Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

26 643 Informatie- en communicatietechnologie (ICT)

29 911 Bestrijding georganiseerde criminaliteit

Nr. 768 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 28 mei 2021

Met deze brief informeer ik u, mede namens de Minister voor Rechtsbescherming en de Staatssecretaris van Economische Zaken en Klimaat, over de voortgang van de integrale aanpak van cybercrime. Ik heb u hier eerder over geïnformeerd op 29 juni 2020.[1] De aanpak van cybercrime en de versterking van cybersecurity hangen met elkaar samen. Over de voortgang van de Nederlandse Cybersecurity Agenda (NCSA) wordt u heden apart geïnformeerd.

Het leven van burgers speelt zich inmiddels voor een groot deel online af, en dit deel is tijdens de coronacrisis verder gegroeid. We zijn in ons dagelijks leven steeds afhankelijker van de online wereld. Dit vergroot de mogelijkheden voor criminelen om slachtoffers te maken en de impact die online criminaliteit kan hebben. De afgelopen jaren is inzet gepleegd op vier sporen, te weten preventie, ondersteuning van slachtoffers, wetenschappelijk onderzoek en opsporing, vervolging en verstoring. In deze brief worden de ontwikkeling van cybercrime en enkele in het oog springende maatregelen uiteengezet. Een overzicht van maatregelen is opgenomen in de bijlage[2]. Ondanks de inspanningen blijft het tegengaan van cybercrime een forse uitdaging die een blijvende inspanning vraagt.

[1] Kamerstukken 26 643 en 33 552, nr. 696.
[2] Raadpleegbaar via www.tweedekamer.nl.

kst-26643-768
ISSN 0921 - 7371
's-Gravenhage 2021

Algemeen beeld – ontwikkeling cybercrime

Cybercrime[3] neemt in de politieregistraties al meerdere jaren gestaag toe. Tijdens de coronacrisis heeft deze toename zich voortgezet. Criminelen hebben ingespeeld op de situatie en de online criminele activiteiten zijn toegenomen. Zo steeg het aantal registraties van computervredebreuk van rond de 2.000 in de jaren 2014–2016 naar 4.865 in 2019 en 11.120 in 2020.[4] De werkelijke dreiging en omvang van cybercrime wijkt waarschijnlijk af van de politieregistraties, omdat de aangiftebereidheid nog steeds zeer laag is. In het kader van de Veiligheidsmonitor gaf in 2019 5,5% van de respondenten aan slachtoffer te zijn geworden van hacken.[5] Als meerdere vormen van online criminaliteit worden bezien, en naast cybercrime andere online delicten zoals aan- en verkoopfraude worden meegenomen, dan geeft 13% van de respondenten aan slachtoffer te zijn geworden.[6] Het verzamelen van aanvullende gegevens over slachtofferschap en schade is nodig om een meer compleet beeld te krijgen. Daarom wordt momenteel gewerkt aan een uitbreiding van de Veiligheidsmonitor en een aparte monitor voor vormen van online criminaliteit.

Cybercriminelen worden steeds geraffineerder in het gebruik van sociale en technische kwetsbaarheden. *Social engineering* en de inzet van *malware* zoals ransomware vormen onverminderd een aanzienlijke dreiging. Gezien de nog vaak onvoldoende beveiligingsmaatregelen en onoplettendheid bij eindgebruikers hoeft een aanval echter niet altijd geraffineerd te zijn om succes te hebben.[7] Het voortbestaan van *cybercrime-as-a-service* blijft er voor zorgen dat ook minder vaardige criminelen cyberaanvallen kunnen uitvoeren. Eén van de conclusies in het Cyber Security Beeld Nederland (CSBN) 2021 is dat cybercriminaliteit de nationale veiligheid kan raken indien dit leidt tot omvangrijke schade aan digitale processen. In een aantal gevallen genieten cybercriminelen bescherming van de staat van waaruit zij opereren of is er sprake van samenwerking.[8]

