nvt	nvt	nvt						
5 Leefomgeving	nvt	nvt		nvt	nvt	nvt	nvt	nvt	nvt	nvt	nvt

De onderzoeker verschaft inzicht in de huidige en toekomstige schade van het betreffende criminele verschijnsel aan de hand van **de vragen** die hieronder zijn vermeld **bij de gevolgcategorieën A t/m E**.
In het geval van **onderzoeksvraag 2** gaat het om de schade in de huidige situatie. Neem daarbij als uitgangspunt het meest recente jaar waarvoor gegevens beschikbaar zijn.

In het geval van **onderzoeksvraag 4** gaat het om een inschatting van de ernst van de gevolgen in 2021.
De vaststellingen voor de schade in de huidige situatie (vraag 2) kunnen fungeren als vertrekpunt, basis, anker voor de inschattingen van de toekomstige schade. De antwoorden op vraag 3 zijn bepalend voor de toekomstige schade: liggen er geen relevante ontwikkelingen in het verschiet dan ligt de toekomstige schade in de lijn van de huidige schade, dienen zich wel belangrijke veranderingen aan dan zal de toekomstige schade gaan afwijken van de huidige schade.

A. Gezondheid

aantasting van fysieke of psychische gezondheid

A1. Fysiek letsel

a. *Hoeveel doden en gewonden zijn jaarlijks het gevolg?*

1. geen 2. enkele 3. tientallen 4. honderden 9. onbekend

b. *Licht je antwoord toe: geef een onderbouwing van de impact*.
(onderbouwing op basis van de indicatoren: doden, gewonden, soort fysiek letsel)

A2. Psychische schade

a. *Bij hoeveel slachtoffers leidt het tot traumatische ervaringen?*

1. niemand 2. enkele 3. tientallen 4. honderden 9. onbekend

b. *Licht je antwoord toe: geef een onderbouwing van de impact*.

B. Milieu

aantasting of bedreiging van milieu of leefomgeving

a. *In hoeverre is er sprake van bedreiging of aantasting van de leefomgeving?*

1. helemaal niet 2. gering 3. matig 4. hoog 9. onbekend

b. *Licht je antwoord toe:* g*eef een onderbouwing van de impact en probeer daarbij zoveel mogelijk te kwantificeren en concrete gevallen te vermelden*.
(maak, indien mogelijk, onderscheid tussen aantasting op het terrein van de (1) ruimtelijke ordening, (2) lucht, water en bodem (3) planten en dieren)

C. Overlast

gedrag dat leidt tot hinder, angst of onbehagen bij anderen

a. *Hoeveel personen en/of bedrijven ondervinden hinder?*

1. niemand 2. enkele 3. tientallen 4. honderden 9. onbekend

b. *Licht je antwoord toe: geef een onderbouwing van de impact*.

D. Financieel

vermogensschade door verlies van geld of goed

a. *Wat is de verwachte jaarlijkse financiële schade uitgedrukt in euro's?*

1. 0-10 miljoen	(enkele miljoenen)
2. 10-100 miljoen	(tientallen miljoenen)
3. 100-1000 miljoen	(honderden miljoenen)
4. 1 miljard of meer	(miljarden)
9. onbekend	

b. *Licht je antwoord toe: geef een onderbouwing van de impact*.
(tot de financiële schade rekenen we niet alleen de directe kosten, maar ook de eventuele kosten die gepaard gaan met verwervingscriminaliteit en de kosten van verslavingszorg)

E. Ondermijning

1. (on)bedoelde beïnvloeding van rechtspleging en rechtsorde
2. (on)bedoelde beïnvloeding van politiek en openbaar bestuur
3. (on)bedoelde beïnvloeding van economie
4. (on)bedoelde beïnvloeding van andere vitale sectoren
5. verweving van onder- en bovenwereld (overige)
6. (on)bedoelde beïnvloeding van het normbesef van burgers

E1. Rechtspleging en rechtsorde [52]

(on)bedoelde beïnvloeding van de rechtspleging d.w.z. beïnvloeding van personen die betrokken zijn in het opsporings- en vervolgingsproces, en aantasting van de staat van de rechtsorde (als resultaat van hoe de rechtspleging functioneert)

a. *In hoeverre staat de rechtspleging onder druk en wordt daarmee de rechtsorde bedreigd/ ondermijnd?*

1. helemaal niet 2. gering 3. matig 4. hoog 9. onbekend

b. *Licht je antwoord toe: geef een onderbouwing van de impact*.
(Komt dat bijvoorbeeld door de gevallen van corruptie, intimidatie, bedreiging en geweld? Of heeft het gebruik van offensieve contrastrategieën wellicht dergelijke gevolgen? Is er sprake van het schaden van de reputatie van politie en justitie? ed.)

