Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Veiligheid en Justitie

Memorandum 2016-1

Cybercrime in cijfers

Een verkenning van de mogelijkheden om cybercrime op te nemen in de Nationale Veiligheidsindices

R.H. De Cuyper
G. Weijters

Memorandum
De reeks Memorandum omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht.
Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Veiligheid en Justitie weergeeft.

Inhoud

1 Inleiding

In de afgelopen jaren heeft het WODC de Nationale Veiligheidsindices (NVI) ontwikkeld om de ontwikkeling in criminaliteit, overlast en onveiligheidsgevoelens in Nederland en op regionaal niveau in kaart te brengen. Om trends in criminaliteit weer te geven is gekeken naar gedragingen die strafbaar zijn, overtredingen worden buiten beschouwing gelaten. In de NVI is criminaliteit opgesplitst naar elf delicttypen, te weten: moord en doodslag, geweldsdelicten, zedendelicten, vermogensdelicten (met geweld), diefstal (zonder geweld), inbraak (zonder geweld), vernielingen en misdrijven tegen de openbare orde, verkeersmisdrijven, fraude en bedrog, drugsmisdrijven en wapenmisdrijven. Om de ontwikkeling van criminaliteit in het algemeen te onderzoeken is daarnaast één criminaliteitsmaat ontwikkeld – de samengestelde criminaliteitsindex – die zes van de elf delicttypen omvat[1]. De trends van de losse delicttypen en de samengestelde criminaliteitsindex laten het algemene beeld zien dat de criminaliteit in de afgelopen jaren is gedaald in Nederland (De Cuyper, Weijters en Jennissen, 2015; zie ook Kalidien & de Heer-de Lange, 2015).
Hoewel een groot aantal delicten wordt meegenomen in de criminaliteitsindex,[2] wordt in de NVI niet apart gekeken naar cybercrime. Cybercrime heeft in de afgelopen jaren steeds meer aandacht gekregen in het maatschappelijke en wetenschappelijke debat. Ook op de Veiligheidsagenda 2015-2018 van het ministerie van Veiligheid en Justitie neemt de bestrijding van cybercrime een prominente postie in. De toenemende digitalisering van de samenleving maakt dat criminelen op nieuwe manieren slachtoffers kunnen maken. Daarnaast zijn computer- en informatiesystemen ook vaker het doelwit van criminaliteit. Het beeld heerst dat traditionele delicten minder vaak worden gepleegd, maar dat cybercrime juist toeneemt in de afgelopen jaren. Met andere woorden: er zou een verschuiving gaande zijn van offline criminaliteit naar online criminaliteit.
In deze haalbaarheidsstudie verkennen wij de mogelijkheden voor het opnemen van cybercrime in de NVI. Daarbij kijken wij naar de definitie van cybercrime, naar de vormen van cybercrime die er bestaan en naar de data die beschikbaar zijn over deze vorm van criminaliteit. Dit onderzoek tracht de volgende vragen te beantwoorden:

1 Hoe kan cybercrime het beste gedefinieerd worden?
2 Kan cybercrime als los delicttype worden meegenomen in de NVI of moet er onderscheid worden gemaakt tussen verschillende vormen van cybercrime?
3 Welke databronnen zijn beschikbaar en bruikbaar om de ontwikkeling in cybercrime in Nederland weer te geven?

In het volgende hoofdstuk gaan wij eerst in op de definitie van het begrip cybercrime. Vervolgens zullen wij in hoofdstuk 3 beschrijven of en welke mogelijkheden er zijn om cybercrime mee te nemen in de NVI. Hoofdstuk 4 is het concluderende hoofdstuk.

---

[1] Dit zijn de delicttypen: geweld, zeden, vermogen, inbraken, diefstal, en vernielingen en misdrijven tegen de openbare orde.

[2] De elf onderscheiden delicttypen in de NVI omvatten 97% van de door de politie geregistreerde criminaliteit (de samengestelde criminaliteitsindex omvat ongeveer 80% van de door de politie geregistreerde criminaliteit).

2 Definities

2.1 Wat is cybercrime?

Voordat gekeken kan worden naar de mogelijkheden om cybercrime op te nemen in de NVI, is het belangrijk om enig inzicht te krijgen in de definities van het begrip cybercrime. Uit de literatuur blijkt namelijk dat er uiteenlopende definities zijn en dat er geen consensus bestaat over de delicten die onder cybercrime vallen. Tevens wordt het begrip 'cybercrime' vaak vervangen door termen als 'computercriminaliteit', 'high tech crime' of 'computer-related cime'.
De definities van cybercrime kennen een grote variatie. Zo wordt cybercrime bijvoorbeeld beschreven als 'misdrijven die worden gepleegd met een computer' (Engelfriet, 2012), of als 'misdaad met behulp van of gericht tegen computernetwerken' (Koops, 2012), of als 'elk delict waarbij informatie en communicatietechnologie van wezenlijk belang is voor de uitvoering ervan' (Stol, Leukfeldt & Klap, 2012). Het valt op dat bij sommige definities wordt uitgegaan van delicten die worden gepleegd met behulp van of zijn gericht op computersystemen. Andere definities includeren een breder scala aan technologieën, zoals mobiele telefoons, navigatiesystemen of chipkaarten als middel en/of doelwit van criminaliteit.
Ook internationaal gezien is er geen eenduidigheid over de definitie van het begrip cybercrime. Zo omschrijft de Europese Commissie cybercrime als 'criminal acts that are committed online by using electronic communications networks and information systems' (European Commission, 2015). Daarbij benadrukt de Europese Commissie het sterk grensoverschrijdende karakter van cybercrime. Voorts laten de Verenigde Naties (VN) in een grootschalig onderzoek naar cybercrime een definitie van cybercrime achterwege (UNODC, 2013). Zij stellen dat het ontbreken van consensus over de definitie over het begrip niet erg is zolang het woord 'cybercrime' maar niet als een juridische term wordt gebruikt. De VN pleiten voor een duidelijke omschrijving van de handelingen die beschouwd kunnen worden als cybercrime en geven daar ook zelf invulling aan (UNODC, 2013).
Hoewel definities over het begrip cybercrime verschillen, wordt er in de literatuur vaak onderscheid gemaakt tussen cybercrime in brede zin en cybercrime in enge zin (Domenie, Leukfeldt, Van Wilsem, Jansen & Stol, 2013; Zebel, De Vries, Giebels, Kuttschreuter & Stol, 2013; Van der Hulst & Neve, 2008). Beide vormen onderscheiden zich van elkaar door de rol die ICT speelt bij de criminele handeling. Zo omvat cybercrime in enge zin delicten waarbij ICT zowel het instrument als het doelwit is van de criminaliteit. Te denken valt aan iemand die inbreekt op een computer en vervolgens (vertrouwelijke) informatie kopieert of verwijdert. Een ander voorbeeld is het platleggen van een website door het versturen van grote hoeveelheden aanvragen (zogenaamde 'DDoS-aanvallen'). Cybercrime in enge zin wordt ook aangeduid als 'cybercriminaliteit' (Politie, 2015; Ministerie van Veiligheid en Justitie, 2015). Deze term wordt ook in dit onderzoek gebruikt om cybercrime in enge zin te duiden.
Cybercrime in brede zin omvat delicten waarbij de ICT onderdeel uitmaakt van de *modus operandi*, maar zelf niet het doelwit is. Veelal richten deze criminele handelingen zich op personen of het verkrijgen van geld (UNODC, 2013). Er valt te denken aan iemand die een product verkoopt op internet en vervolgens het product niet levert aan de koper ('e-fraude'). Of het stelen van naaktfoto's van een computer waarna er om losgeld wordt gevraagd om verspreiding van de foto's te voorkomen (afpersing). Bij cybercrime in brede zin gaat het vaak om alleszins traditionele delicten die met behulp van ICT worden gepleegd. Deze oudere vormen van criminaliteit gepleegd met nieuwe middelen worden ook wel aangeduid als gedigitaliseerde crimi-