Gerichte ransomware-aanvallen op grote bedrijven en instellingen vormen een toenemende dreiging voor de economische en maatschappelijk veiligheid.[9] Ondanks het gebrek aan kwantitatieve gegevens is het beeld van de politie dat zowel het MKB als grote organisaties in toenemende mate doelwit zijn van ransomware. Recente cybercriminele incidenten zoals bij de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en de gemeente 't Hof van Twente tonen de grote impact die deze criminaliteitsvorm ook in Nederland kan hebben.[10] De politie heeft gesignaleerd dat een deel van het ontvangen losgeld direct wordt geïnvesteerd in nieuwe aanvallen. Ransomware wordt bovendien steeds vaker gecombineerd met het publiceren of doorverkopen van tijdens de aanval weggesluisde informatie. Door het gebruik van

---

[3] De term cybercrime betreft in deze brief criminaliteit waarbij ICT-systemen zowel doel als middel zijn (ook wel cybercrime in enge zin genoemd). Voorbeelden daarvan zijn ransomware en het inbreken in computersystemen («hacken»). Criminaliteit waarbij ICT-middelen enkel faciliterend zijn, zoals eenvoudige fraudevormen en online drugshandel, wordt aangeduid met de term gedigitaliseerde criminaliteit. De term online criminaliteit omvat beide. Overigens zijn er diverse criminele werkwijzen die elementen van cybercrime in enge zin en gedigitaliseerde criminaliteit combineren.

[4] www. data.politie.nl.

[5] www. opendata.cbs.nl.

[6] Veiligheidsmonitor 2019. Het genoemde percentage betreft vier onderzochte delicten, te weten hacken, identiteitsfraude, aan- en verkoopfraude en cyberpesten.

[7] Jaarverantwoording politie 2020; Europol Internet Organised Crime Threat Assessment (IOCTA) 2020.

[8] Cyber Security Beeld Nederland (CSBN) 2021.

[9] IOCTA 2020, ENISA Threat Landscape 2020.

[10] Kamerstukken 31 288 en 26 643, nr. 910.

cryptovaluta zorgen criminelen dat hun identiteit bij het ontvangen van losgeld afgeschermd blijft in het geval van cybercriminele afpersing zoals ransomware.[11] Ook DDoS-aanvallen worden gecombineerd met pogingen tot afpersing. In de Jaarverantwoording Politie en in het CSBN wordt uitgebreid op de dreiging van onder meer ransomware ingegaan.

Advies betalen losgeld

Het advies vanuit het Kabinet, het OM en de politie blijft om geen losgeld te betalen bij een ransomware-aanval. Het betalen van losgeld biedt geen garantie op ontsleuteling van gegevens en houdt het criminele verdienmodel in stand. Om ransomware te voorkomen is het onder meer belangrijk om de digitale weerbaarheid op orde te hebben. Het instellen van twee-factorauthenticatie kan hierbij al aanzienlijk helpen.

Preventie

Het verhogen van de cyberweerbaarheid van burgers, bedrijven en instellingen blijft een punt van aandacht. Mensen gedragen zich online minder veilig dan ze denken en schatten de kans dat ze schade ondervinden van online risico's laag in. Bij veel succesvolle cyberaanvallen zijn onvoldoende basismaatregelen voor digitale weerbaarheid getroffen. De afgelopen jaren zijn diverse activiteiten uitgevoerd om de bewustwording van risico's en de bekendheid met basismaatregelen te ondersteunen. Deze activiteiten zijn gericht op het algemene publiek en op de specifieke doelgroepen jongeren, senioren, laaggeletterden en het MKB. Voor het algemene publiek zijn twee landelijke campagnes uitgevoerd, te weten «Eerst checken, dan klikken» door het Ministerie van JenV in 2019 en «Doe je updates» door het Ministerie van EZK van november 2019 tot januari 2021.[12] In het kader van het convenant voor de preventie van cybercrime wordt met private partners samengewerkt aan onder meer het aanpakken van *social engineering* en *spoofing*, evenals aan de verbreding van het gebruik van twee-factorauthenticatie. Op de website www.veiliginternetten.nl kunnen burgers terecht voor voorlichting en vragen over veilig online gedrag. Ten behoeve van de verspreiding van informatie over actuele cybercrimefenomenen en preventieve tips is, mede naar aanleiding van de suggestie van het Kamerlid Van Dam (CDA) tijdens het Algemeen Overleg cybersecurity op 9 december 2020, in samenwerking met de politie en de Fraudehelpdesk een pilot gestart met een periodiek «cyberweerbericht». In dat bericht worden actuele dreigingen en preventieve maatregelen periodiek gepubliceerd, onder meer op www.veiliginternetten.nl.