52 Rechtspleging: wijze van procederen (de rechtspraak) (Van Dale). Rechtsorde: het geheel van door het recht beheerste regels in een gemeenschap, de gezamenlijke instellingen op juridisch gebied van een bepaald land (Van Dale)

E2. Politiek en openbaar bestuur
(on)bedoelde beïnvloeding van de besluitvorming in de politiek en van het openbaar bestuur

a. *In hoeverre wordt de politieke of bestuurlijke besluitvorming beïnvloed?*
1. helemaal niet 2. gering 3. matig 4. hoog 9. onbekend

b. *Licht je antwoord toe: geef een onderbouwing van de impact*.
(onderbouw zoveel als mogelijk met empirie, bijvoorbeeld op basis van concrete gevallen van corruptie, intimidatie en geweld, connecties)

E3. Economie
(on)bedoelde verstoring van sociaaleconomische verhoudingen

a. *In hoeverre worden sociaaleconomische verhoudingen verstoord?*
1. helemaal niet 2. gering 3. matig 4. hoog 9. onbekend

b. *Licht je antwoord toe: geef een onderbouwing van de impact*.
(onderbouw waar mogelijk met concrete gevallen, bijvoorbeeld van oneerlijke concurrentie, prijsmanipulatie/ kartelvorming, verlies van vertrouwen in monetair stelsel)

E4. Infrastructuur
(on)bedoelde aantasting of bedreiging van vitale infrastructurele voorzieningen[53]
(Energie, Telecommunicatie & ICT, Drinkwater, Voedsel, Gezondheid, Financieel, Keren en beheren oppervlaktewater, Transport en Chemische & nucleaire industrie)

a. *In hoeverre worden infrastructurele voorzieningen aangetast?*
1. helemaal niet 2. gering 3. matig 4. hoog 9. onbekend

b. *Licht je antwoord toe: waaruit bestaat de aantasting en wat is daarvan de impact voor de Nederlandse samenleving?*

53 Door de overheid zijn 12 vitale sectoren vastgesteld: Energie, Telecommunicatie & ICT, Drinkwater, Voedsel, Gezondheid, Financieel, Keren en beheren oppervlaktewater, Openbare orde & veiligheid, Rechtsorde, Openbaar bestuur, Transport en Chemische & nucleaire industrie, zie ook de Nationale Coördinator Terrorismebestrijding en Veiligheid (www.nctv.nl/onderwerpen/nv/voorkomen-voorbereiden/bescherming-vitale-infrastructuur Drie van de 12 vitale sectoren die door de overheid zijn vastgesteld, zijn hiervoor al aan de orde gesteld en blijven hier (bij E4) verder buiten beschouwing: Openbare orde & veiligheid, Rechtsorde (E1), Openbaar bestuur (E2).

E5. Verweving van onder- en bovenwereld (overige)

Verweving van onder- en bovenwereld wordt hier gekarakteriseerd als een toestand, een min of meer *bestendige situatie*, waarin de georganiseerde misdaad zich een *machtspositie* heeft verworven binnen legale partijen: branches, sectoren of bij de overheid. Van verweving is sprake bij 1) corrumptieve contacten met overheidspersoneel, vrijberoepsbeoefenaars en personen werkzaam in het bedrijfsleven, en 2) zeggenschap van criminelen over het eigendom van onroerend goed of zeggenschap over ondernemingen (in de vorm van aandelen of als eigenaar, bestuurslid en dergelijke). Hier gaat het om vormen van verweving die nog niet aan de orde zijn gesteld onder E1 t/m E4. Te denken valt bijvoorbeeld aan het gebruik van dekmantelfirma's, het gebruik van ondernemingen voor witwassen of het faciliteren van csv's door advocaten en notarissen.

a. *In hoeverre is sprake van verweving?*

1. helemaal niet 2. gering 3. matig 4. hoog 9. onbekend

b. *Licht je antwoord toe:* w*aaruit bestaat de verweving en geef een onderbouwing van de impact.*

E6. Normbesef burgers

Criminelen kunnen door hun gedrag een negatieve invloed hebben op het normbesef van burgers. Bijvoorbeeld door nadrukkelijk als 'onaantastbaren' aanwezigheid te zijn, door ongelimiteerd opschepgedrag, patsergedrag te vertonen of door openlijk drugs te dealen of goederen te helen.

a. *Zijn er locaties (buurten, straten ed.) aan te wijzen waar de criminele activiteiten en gedragingen zich concentreren en dusdanig zichtbaar zijn dat het aanleiding kan geven tot normvervaging?*

1. ja 2. nee 9. onbekend

b. *Licht je antwoord toe: welke activiteiten/gedragingen vinden er plaats en op welke locatie?*

www.politie.nl

Elke vier jaar maakt de politie in opdracht van het College van procureurs-generaal een nationaal dreigingsbeeld georganiseerde criminaliteit. Het Nationaal dreigingsbeeld 2017 (NDB2017) is een analyse waarin de huidige en verwachte toekomstige situatie van de georganiseerde criminaliteit in Nederland wordt beschreven. Het doel van dit dreigingsbeeld is een onderbouwing te leveren voor de prioritering in de aanpak van de georganiseerde criminaliteit en het signaleren van nieuwe ontwikkelingen op dit terrein.

Het NDB2017 is het vierde dreigingsbeeld dat verschijnt: het eerste verscheen in 2004, de volgende dreigingsbeelden zagen het licht in 2008 en 2012. Aan het NDB2017 werkten velen mee, onder wie ruim vijftig onderzoekers: onderzoekers van de politie (zowel Landelijke Eenheid als regionale eenheden), de FIOD, de Inspectie van Sociale Zaken en Werkgelegenheid, onderzoeksbureau Bruinsma, de Politieacademie en de Koninklijke Marechaussee.

De analyse van de georganiseerde criminaliteit beslaat uiteenlopende criminele verschijnselen op de terreinen van de illegale markten, fraude en witwassen en de georganiseerde vermogenscriminaliteit. Daarnaast is bijzondere aandacht besteed aan milieucriminaliteit en cybercrime.

« waakzaam en dienstbaar »

17001