naliteit (Politie, 2015; Ministerie van Veiligheid en Justitie, 2015). Ook in dit onderzoek gebruiken wij deze term voor cybercrime in brede zin.
In dit onderzoek is er voor gekozen om voor de betekenis van cybercrime de definitie van het Team High Tech Crime (THTC) van de politie aan te houden. Het THTC omschrijft cybercrime als 'elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is' (Bernaards, Monsma & Zin, 2012). Deze definitie wordt ondersteund en gebruikt door het Nationaal Cyber Security Centrum (NCSC) en door het Openbaar Ministerie (OM). Uit deze definitie kan worden opgemaakt dat het zowel gaat om delicten die met behulp van ICT gepleegd worden en om misdrijven waarbij ICT het doelwit is. Verder strekt geautomatiseerd werk verder dan computers, maar omvat het ook informatiesystemen en telecommunicatiemiddelen.

2.2 Cybercrime en het Wetboek van Strafrecht

Niet alleen in de literatuur worden definities gegeven van cybercrime. Ook in het Wetboek van Strafrecht zijn wetsartikelen opgenomen die cybercrime definiëren en strafbaar stellen.
In het Wetboek van Strafrecht (Sr)zijn verschillende artikelen opgenomen die refereren aan cybercrime. Het gaat daarbij in het bijzonder om wetsartikelen die gericht zijn op strafbaarstelling van cybercriminaliteit. In artikel 138ab wordt bijvoorbeeld het opzettelijk en wederrechtelijk toegang verschaffen tot een geautomatiseerd werk of een deel daarvan strafbaar gesteld. Dit refereert aan computervredebreuk. Andere vormen van cybercrime die in de wet middels een specifiek artikel strafbaar zijn gesteld zijn: het veroorzaken van stoornis in het systeem (art. 161sexies en 161septies Sr), vernieling van gegevens (art. 350a en 350b Sr), het aftappen en/ of opnemen van gegevens (art. 139c Sr) en het plaatsen van aftapapparatuur (art. 139d Sr) (Leukfeldt, Domenie en Stol, 2010; p.11). Voor een uitgebreide bespreking van de wetsartikelen over cybercriminaliteit verwijzen wij naar Koops (2012). Het gaat hier dus om wetsartikelen die criminaliteit strafbaar stelt waarbij ICT als middel wordt gebruikt, maar ook ICT als doelwit heeft.
Gedigitaliseerde criminaliteit is niet zondermeer te herleiden uit de bestaande wetsartikelen. Voor gedigitaliseerde criminaliteit geldt dat delicten doorgaans worden vastgesteld onder wetsartikelen die refereren aan traditionele delicten. Zo wordt een aangifte of melding over bijvoorbeeld een niet-geleverde aankoop bij een online veilingsite in de meeste gevallen vastgelegd onder wetten die gaan over algemene fraude en bedrog. Een duidelijke koppeling met een wetsartikel refererend aan cybercrime is daarbij niet altijd het geval. Er zijn een aantal wetsartikelen waarin geautomatiseerd werk als het middel tot het plegen van een delict wordt omschreven. Zo is afpersing door het dreigen met het onbruikbaar maken van digitale gegevens strafbaar gesteld onder artikel 317, lid 2 Sr. Wat betreft gedigitaliseerde criminaliteit gaat het echter om slechts een klein aantal misdrijven met een eigen bepaling in het Wetboek van Strafrecht. Het zou makkelijk zijn als bij het opmaken van een proces-verbaal systematisch wordt bijgehouden of geautomatiseerd werk (bijv. Internet) een middel is geweest om het delict te plegen. Zodoende kan herleid worden of er sprake is geweest van cybercrime in brede zin. Helaas wordt de rol van geautomatiseerd werk niet per definitie vermeld door de politie en zodoende is de rol van ICT bij het plegen van traditionele delicten lastig te bepalen.
In tabel 1 (overgenomen uit Zebel et al., 2013, p.42) staan de wetsartikelen weergegeven die te maken hebben met cybercriminaliteit en met gedigitaliseerde criminaliteit.