Voor het voorkómen en tegengaan van daderschap van cybercrime onder jongeren ontwikkelde de politie in navolging van eerdere campagnes het lesprogramma «Framed». Jongeren krijgen via het spelen van een online spel inzicht in verschillende cybercrimedelicten en de gevolgen daarvan. De campagne heeft inmiddels de Digital Interactive Award ontvangen in de categorie Activation. Stichting Halt heeft begin 2021 een nieuwe lesmodule over (online) fraude en cybercrime voor jongeren gelanceerd, gericht op het voorkómen van slachtoffer- en daderschap. Deze activiteiten maken deel uit van de brede aanpak van jeugdcriminaliteit. Op 23 juni jl. heeft de Minister voor Rechtsbescherming u nader over de voortgang van deze aanpak geïnformeerd.[13]

---

[11] IOCTA 2020.
[12] Kamerstukken 26 643 en 33 552, nr. 696.
[13] Kamerstuk 28 741, nr. 81.

Cyber Offender Prevention Squad (COPS)

In 2020 is bij de politie een tijdelijk projectteam gestart dat zich richt op daderpreventie. Het projectteam COPS beoogt het afschrikken van (potentiële) daders, het stimuleren van positieve keuzes en het verzwakken en verstoren van daders die bewust kiezen voor cybercrime. In 2020 zijn een daderpreventiestrategie en een interventietoolkit ontwikkeld en getest. Ook is een samenwerking met de gaming-industrie gestart.

In april 2020 is de campagnemaand «Senioren en Veiligheid» georganiseerd om senioren meer weerbaar te maken. Hiervoor is onder meer voorlichtingsmateriaal over online fraude en cybercrime verspreid en zijn vrijwilligers van ouderenbonden voorgelicht om hierover de juiste informatie te geven aan senioren. Voor laaggeletterden heeft het Ministerie van BZK in samenwerking met JenV het programma «Klik en Tik: Veilig Online» gelanceerd op www.oefenen.nl.

De door de Ministeries van JenV en BZK samen het Digital Trust Center (DTC) geïnitieerde City Deal Lokale Weerbaarheid Cybercrime is in oktober 2020 ondertekend. Deze City Deal omvat momenteel 18 projecten van gemeenten, regionale samenwerkingsverbanden Veiligheid en Platforms Veilig Ondernemen, gericht op het versterken van de weerbaarheid van jongeren, laaggeletterden, senioren en het MKB. Een voorbeeld is het project van de gemeente Breda, waar een groot aantal digitale wijkambassadeurs zijn opgeleid. Het netwerk van ambassadeurs helpt bij de uitvoering van de preventieve aanpak op het gebied van digitale criminaliteit. De opleidingsmodule die voor de digitale ambassadeurs is ontwikkeld kan ook in andere gemeenten worden ingezet.

In het Actieprogramma Veilig Ondernemen 2019–2022 heeft het Nationaal Platform Criminaliteitsbeheersing cybersecurity in het MKB als prioriteit opgenomen. De pilots in de City Deal Lokale Weerbaarheid Cybercrime gericht op het MKB passen binnen de doelstelling van het Actieprogramma. In het kader van het Actieprogramma is een onderzoek naar cyber-ketenafhankelijkheden in waardeketens van bedrijven gepubliceerd. Vervolgonderzoek richt zich op concreet handelingsperspectief voor het MKB binnen de ketens. Daarnaast is een gedragsexperiment gestart om inzicht te krijgen in gedragsbeïnvloeding en gedragsinterventies.

Het DTC heeft de afgelopen twee jaar meerdere projecten gestart en producten ontwikkeld gericht op bedrijven. Zo kunnen ondernemers de weerbaarheid van hun onderneming testen met de Basisscan Cyberweerbaarheid, is er een *Digital Trust Community* waarin aangesloten bedrijven actuele en relevante informatie kunnen uitwisselen en is de Wegwijzer voor cybersecurity-initiatieven ontwikkeld. Deze wegwijzer helpt ondernemers snel hun weg te vinden in de vele cybersecurity-initiatieven die Nederland rijk is.