Tabel 1 Wetsartikelen die te maken hebben met cybercrime

Wetsartikel	Beschrijving
Cybercriminaliteit	
Art. 138ab, lid 1 Sr	Hacken: opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk
Art. 138ab, lid 2 Sr	Hacken: overnemen, aftappen of opnemen van gegevens uit een geautomatiseerd werk na binnendringen daarvan
Art. 138ab, lid 3 Sr	Hacken door tussenkomst van een openbaar telecommunicatienetwerk
Art. 138b Sr	Het belemmeren van toegang tot of gebruik van een geautomatiseerd werk
Art. 139c Sr	Het aftappen of opnemen van gegevens (afluisteren)
Art. 139d, lid 1 Sr	Plaatsen van opname-, aftap- of afluisterapparatuur; voorbereidingshandelingen
Art. 139d, lid 2 Sr	Het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen of toegangscodes bedoeld om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen
Art. 139d, lid 3 Sr	Zoals in art. 139d, lid 2 Sr, maar met oogmerk gericht op art. 138ab, lid 2 en 3 Sr
Art. 139e Sr	Het bezit en verspreiden van gegevens of een voorwerp waarop gegevens staan die door wederrechtelijk aftappen of opnemen zijn verkregen
Art. 161sexies Sr	Opzettelijk vernielen etc. van een geautomatiseerd werk of werk voor telecommunicatie; voorbereidingshandelingen
Art. 161septies Sr	Vernieling etc. van een geautomatiseerd werk of werk voor telecommunicatie door schuld
Art. 350a, lid 1 Sr	Opzettelijke vernieling van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen
Art. 350a, lid 2 Sr	Het feit gepleegd in lid 1 met tussenkomst van een openbaar telecommunicatienetwerk
Art. 350a, lid 3 Sr	Opzettelijk gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk
Art. 350b, lid 1 Sr	Vernieling door schuld van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen
Art. 350b, lid 2 Sr	Door schuld gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk
Gedigitaliseerde criminaliteit	
Art. 232 Sr	Opzettelijk valselijk opmaken, vervalsen, gebruiken, etc. van betaalpas, waardekaart e.d.
Art. 240b Sr	Kinderpornografie
Art. 248e Sr	Grooming
Art. 273, lid 2 Sr	Bekendmaking bedrijfsgeheimen; heling computergegevens ondernemingen
Art. 273d Sr	Schending telecommunicatiegeheim
Art. 317, lid 2 Sr	Afpersing door de bedreiging dat gegevens opgeslagen door een geautomatiseerd werk onbruikbaar, ontoegankelijk of gewist worden
Art. 326c Sr	het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen

Noot. Tabel overgenomen uit *Jeugdige daders van cybercrime in Nederland: Een empirische verkenning* (Zebel, De Vries, Giebels, Kuttschreuter & Stol, 2013 p. 42).

3 Cybercrime in de NVI

De opsplitsing tussen gedigitaliseerde criminaliteit en cybercriminaliteit, en de bestaande wetten over cybercrime, zijn ook relevant voor het beantwoorden van de vraag of en op welke wijze cybercrime opgenomen kan worden in de NVI. Om dit te begrijpen is enige informatie nodig over de criminaliteitsindex van de NVI.
De criminaliteitsindex is momenteel opgedeeld in elf delicttypen. De trends van de onderscheiden delicttypen zijn gebaseerd op verschillende databronnen. De delicttypen zeden, vermogen (met geweld), inbraak (zonder geweld), diefstal (zonder geweld), vernielingen en delicten tegen de openbare orde, wapenmisdrijven, drugsmisdrijven, het verkeersmisdrijf 'doorrijden na een ongeval', en fraude en bedrog zijn gebaseerd op cijfers die door de politie worden geregistreerd. Data van de veiligheidsmonitor worden gebruikt om inzicht te krijgen in de ontwikkeling van geweldsmisdrijven. Verder is het aantal moorden en doodslagen gebaseerd op de doodsoorzakenstatistiek en is het verkeersdelict 'rijden onder invloed' gebaseerd op het Water, Verkeer en Leefomgeving (WVL) onderzoek van Rijkswaterstaat.
Binnen de delicttypen van de NVI worden de wetsartikelen die te maken hebben met cybercriminaliteit al meegenomen. De misdrijven die strafbaar zijn gesteld onder wetsartikel 138ab Sr (computervredebreuk) vallen bijvoorbeeld in de categorie misdrijven tegen de openbare orde en de misdrijven die strafbaar zijn gesteld onder wetsartikelen 350a en 350b Sr (vernieling van digitale gegevens) vallen onder de categorie vernieling en beschadiging. Ook gedigitaliseerde criminaliteit wordt al indirect meegenomen in de criminaliteitsindex. Aan gedigitaliseerde misdrijven worden immers vaak wetsartikelen toegekend die gerelateerd zijn aan alleszins traditionele delicten. Deze wetsartikelen omvatten het merendeel van de misdrijven in de NVI en vallen binnen de verschillende delicttypen.
Om inzicht te krijgen in de ontwikkelingen in cybercriminaliteit en gedigitaliseerde criminaliteit moeten beide vormen van cybercrime dus losgekoppeld worden van de onderscheiden delicttypen in de NVI. Daarnaast zal onderzocht moeten worden of andere databronnen nodig zijn om een betrouwbaar beeld te geven van de ontwikkeling in cybercrime. Eerst zullen wij de mogelijkheden bespreken om gedigitaliseerde criminaliteit los te koppelen van de onderscheiden delicttypen. Daarna zullen wij ingaan op cybercriminaliteit en de mogelijkheden om deze delictvorm op te nemen in de NVI.

3.1 Gedigitaliseerde criminaliteit

De mogelijkheid om gedigitaliseerde criminaliteit in kaart te brengen voor de NVI hangt af van de databronnen die zijn gebruikt voor de onderscheiden delicttypen. Deze databronnen moeten het mogelijk maken om een onderscheid te maken tussen een online gepleegd delict en een offline gepleegd delict.
Bij delicttypen die zijn gebaseerd op andere data dan politiedata is een opsplitsing naar misdrijven met een digitale component niet mogelijk. Behalve de politiecijfers bevatten de databronnen die worden gebruikt in de NVI namelijk geen informatie over de manier waarop misdrijven zijn gepleegd, waardoor het onderscheid tussen online of offline gepleegd niet gemaakt kan worden. Dat delicttypen niet verder kunnen worden opgesplitst hoeft echter geen probleem te zijn. Zo lijkt de kans dat ICT een rol speelt bij moorden en doodslagen en bij het verkeersmisdrijf 'rijden onder invloed' vooralsnog zeer klein. Voor geweldsmisdrijven ligt dit anders; bij deze misdrijven kan ICT wel een rol spelen. In de NVI valt bedreiging onder geweldsmisdrijven. Bedreiging is in de NVI gemeten met de vraag uit de Veiligheidsmonitor of iemand slachtoffer is geweest van dit misdrijf in het afgelopen jaar. Hoewel deze

vraag inzicht biedt in het aantal bedreigingen dat in Nederland voorkomt, wordt niet doorgevraagd naar de rol die ICT heeft gespeeld bij het plegen van het delict.[3] Hierdoor is een verdere opsplitsing van bedreiging met een digitale component niet mogelijk.

Er zijn twee delicttypen in de NVI die zijn gebaseerd op politiedata en waarbij wij een verdere opsplitsing naar gedigitaliseerde criminaliteit niet relevant achten. Zo veronderstellen wij dat de kans klein is dat ICT een rol speelt bij het delicttype 'inbraken (zonder geweld)' (zie ook Montoya, Junger & Hartel, 2013). Onder dit delicttype vallen de misdrijven: inbraken uit een woning en inbraken uit een schuur/garage. De middelen die worden gebruikt om deze misdrijven te plegen zullen doorgaans niet ICT-gerelateerd zijn. Verder speelt ICT geen rol bij het delicttype 'doorrijden na een ongeval'.

Bij de andere delicttypen die zijn gebaseerd op politiecijfers is een verdere opsplitsing naar misdrijven met een digitale component denkbaar. Deze delicttypen omvatten meerdere misdrijven die gerelateerd kunnen zijn aan het gebruik van ICT. Wij bespreken ze hieronder kort:

a Zedenmisdrijven
  Binnen de categorie 'zedenmisdrijven' vallen verschillende delicten die met behulp van geautomatiseerd werk gepleegd kunnen worden. Te denken valt aan het verspreiden van kinderpornografie via internet of grooming. Van grooming is sprake als een volwassene via ICT contact legt met een kind met als doel om een zedendelict te plegen (Leukfeldt et al., 2010).
b Vermogensmisdrijven (met geweld)
  De delicten die in de NVI vallen onder vermogensmisdrijven met geweld zijn: diefstal met geweld, inbraak met geweld en afpersing en afdreiging. ICT kan een rol spelen in de laatste categorie delicten. Afpersing en afdreiging kan bijvoorbeeld voortvloeien uit geïnstalleerde ransomware. Bij ransomware wordt de toegang tot de computer geblokkeerd waarna slachtoffers worden aangezet om losgeld te betalen om toegang tot de computer terug te krijgen (Bernaards, Monsma & Zinn, 2012).
c Diefstal (zonder geweld)
  Diefstal zonder geweld omvat in de NVI verschillende delicten. De delicten die in de NVI onder dit delicttype vallen zijn: diefstal van een fiets, bromfiets/snorfiets, motor, scooter, personenauto, vervoermiddel (overig), vaartuig, personenauto, vervoermiddel (overig), vaartuig, dier, zakkenrollerij en winkeldiefstal. Het stelen van digitale goederen wordt ook vastgesteld onder wetten die te maken hebben met diefstal. In 2007 werden bijvoorbeeld twee tieners gearresteerd die verdacht werden van het stelen van virtuele meubelen uit het online spel Habbo Hotel.[4]
d Vernielingen en misdrijven tegen de openbare orde
  Onder misdrijven tegen de openbare orde valt onder andere het beledigen of discrimineren van groepen in de samenleving. Een voorbeeld daarvan is het zaaien van haat via internet. Volgens Van Stokkom en collega's (2007) heeft internet gezorgd voor een nieuw podium waar mensen hun haat kunnen uiten.
e Fraude en bedrog
  Een vorm van fraude en bedrog die via geautomatiseerd werk plaatsvindt is e-fraude. Onder e-fraude valt bijvoorbeeld het plegen van fraude op internetwinkels of het stelen van digitale persoonsgegevens om identiteitsfraude te plegen (Domenie et al., 2013). Uit onderzoek van Montoya en collega's (2013) blijkt dat ICT een rol speelt bij 41% van de fraudezaken die bij de politie bekend is.

---

[3] Sinds 2012 zijn wel vragen in de Veiligheidsmonitor (VM) opgenomen over slachtofferschap van identiteitsfraude, online koop- en verkoopfraude en hacken (Kloosterman, 2015). Vragen over online bedreiging worden niet gesteld in de VM.

[4] www.volkskrant.nl/leven/eerste-arrestatie-wegens-virtuele-diefstal-uit-habbo-hotel~a844538/

f Drugsmisdrijven
Ook bij drugsmisdrijven kan ICT een rol spelen. Te denken valt bijvoorbeeld aan het verkopen van drugs via internet of het smokkelen van drugs door een digitaal controlesysteem (in bijvoorbeeld een zeehaven) te manipuleren of plat te leggen.
g Wapenmisdrijven
Een verband tussen wapenmisdrijven en ICT kan bijvoorbeeld gevonden worden in het kopen en verkopen van (vuur)wapens via internet.

Om te onderzoeken of ICT een rol heeft gespeeld bij geregistreerde misdrijven, is het van belang om aangiften en meldingen bij de politie nader te analyseren. Bij het opnemen van een aangifte door de politie worden verschillende stappen doorlopen (Leukfeldt et al., 2012). Zo wordt er onder andere bepaald om welk delict het gaat en welke wetsartikelen van toepassing zijn. De wetsartikelen bij een aangifte kunnen informatie geven over de manier waarop het misdrijf is gepleegd. De misdrijven kunnen worden vastgelegd onder wetsartikelen die te maken hebben met cybercriminaliteit, onder wetsartikelen die verwijzen naar traditionele delictsvormen (waarbij ICT een rol kan spelen) en onder een combinatie van wetsartikelen die zowel naar cybercriminaliteit als naar traditionele delicten verwijzen. Op basis van deze wetsartikelen kan echter geen volledig uitsluitsel worden gegeven over gebruik van ICT bij het plegen van misdrijven. Het is bijvoorbeeld mogelijk dat gedigitaliseerde criminaliteit wordt vastgelegd onder wetsartikelen die enkel verwijzen naar traditionele delictsvormen waarbij niet expliciet het gebruik van ICT staat vermeld. Het kan daarom nuttig zijn om aan de hand van ICT-gerelateerde trefwoorden en zoektermen een analyse te maken van gedigitaliseerde criminaliteit in de politieregistratie.
Een methode waarmee dit gedaan zou kunnen worden is textmining. Textmining kan worden ingezet om de analyse van ongestructureerde databestanden te automatiseren. De methode is bijvoorbeeld eerder gebruikt door Choenni en collega's om de rol van ICT bij geregistreerde klachten te onderzoeken (Choenni, Leertouwer & Busker, 2011). Om te onderzoeken welke rol ICT speelt bij de klachten, analyseerden zij twee datasystemen van de overheid. Dit deden zij door vrije tekstvelden in beide systemen te analyseren met behulp van ICT-gerelateerde trefwoorden en zoektermen. Uit hun onderzoek bleek dat textmining goed bruikbaar is om de rol van ICT bij klachten te bepalen als er geen vaste invoervelden zijn waarin de rol van ICT wordt vastgelegd.
In hoeverre textmining kan leiden tot een betrouwbaar beeld van gedigitaliseerde criminaliteit is nog onduidelijk. Zo hebben de politiedata verschillende beperkingen als het gaat om het meten van cybercrime. In de eerste plaats doen slachtoffers niet altijd aangifte bij de politie. Hoewel dit een bekend probleem is bij het gebruik van politiedata, wordt er beargumenteerd dat dit probleem groter is bij cybercrime (Leukfeldt et al., 2010, p. xxiv). Mensen zouden vaak niet doorhebben dat zij slachtoffer zijn van cybermisdrijven. Ten tweede wordt van verschillende misdrijven wel aangifte gedaan, maar verwerkt de politie deze aangiften niet altijd in het registratiesysteem. Ten derde worden misdrijven waarvan aangifte wordt gedaan en die worden geregistreerd door de politie soms in een ander registratiesysteem bijgehouden dan in de basisprocessensystemen. Bij een analyse van de politiedata (bijvoorbeeld via BlueView[5]) worden deze misdrijven dan niet meegenomen (zie Leukfeldt et al., 2010, p. 13). Deze drie beperkingen maken dat politiecijfers volgens Leukfeldt en collega's een beperkt beeld geven van cybercrime.
Een andere nadeel bij het toepassen van textmining is dat geen gebruik meer gemaakt kan worden van de politiecijfers die door het CBS worden gepubliceerd. Deze politiecijfers zijn voor iedereen via Statline op te vragen en momenteel voor de cri-