Opsporing, vervolging en verstoring

Het internet mag geen vrijplaats voor criminelen zijn. Adequate opsporing en vervolging zijn hiervoor noodzakelijk. Eerder heb ik uw Kamer geïnformeerd over de uitdagingen bij de rechtshandhaving in het digitale domein.[14] De schaalbaarheid van cybercrime creëert een grote hoeveelheid (potentiële) slachtoffers. Daarnaast is het internet inherent grenzeloos en biedt het veel technische mogelijkheden voor anonimisering. Om deze uitdagingen het hoofd te kunnen bieden is de afgelopen

[14] Kamerstuk 28 684, nr. 621.

jaren geïnvesteerd in de versterking van de opsporing in het digitale domein in het algemeen en de bestrijding van cybercrime in het bijzonder. Een deel van de middelen uit het Regeerakkoord en een deel van de eenmalige investering bij de Najaarsnota in 2018 zijn hieraan besteed, met name bij de politie, het OM en het NFI.

De politie werkt inmiddels met een landelijk dekkende aanpak, bestaande uit onder meer het *Team High Tech Crime* (THTC) en tien cybercrimeteams in de regionale eenheden. De onderzoeken zijn conform de Veiligheidsagenda verdeeld in reguliere onderzoeken uitgevoerd op regionaal niveau, fenomeenonderzoeken, die gericht zijn op de brede bestrijding van eenheidoverstijgende cybercriminele fenomenen en dadergroepen, en onderzoeken van het THTC, waar het gaat om onderzoeken met een *high tech*-component. De regionale cybercrimeteams zijn daarbij steeds complexere zaken gaan uitvoeren. Ze assisteren bovendien reguliere opsporingsteams bij de bestrijding van gedigitaliseerde criminaliteit die zowel door cybercriminelen als door niet-cybercriminelen wordt gepleegd, zoals helpdeskfraude, vriend-in-noodfraude en betaalverzoekfraude. De capaciteit bij het OM blijft nog achter bij die van de politie.

De resultaten in het kader van de Veiligheidsagenda tonen de afgelopen jaren een stijgende lijn. Het aantal uitgevoerde reguliere onderzoeken bij politie vertoont een forse stijging, van 299 in 2018 naar 468 onderzoeken in 2020. Ook het aantal fenomeenonderzoeken stijgt. Ondanks dat de ambitie van 41 in 2020 met 39 net niet is behaald, is dit wel een stevige toename ten opzichte van de 21 fenomeenonderzoeken in 2019. Eén fenomeenonderzoek omvat vaak vele, soms duizenden slachtoffers, en soms betreft het vele miljoenen aan financiële schade. De ambitie van 20 *high tech crime*-onderzoeken is met 12 opsporingsonderzoeken niet behaald en gedaald ten opzichte van voorgaande jaren. De oorzaak daarvan ligt vooral in de toenemende technische en juridische complexiteit van de fenomenen en de onderzoeken, wat een grotere inzet van capaciteit en hoogwaardige kennis vergt. Deze onderzoeken betreffen de meest hoogtechnologische of nieuwe criminele werkwijzen en opsporingsmethoden. Ze nemen vaak meerdere jaren in beslag en bestrijken veelal verschillende subdoelstellingen. Ook wordt er binnen de onderzoeken aan technische en juridische innovaties gewerkt, die vervolgens aan de hele opsporing ten goede komen.

De politie zet in op datagedreven bestrijding van cybercrime, waarbij sprake is van intensieve samenwerking: nationaal en internationaal, publiek en privaat. Vaak is er sprake van brede samenwerkingsverbanden waarbij het THTC en het Landelijk Parket van het OM samenwerken in (internationale) coalities van overheidsdiensten en private bedrijven. Het THTC was tot april 2021 voorzitter van de *Joint Cybercrime Action Taskforce* van Europol en de politie neemt deel aan het *EMPACT-platform*.[15] De Landelijk Officier van Justitie voor Cybercrime bij het Landelijk Parket is lid van het *European Judicial Cybercrime Network* (EJCN). Ook investeren de politie en het OM in samenwerking met private partijen. De projecten NoMoreDDoS, NoMoreRansom, NoMorePhishing en het afgeronde project ter bestrijding van de *Tech Support Scam* zijn voorbeelden hiervan. Het *NoMoreRansom*-portal had in juni 2020 sinds de lancering vier jaar eerder ervoor gezorgd dat zo'n $ 632 miljoen aan geëist losgeld niet in de zakken van criminelen terecht is gekomen. Voor de bestrijding van ransomware heeft de politie een speciale taskforce opgericht met als doel in internationaal verband en met publieke en private partijen ransomware te bestrijden. Daarnaast nemen de politie en