[5] BlueView is een systeem van de politie waarmee landelijk alle aangiften en processen-verbaal kunnen worden doorzocht.

minaliteitsindex in de NVI gebruikt. In het Strategisch Beraad Veiligheid (SBV) is de wens uitgesproken om gegevens voor de NVI te gebruiken die als open data toegankelijk zijn. Het analyseren van politiedata aan de hand van ICT-gerelateerde trefwoorden en zoektermen vraagt gebruik te maken van databestanden die niet vrij toegankelijk zijn.
Kortom, een opsplitsing naar gedigitaliseerde criminaliteit kan haalbaar zijn voor delicttypen die zijn gebaseerd op politiecijfers, maar er kleven bezwaren aan een dergelijke opsplitsing. Een dergelijke opsplitsing betekent ook dat de criminaliteitstak van de NVI een totaal ander beeld gaat geven. In tabel 2 is een overzicht van onderscheiden delicttypen in de NVI weergegeven. Per delicttype is aangegeven of het van belang is om na te gaan of een opsplitsing naar misdrijven met een digitale component mogelijk is.

Tabel 2 De onderscheiden delicttypen in de NVI[a]

	Is een opsplitsing naar gedigitaliseerde criminaliteit mogelijk?
Delicttypen gebaseerd op politiecijfers	
Zedenmisdrijven	Ja
Vermogensmisdrijven (met geweld)	Ja
Diefstallen (zonder geweld)	Ja
Inbraken (zonder geweld)	Nee
Vernielingen en misdrijven tegen de openbare orde	Ja
Verkeersmisdrijven (doorrijden na een ongeval)	Nee
Fraude en bedrog	Ja
Drugsmisdrijven	Ja
Wapenmisdrijven	Ja
Delicttypen gebaseerd op andere bronnen	
Moord en doodslag	Nee
Verkeersmisdrijven (rijden onder invloed)	Nee
Geweldsmisdrijven	Nee

[a] In de tabel staan 12 in plaats van de 11 onderscheiden delicttypen weergegeven. Dit komt doordat verkeersmisdrijven zijn opgesplitst naar het misdrijf 'doorrijden na een ongeval' en het misdrijf 'rijden onder invloed'.

3.2 Cybercriminaliteit

Voor de NVI zijn er ook mogelijkheden om cybercriminaliteit apart mee te nemen. Omdat er verschillende wetsartikelen zijn die gaan over misdrijven waarbij ICT zowel het middel als het doelwit is, is cybercriminaliteit relatief makkelijk los te koppelen van de bestaande delicttypen. Er zijn vervolgens verschillende manieren om cybercriminaliteit op te nemen in de criminaliteitsindex. Wij bespreken er drie.
Een eerste mogelijkheid om cybercriminaliteit mee te nemen is door de betreffende wetsartikelen uit de onderscheiden delicttypen te halen en als aparte indices mee te nemen. Zebel en collega's groeperen bijvoorbeeld de wetsartikelen in vier categorieën, te weten: 'hacken' (art. 138ab, 138b Sr), 'aftappen en opnemen van digitale gegevens' (art. 139c, 139d, 139e Sr), 'vernieling van geautomatiseerde werken' (art. 161sexies, 161septies Sr) en 'vernielingen van digitale gegevens' (art. 350a, 350b Sr) (Zebel et al., 2013). Voor de NVI kan een soortgelijke opsplitsing worden gemaakt en vier aparte indices worden meegenomen die inzicht bieden in de ontwikkelingen in cybercriminaliteit.
Er kleven echter bezwaren aan het gebruik van politiecijfers om cybercriminaliteit te meten. Evenals voor gedigitaliseerde criminaliteit en criminaliteit in het algemeen, geldt ook voor cybercriminaliteit dat vaak geen aangifte bij de politie wordt gedaan. Redenen hiervoor zijn dat slachtoffers vaak niet door hebben dat ze slachtoffer van

cybercriminaliteit zijn (Bernaards et al., 2012) of dat ze minder bereid zijn aangifte te doen van deze delicten (Leukfeldt, Domenie, Jansen, Van Wilsem & Stol, 2013). Hierdoor is de cybercriminaliteit die bekend is bij de politie slechts het topje van de ijsberg. Dit blijkt ook uit eerdere analyses van justitiële registratiedata. Zo laat een analyse van Zebel en collega's zien dat er in de periode 2006-2011 slechts 2.611 afgedane strafzaken van cybercrime waren (Zebel et al., 2013). Hierbij betrof het in 9% van de gevallen hacken, 1,8% vernieling van digitale gegevens, 0,6% vernieling van geautomatiseerd werk en 0,4% het aftappen of opnemen van digitale gegevens (Zebel et al., 2013). Ook uit ongepubliceerde cijfers van het WODC blijkt dat cybercriminaliteit niet vaak voorkomt in de registratie van het OM (tabel opgenomen in bijlage 1).[6] Een eventuele onderrapportage in cybercriminaliteit bij de politie hoeft echter geen gevolgen te hebben voor de NVI. De NVI hebben namelijk als doel om trends in sociale veiligheid weer te geven; niet de totale omvang in criminaliteit.
Wat wel invloed heeft op de NVI is de toegenomen aandacht voor cybercriminaliteit. De laatste jaren besteedt de politie meer aandacht aan cybercriminaliteit, waardoor cybercriminaliteit vaker wordt geregistreerd. Meer geregistreerde misdrijven wil daarom niet per definitie zeggen dat er ook meer delicten worden gepleegd: een toename kan ook toe te schrijven zijn aan een verandering in aandacht voor het fenomeen.
Een tweede mogelijkheid om cybercriminaliteit mee te nemen is door de wetsartikelen uit de onderscheiden delicttypen te halen en vervolgens vormen van cybercriminaliteit te meten met verschillende databronnen. In de literatuur wordt cybercriminaliteit niet opgevat als één delicttype, maar vaak opgedeeld in verschillende verschijningsvormen. Voorbeelden van vormen die vaak worden genoemd zijn hacken, botnets, DDoS-aanvallen, malware en defacing.
Deze verschillende verschijningsvormen van cybercrime zijn echter sterk aan elkaar gerelateerd. Zo is bij het opzetten van een botnet ook automatisch sprake van hacken, aangezien er moet worden ingebroken op een computer om hierover controle te krijgen en de computer op te nemen in een botnet. Door deze verwevenheid van de verschijningsvormen bestaat het risico dat misdrijven dubbel worden meegeteld in de statistieken. Indien de verschijningsvormen worden opgenomen in de NVI kan het probleem van cybercriminaliteit dus groter lijken dan werkelijk het geval is.
Een derde mogelijkheid om cybercriminaliteit op te nemen in de NVI is door hacken los te koppelen van de huidige delicttypen en als aparte index mee te nemen. Hacken hangt sterk samen met de meeste andere verschijningsvormen van cybercriminaliteit. Zo is bij defacing en het installeren van malware (bijna) altijd sprake van hacken, en gaat hacken vooraf aan het opzetten van een botnet en een DDoS-aanval (zie Leukfeldt et al., 2012). Een nadeel van het opnemen van hacken als aparte index is dat hacken vaak niet op zichzelf staat. Dit geldt ook voor de andere verschijningsvormen van cybercriminaliteit. Veelal wordt hacken als middel gebruikt om andere vormen van criminaliteit te plegen. Zo zouden cybercriminelen tegenwoordig niet meer hacken voor de status en het aanzien, maar voornamelijk voor het financiële gewin. Dit wordt ook wel aangeduid als een verschuiving van 'hacken for fame' naar het 'hacken for fortune' (o.a. Van der Hulst & Neve, 2008; Leukfeldt et al., 2013). Een aparte index voor hacken is dan ook moeilijk los te zien van gedigitaliseerde criminaliteit. Ook bij het opnemen van hacken bestaat het risico dat misdrijven dubbel worden meegeteld in de statistieken. Dit kan een vertekening van het criminaliteitsprobleem opleveren.

[6] De auteurs willen Debora Moolenaar bedanken voor de cijfers over cybercriminaliteit zoals opgenomen in de appendix van dit haalbaarheidsonderzoek.

Beschikbare bronnen
Er zijn meerdere databronnen die inzicht kunnen geven in de omvang van de verschillende vormen van cybercriminaliteit. Deze databronnen zijn grofweg op te delen in vier groepen (zie ook UNODC, 2013). De eerste groep databronnen is reeds besproken en betreft registratiecijfers van politie en justitie. De andere databronnen omvatten cijfers van slachtofferenquêtes, cijfers van meldpunten en cijfers van aanbieders van cybersecurity producten. Slachtofferenquêtes hebben het voordeel dat de misdrijven die niet worden aangegeven bij de politie vaak wel in een enquête worden gemeld. De enquêtegegevens zijn echter afhankelijk van de gebruikte steekproef, het onderzoeksdesign en de vragen die worden gesteld (UNODC, 2013). Bij cijfers van meldpunten over cybercrime kan in Nederland gedacht worden aan gegevens van het Landelijk Meldpunt Internetoplichting (LMIO), Meldpunt Kinderporno, meldpunt Spamklacht en Meldpunt Discriminatie Internet (MDI). Hoewel meldpunten een belangrijke bijdrage kunnen leveren aan de inzichten over cybercriminaliteit, blijft het probleem van een 'dark number' ook bij deze databron een punt van zorg (UNODC, 2013). Ten slotte verschaffen aanbieders van cybersecurity producten (o.a. ontwikkelaars van antivirus software en firewalls) cijfers over verschijningsvormen van cybercriminaliteit. Voorbeelden van aanbieders zijn: AVG, Cisco, IBM, McAfee, Microsoft, PandaLabs, Sophos, Norton Symantec, Total Defense en Trend Micro (UNODC, 2013). Een beperking van deze data is dat het vaak onbekend is hoe en van wie de gegevens zijn verzameld. Voorts hebben de belangen van de verschillende aanbieders invloed op statistieken waardoor cijfers vertekenend kunnen zijn (Bernaards et al., 2012).
Er zijn dus meerdere databronnen die gebruikt kunnen worden om de omvang en ontwikkeling in cybercriminaliteit in kaart te brengen. Er bestaat echter nog geen eenduidigheid over de databronnen die de verschijningsvormen het beste kunnen meten. Het THTC van de landelijke politie pleit dan ook voor een samenwerking tussen verschillende instanties in Nederland (waaronder het NCSC, universiteiten, het CBS en het WODC) om een lijst op te maken van databronnen die een betrouwbaar beeld geven van de verschijningsvormen van cybercriminaliteit. Het opnemen van de verschillende vormen van cybercriminaliteit in de NVI is een optie als een dergelijke lijst is samengesteld.

Samenvattend zijn er dus meerdere mogelijkheden om cybercriminaliteit mee te nemen in de NVI, maar alle mogelijkheden kennen belangrijke beperkingen. Daarnaast is er landelijk nog veel onbekend over welke databronnen een betrouwbaar beeld kunnen geven van cybercriminaliteit.

4 Conclusie en discussie

In deze haalbaarheidsstudie is onderzocht in hoeverre cybercrime meegenomen kan worden in de Nationale Veiligheidsindices (NVI). Daarbij is cybercrime opgedeeld in gedigitaliseerde criminaliteit, refererend aan alleszins traditionele misdrijven waarbij ICT een belangrijk onderdeel is van de *modus operandi*, en cybercriminaliteit, refererend aan misdrijven waarbij ICT zowel het middel als het doelwit is. Eén van de doelen van de NVI is om ontwikkelingen op het gebied van criminaliteit zo betrouwbaar mogelijk te beschrijven om zodoende een beeld te geven van de ontwikkeling van 'de' criminaliteit. Om de NVI uit te breiden met ontwikkelingen in cybercrime, zijn we dan ook nagegaan op welke manier een beeld gegeven kan worden van 'de' cybercrime.