[15] *European Multidisciplinary Platform Against Criminal Threats*. Hierbinnen prioriteren politiediensten van EU-lidstaten en Europol cybercrimebestrijding op Europees niveau.

het Ministerie van EZK deel aan het in 2020 opgerichte Anti-Abuse Netwerk (AAN), een publiek-privaat samenwerkingsverband voor het tegengaan van het onwetend faciliteren van criminaliteit door hostingproviders. Een voorbeeld van een regionaal samenwerkingsverband is de Taskforce Digitale Veiligheid van de regio Amsterdam, waar het OM aan deelneemt, dat zich richt op het verhogen van de weerbaarheid tegen digitale indringers en criminelen. In 2020 zijn tien politiemensen geworven voor versterking van de publiek-private samenwerking van de regionale cybercrimeteams.

Internationale politieoperatie Ladybird

Begin 2021 haalde de omvangrijke internationale politieoperatie Ladybird het complexe netwerk van servers achter de agressieve malware Emotet uit de lucht. Emotet besmette de systemen van ruim 1 miljoen slachtoffers wereldwijd met malware, 600.000 mailadressen waren gecompromitteerd en de wereldwijde schade loopt waarschijnlijk in de honderden miljoenen euro's. De criminele werkwijze was sterk georganiseerd, adaptief en technisch zeer complex. De aanpak vergde een omvangrijke samenwerking van vele politiemensen en officieren van justitie in acht landen. Twee van de drie hoofdservers bleken in Nederland te staan. Uiteindelijk lukte het om toegang te verkrijgen tot de cybercriminele infrastructuur van Emotet en deze te doorzoeken. Daarbij hebben de politie en het OM mede gebruik gemaakt van de bevoegdheid tot binnendringen in een geautomatiseerd werk. Uiteindelijk is het netwerk overgenomen en is de Emotet-malware gedeactiveerd. In samenwerking met het NCSC zijn zoveel mogelijk slachtoffers genotificeerd.

Voor een effectieve opsporing in het digitale domein is zowel nationaal als internationaal regelgeving nodig die is toegesneden op het digitale domein. De Wet computercriminaliteit III is nu ruim twee jaar van kracht. De politie en het OM hebben voortvarend invulling gegeven aan de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk. Recent is de bevoegdheid ook in internationaal onderzoek ingezet. De Inspectie Justitie en Veiligheid houdt toezicht op de inzet van de bevoegdheid. Het jaarlijkse toezichtsrapport en de reactie daarop worden voor het zomerreces aan de Kamer gestuurd. Het WODC is inmiddels gestart met de evaluatie. Deze wordt naar verwachting begin 2022 gepubliceerd.

Om de grensoverschrijdende opsporing in het digitale domein te versterken heeft Nederland in de afgelopen jaren actief deelgenomen aan de gesprekken over de E-Evidenceverordening van de EU en over het tweede protocol bij het Cybercrimeverdrag in het kader van de Raad van Europa. De triloog over de E-evidence-verordening is inmiddels gestart. Het concept van het tweede protocol is eind mei goedgekeurd en openbaar gemaakt. Daarmee is een belangrijke mijlpaal bereikt in de gesprekken die in 2017 formeel zijn gestart. Na goedkeuring op politiek niveau en ratificatie zal het protocol snellere en meer efficiënte samenwerking in opsporingsonderzoeken mogelijk maken.