Uit deze eerste verkenning blijkt dat gedigitaliseerde criminaliteit niet op korte termijn kan worden meegenomen in de NVI. Momenteel wordt gedigitaliseerde criminaliteit al meegeteld in de bestaande delicttypen van de NVI. Eerst zal een manier ontwikkeld moeten worden om gedigitaliseerde criminaliteit los te koppelen van de bestaande delicttypen. Een mogelijke methode is door aangiften en meldingen bij de politie nader te analyseren met behulp van textmining (zie ook Domenie et al., 2009). Het is aan te raden om in een pilotstudie na te gaan of, en welke, ICT-gerelateerde zoektermen gebruikt kunnen worden om een betrouwbaar beeld te geven van gedigitaliseerde criminaliteit. Textmining heeft echter grote gevolgen voor de methode van de NVI. Nu worden politiedata gebruikt die voor iedereen zijn op te vragen via het CBS. Bij textmining dient data te worden gebruikt die niet vrij toegankelijk zijn. Daarnaast zal de criminaliteitsindex van de NVI een ander beeld geven dan tot op heden wanneer de online gepleegde delicten losgekoppeld worden van de offlinedelicten.

Ook is het afzonderlijk meenemen van cybercriminaliteit in de NVI op korte termijn niet opportuun. Omdat politiecijfers slechts een beperkt beeld geven van cybercriminaliteit, zijn deze cijfers nog niet geschikt om de ontwikkeling in cybercriminaliteit betrouwbaar te beschrijven. Een alternatief is om de ontwikkeling in cybercriminaliteit te beschrijven aan de hand van de ontwikkelingen in verschillende verschijningsvormen, zoals: hacken, botnets, DDoS-aanvallen, malware en defacing. Deze verschijningsvormen kunnen worden gemeten met (een combinatie van) data van politie en justitie, slachtofferenquêtes, meldpunten en aanbieders van cybersecurity software. Eerst zal echter een lijst moeten worden opgemaakt van databronnen die een betrouwbaar beeld geven van de verschijningsvormen. Hierover is namelijk nog veel onbekend. Daarbij is het aan te raden, samen te werken met andere instanties die hier een belang bij en behoefte aan hebben. Te denken valt aan het NCSC, het THTC van de politie en het CBS. Verder zal er rekening gehouden moeten worden met de grote mate van overlap tussen de verschillende verschijningsvormen, en tussen de verschijningsvormen en andere misdrijven. Deze overlap kan namelijk leiden tot dubbeltellingen van delicten en zodoende tot een vertekening van de criminaliteitsontwikkeling in de NVI.

Dit haalbaarheidsonderzoek laat dus zien dat er mogelijkheden zijn om cybercrime op termijn op te nemen in de NVI. De mogelijkheden hiertoe leiden wel tot grote verschuivingen in de gehanteerde methode en vereisen data die niet vrij toegankelijk zijn. Gezien de verschuiving van offline criminaliteit naar online criminaliteit is het wenselijk om op korte termijn meer inzicht te krijgen in de ontwikkeling van cybercrime, naast de ontwikkeling van de offline criminaliteit. Zoals we in deze studie hebben laten zien, is er nog veel onduidelijk hoe ontwikkelingen in *de* cybercrime het meest betrouwbaar in beeld gebracht kan worden. Binnen het WODC worden momenteel meerdere initiatieven genomen om hier inzicht in te geven. Zo wordt er momenteel gewerkt aan het opstellen van een onderzoeksprogramma om

meer inzicht te krijgen in cybercrime onder jeugdigen. Verder staat er een project gepland waarbij (ontwikkelingen in) de verschillende vormen van cybercrime aan de hand van beschikbare databronnen in kaart worden gebracht. Het streven hierbij is niet alleen gebruik te maken van traditionele databronnen, zoals politieregistraties en slachtofferenquêtes, maar ook van 'nieuwe' data afkomstig van bijvoorbeeld (internet)meldpunten en beveiligingsbedrijven. Aan de hand van de uitkomsten van deze projecten kan vervolgens gekeken worden op welke wijze de NVI uitgebreid kan worden met de ontwikkeling van 'de' cybercrime.

Summary

Cybercrime in numbers
Exploring the possibilities to include cybercrime in the National Security Indices

This study examines whether and how cybercrime can be included in the National Security Indices. Cybercrime is generally used as an overarching term to describe offences where ICTs play a prominent role. In line with previous studies, we make a distinction between offences where ICTs are used as a mean to commit crimes (referred to as 'digitized crime') and offences where ICTs are the target of the criminal activity (referred to as 'cybercrime').

In our explorative study, we show that it is currently impossible to distinguish digitized crime from other crimes in the National Security Indices. Although digitized offences are already included in the crime index, they are not recorded as a separate category. The crime index is predominantly based on police crime records. Through use of ICT-related terms, text mining methods might be useful to further analyze police crime records and to make a distinction between offences with a digital component and offences without a digital component. However, more research is needed on this issue. We suggest that a pilot study be undertaken to explore whether and which ICT-related terms allow a reliable measurement of digitized crime. A drawback of applying text mining is that it causes some major changes in the methods of the National Security Indices. By applying it we cannot rely on open access data anymore, but need to use police data that are not openly available to the public. Moreover, it may drastically change the crime trends of the security indices.

Furthermore, we show that the inclusion of cybercrime in the security indices is not feasible in the short term. Because police statistics give a limited view of cybercrime, these figures seem less suited to examine cybercrime. It is possible to examine changes in cybercrime by focusing on its forms, such as hacking, botnets, Denial-of-service attacks, malware and defacing. These forms can be measured by using (and combining) data from law enforcement officials, crime victimization surveys, victim reporting initiatives (e.g. a website or hotline), and developers of cyber security software (e.g. anti-virus software and firewalls). First, however, a list should be made of data sources that provide a reliable picture of the forms of cybercrime. Still much is unknown about this matter. It is recommended to cooperate with other Dutch organizations that have an interest in drawing up such a list. These organizations include the National Cyber Security Centre, Team High Tech Crime of the police, and Statistics Netherlands. Moreover, when examining different forms of cybercrime, one needs to take into account the level of overlap between the forms of cybercrime, and between these forms and traditional crimes. Neglecting this overlap would lead to double counting of offenses and therefore to an overestimation of the crime problem.

This study shows that there are opportunities to include digitized crime and cybercrime in the National Security Indices. These opportunities however lead to major changes in the methods used, and require data that are not openly accessible. Because there is a general shift from offline to online crime, we believe that trends in cybercrime should be analyzed alongside trends in more traditional crimes. Yet, as

shown in this study, there are still questions about the reliability of measuring cybercrime left unanswered.

Within the WODC, there are now taken several initiatives to provide insight into how to measure cybercrime. Currently, we are drawing up a research program to better understand cybercrime among young people. There is also a project planned to describe (developments in) the various forms of cybercrime on the basis of all available data sources. The aim in this project is not only to use traditional data sources such as police records and victim surveys, but also to use 'new' data from, for example, (Internet) reporting centers and security companies. On the basis of the results of these projects can be examined how the NVI can be expanded with the development of 'the' cybercrime.

Literatuur

Bernaards, F., Monsma, E., & Zin, P. (2012). *High tech crime: Criminaliteitsbeeld-analyse 2012*. Woerden: KLPD.

Choenni, S., Leertouwer, E. & Busker, T. (2008). Klachten over toepassingen van informatietechnologie: Analyse van een aantal overheidsbestanden. In D. Broeders, C. Cuijpers & C. Prins (red.), *WRR: De staat van informatie* (pp. 223-245). Amsterdam: Amsterdam University Press.

De Cuyper, R.H., Weijters, G., & Jennissen, R.P.W. (2015). *Resultaten van de Nationale Veiligheidsindices 2014*. Den Haag: WODC. Factsheet 2015-4.

Domenie, M.M.L., Leukfeldt, E.R., Toutenhoofd-Visser, M.H., & Stol, W.Ph. (2009). *Werkaanbod cybercrime bij de politie: Een verkennend onderzoek naar de omvang van het geregistreerde werkaanbod cybercime.* Leeuwarden: Lectoraat Cybersafety, Noordelijke Hogeschool Leeuwarden.

Domenie, M.M.L., Leukfeldt, E.R., Van Wilsem, J.A., Jansen, J., & Stol, W.Ph. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit.* Den Haag: Boom Lemma uitgevers.

Engelfriet, A. (2012). *De Wet Computercriminaliteit: Wat is computercriminaliteit?* Geraadpleegd in november 2015: www.iusmentis.com/beveiliging/hacken/computercriminaliteit/cybercrime/

European Commission (2015). *Cybercrime*. Geraadpleegd in november 2015: ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/

Hulst, R.C. van der, & Neve, R.J.M. (2008). *High-tech crime: Inventarisatie van literatuur over soorten criminaliteit en hun daders*. Den Haag: Boom Jusidusche uitgevers. Ondezoek en beleid 264.

Kalidien, S.N., & De Heer-de Lange, N.E. (2015). *Criminaliteit en Rechtshandhaving 2014: Ontwikkelingen en samenhangen.* Den Haag: Boom criminologie. Justitie in statistiek 5.

Kloosterman, R. (2015). *Slachtofferschap cybercrime en internetgebruik*. Den Haag: Centraal Bureau voor de Statistiek.

Koops, B.J. (2012). De dynamiek van cybercrimewetgeving in Europa en Nederland. *Justitiële Verkenningen*, *38*(1), 9-24.

Leukfeldt, E.R., Domenie, M.M.L., Jansen, J., Van Wilsem, J.A., & Stol, W.Ph. (2013). Slachtofferschap van delicten met een digitale component en de rol van de politie. *Tijschrift voor de Politie*, *75*(2), 30-34.

Leukfeldt, E.R., Domenie, M.M.L., & Stol, W.Ph. (2010). *Verkenning cybercrime in Nederland 2009*. Den Haag: Boom Juridische uitgevers.

Leukfeldt, E.R., Kentgens, A., Frans, B., Toutenhoofd, M., Stol, W.Ph., & Stamhuis, E. (2012). *Alledaags politiewerk in een gedigitaliseerde wereld: Handreiking voor delicten met een digitale component*. Den Haag: Boom Lemma uitgevers.

Ministerie van Veiligheid en Justitie (2015). *Veiligheidsagenda 2015-2018.* Den Haag: Ministerie van Veiligheid en Justitie.

Montoya, L., Junger, M., & Hartel, P. (2013). How 'digital' is traditional crime? In European Intelligence and Security Informatics Conference (EISIC), Uppsala, Zweden, augustus 2013. IEEE Computer Society.

Politie (2015). *Cybercrime*. Geraadpleegd in november 2015: www.politie.nl/themas/cybercrime.html

Stokkom, B.A.M. van, Sackers, H.J.B., & Wils, J.P. (2007). *Godslastering, discriminerende uitingen wegens godsdienst en haatuitingen: Een inventariserende studie.* Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 248.

Stol, W.Ph., Leukfeldt, E.R., & Klap, H. (2012). Cybercrime en politie; een schets van de Nederlandse situatie anno 2012. *Justitiële Verkenningen*, *38*(1), 25-39.
UNODC (2013). *Comprehensive Study on Cybercrime. Draft 2013*. New York: United Nations.
Zebel, S., De Vries, P., Giebels, E., Kuttschreuter, M., & Stol, W.Ph. (2013). *Jeugdige daders van cybercrime in Nederland: Een empirische verkenning*. Enschede: Universiteit Twente.

Bijlage 1 Instroom bij het OM van cybercriminaliteit

Tabel A Instroom bij het OM van cybercriminaliteit in absolute aantallen[a]

	2007	2008	2009	2010	2011	2012	2013
Totale instroom	73	117	105	81	87	103	81
Het binnendringen in een geautomatiseerd werk (art. 138ab Sr[b])	68	94	89	63	66	83	61
Toegang belemmeren tot een geautomatiseerd werk (art. 138b Sr)	0	0	1	0	1	1	0
Het aftappen en/of opnemen van gegevens (art. 139c Sr)	0	1	1	1	0	0	0
Het plaatsen van opname-, aftap- en/of afluisterapparatuur (art. 139d Sr)	0	4	2	1	4	3	2
Opzettelijk veroorzaken van stoornis in een geautomatiseerd werk of telecommunicatie (art. 161sexies Sr)	1	0	4	0	2	1	8
Stoornis in een geautomatiseerd werk of telecommunicatie door schuld (art. 161septies Sr)	0	0	0	0	1	0	0
Het opzettelijk onbruikbaar maken en veranderen van gegevens (art. 350a Sr)	4	18	8	16	13	15	10
Het onbruikbaar maken en veranderen van gegevens door schuld (art. 350b Sr)	0	0	0	0	0	0	0

[a] De aantallen betreffen feiten, geen zaken. De feiten kun in combinatie met elkaar voorkomen en in combinatie met andere, hier niet genoemde delicten.

[b] Tot 1 oktober 2010 was dit artikel 138a Sr.

Bron: OM-data; Bewerking WODC