Ondanks de inspanningen en successen in de afgelopen jaren maken de toenemende hoeveelheid cybercrimedelicten en de complexiteit van de opsporing in het digitale domein het lastig voldoende capaciteit en expertise te realiseren. De politie en het OM signaleren bovendien dat zware criminaliteit in het fysieke domein, zoals drugshandel, in toenemende mate wordt ondersteund door gespecialiseerde, criminele digitale dienstverlening. De bestrijding van deze criminaliteitsvormen vraagt steeds vaker een aanpak in het digitale domein, waarbij een beroep wordt gedaan op de gespecialiseerde cybercrimecapaciteit van de politie en het

OM. Daarmee worden belangrijke successen geboekt, zoals bij de aanpak van Encrochat en bij de operatie *Trojan Shield*, waarbij het berichtenverkeer van vele criminelen kon worden ingezien. Om een sterkere handhavingsketen te realiseren adviseert de Cyber Security Raad € 330 miljoen extra te investeren in het vergroten van inzicht en de aanpak van cybercrime door het OM, de KMar en de politie.[16]

Aandacht voor het slachtoffer

De impact van online criminaliteit op slachtoffers kan groot zijn. Het is van belang slachtofferschap te erkennen en hen hierin te ondersteunen. Slachtofferhulp Nederland heeft in 2020 een grote groep mensen bereikt met de campagne «Van oplichting naar opluchting». Hierin deelden slachtoffers van online criminaliteit hun verhaal. Mede door deze campagne zijn meer mensen lid geworden van online lotgenotengroepen, waarbij slachtoffers over de gevolgen kunnen praten.

Het zorgen voor een adequate behandeling van slachtoffers en tegelijk het effectief houden van de vervolging en het strafproces vormt een forse uitdaging. Vanwege de grote schaalbaarheid van het internet kan een enkel cybercrimedelict immers duizenden slachtoffers maken. In 2020 is er € 1,8 miljoen geïnvesteerd om bij het OM 20 slachtoffercoördinatoren te werven voor het bijstaan van slachtoffers bij impactvolle zaken. Deze coördinatoren zijn niet speciaal voor online criminaliteit aangesteld, maar indien online criminaliteit veel impact heeft, kunnen de coördinatoren hiervoor worden ingezet. De opleidingen van de coördinatoren zijn op 1 januari 2021 gestart. In 2021 wordt het aantal slachtoffercoördinatoren uitgebreid met nog eens 21.

Wetenschappelijk onderzoek

De afgelopen jaren is in het kader van de integrale aanpak van cybercrime wetenschappelijk onderzoek uitgevoerd naar onder meer daders, slachtoffers en de aard en omvang van cybercrime in Nederland. De uitkomsten onderstreepten in het algemeen de gekozen aanpak en waren daarnaast nuttig voor enige verscherping van de maatregelen. Een adequate aanpak tegen cybercrime vraagt blijvende kennisopbouw. Daarom starten op korte termijn drie nieuwe WODC-onderzoeken en wordt naar verwachting voor de zomer het WODC-onderzoek naar de opsporing, vervolging en verstoring van cybercrime gepubliceerd.

Het is van belang naast kwalitatieve inzichten over voldoende kwantitatieve gegevens te beschikken. Daarom wordt de tweejaarlijkse Veiligheidsmonitor van het CBS uitgebreid ten aanzien van de opgenomen cybercrimedelicten en online criminele fenomenen. De eerste resultaten van de aangepaste Veiligheidsmonitor worden naar verwachting in 2022 gepubliceerd. Om structureel inzicht te krijgen in de trends van diverse vormen van online criminaliteit wordt momenteel gewerkt aan een aanvullende monitor. Deze Monitor Online Criminaliteit zal voortbouwen op de Veiligheidsmonitor en zal in de tussenliggende jaren worden gepubliceerd. De eerste inzichten uit deze monitor worden in 2023 verwacht.

Tot slot

Deze brief toont de voortgang van de integrale aanpak van cybercrime. De investeringen en de inzet van vele partijen hebben geleid tot meer kennis en capaciteit, vele initiatieven die burgers en bedrijven beschermen en

[16] Cyber Securty Raad, *Integrale aanpak cyberweerbaarheid*, 6 april 2021.

ondersteunen, en een versterking van de strafrechtelijke aanpak. Dat is een resultaat om trots op te zijn. Tegelijkertijd is het aantal cybercrimedelicten de afgelopen jaren sterk toegenomen en blijft opsporing in het digitale domein complex. Het probleem dat cybercrime voor de maatschappij vormt, zal naar verwachting blijven toenemen. Dit is een grote opgave, die de komende jaren structurele inspanningen vraagt.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus