34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

Nr. 33 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 mei 2026

Op 13 januari 2026 heeft mijn ambtsvoorganger uw Kamer de wetsevaluatie van de Wet computercriminaliteit III (Wet CCIII) aangeboden, die is uitgevoerd door het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) (Kamerstuk 34372, nr. 32). In deze brief reageer ik op de wetsevaluatie.

Op 1 maart 2019 is de Wet CIII in werking getreden. Met deze wet zijn zeven nieuwe dan wel aangepaste wettelijke bepalingen geïntroduceerd: vijf strafbaarstellingen en twee (bijzondere) opsporingsbevoegdheden. De bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk (de wettelijke hackbevoegheid, hierna voor de leesbaarheid “hackbevoegdheid” genoemd), een van de twee in deze wet opgenomen bevoegdheden, is al eerder geëvalueerd in 2023.[1] Hieronder wordt naast een algemene reactie ook per bepaling gereageerd op deze evaluatie.

Algemeen

In de evaluatie stond de vraag centraal in hoeverre de doelstellingen zoals geformuleerd in de Wet CCIII in de praktijk worden gerealiseerd. In zijn algemeenheid kan worden gesteld dat de geëvalueerde bepalingen en bevoegdheden hun waarde in de praktijk hebben bewezen en worden toegepast. Van belang is dat de nieuwe artikelen intussen onderwerp zijn geweest van rechterlijke toetsing, waardoor de reikwijdte en toepassing in de praktijk nader zijn verduidelijkt.

[1] Kamerstukken II 2023/24, 34372, nr. 31.

In de evaluatie zijn vier aspecten naar voren gekomen die meerdere wettelijke bepalingen uit de Wet CCIII raken: 1) nieuwe ontwikkelingen; 2) beschikbare capaciteit; 3) zaken met een internationale component; en 4) (rechtsstatelijke) waarborgen bij de inzet van bijzondere opsporingsbevoegdheden.

Ten eerste moeten nieuwe ontwikkelingen in het oog worden gehouden. Zo ondervindt de maatschappij bijvoorbeeld de gevolgen van een toename van de illegale handel in (persoons-)gegevens en het aantal slachtoffers daarvan. Het kabinet zal hier aandacht voor houden en dit ook meenemen bij de uitwerking van de verhoging van de strafmaxima voor ernstige cyberdelicten zoals aangekondigd in het coalitieakkoord.

Ten tweede is een breed gedeeld beeld dat capaciteitsoverwegingen mee spelen bij de inzet van bevoegdheden. Oplossingen hiervoor zijn niet eenvoudig, er zullen binnen opsporingsonderzoeken altijd keuzes gemaakt moeten worden welke (combinatie van) inzet van bevoegdheden passend is. Dit kan aanleiding zijn om nieuwe bevoegdheden of strafbaarstellingen niet in alle daartoe in aanmerking komende gevallen te gebruiken. Tegelijkertijd kan het capaciteit opleveren als de nieuwe bevoegdheden meer tijdrovende traditionele bevoegdheden vervangen.

Ook wordt in het rapport meermaals gerefereerd aan de complicaties die ontstaan als zaken een internationale component bevatten. In veel gevallen zijn rechtshulpverzoeken nodig die veel tijd in beslag nemen. Ik onderken deze complicaties en zet me ervoor in om daar waar het kan het effect op de opsporing te mitigeren. Zo wordt er actief ingezet op verbeterde samenwerking met en binnen Europol en kan ook de implementatie van de Europese E-evidence verordening de samenwerking bevorderen en versnellen.

Het WODC concludeert ten slotte dat er spanning bestaat tussen de inzet van bijzondere opsporingsbevoegdheden en grondrechten van burgers. Om die reden zijn de bevoegdheden met meerdere rechtsstatelijke waarborgen omkleed. Uit de evaluatie blijkt dat deze waarborgen soms het opsporingsbelang (onnodig) in de weg kunnen zitten. In dit kader zal de inzet van de bevoegdheid in

artikel 125p Sv vereenvoudigd worden. Dit wordt hieronder nader toegelicht.

Stelen van gegevens (artikel 138c Sr) en helen van gegevens (artikel 139g Sr)

Artikel 138c Sr regelt dat het strafbaar is om gegevens over te nemen. Een belangrijke veronderstelling van de wetgever was dat gegevens door artikel 138c Sr beter zouden worden beschermd tegen misbruik ervan. Voor de introductie was dat ingewikkelder omdat de destijds bestaande strafbaarstellingen niet altijd van toepassing waren op het wederrechtelijk overnemen van opgeslagen gegevens. Op basis van 139g Sr is het strafbaar geworden om gegevens te helen. Een belangrijke veronderstelling van de wetgever was dat door de komst van artikel 139g Sr burgers beschermd worden van wie gegevens, ontvreemd door een ander, bekend worden gemaakt, verkocht of op internet geplaatst.

Uit de evaluatie blijkt dat deze twee nieuwe strafbaarstellingen hun nut in de praktijk hebben bewezen. In verschillende gevallen konden verdachten vervolgd worden voor feiten waarbij dat voor de introductie van de wet minder goed mogelijk was. Ook konden door de nieuwe strafbaarstellingen extra opsporingshandelingen worden verricht, kunnen slachtoffers zich voegen in het strafgeding en kunnen gegevensdragers worden onttrokken aan het verkeer. Tegelijkertijd worden tot op heden beide artikelen nog beperkt zelfstandig toegepast en is de jurisprudentie nog in ontwikkeling.

De evaluatie concludeert dat de strafmaat afhankelijk van het soort gegevens dat wordt gestolen of geheeld aan de lage kant is. Het rapport wijst op technologische ontwikkelingen die een impact hebben op de hoeveelheid gegevens die gestolen kunnen worden en op het feit dat de illegale handel in gestolen gegevens toeneemt en de impact die dat kan hebben. Naast de hoeveelheid data die in een zaak wordt gestolen, weegt ook het soort data mee (bijvoorbeeld persoonsgegevens) en het aantal potentiële nieuwe slachtoffers dat met die data kan worden gemaakt.

Ik onderschrijf de conclusie dat de huidige strafmaxima op deze onderdelen niet in verhouding staan tot de ernst, schaal en maatschappelijke impact van deze delicten. In het coalitieakkoord is aangekondigd dat de strafmaxima voor zware cyberdelicten

zullen worden verhoogd. Bij de nadere beleidsuitwerking hiervan zal ook aandacht worden besteed aan recente incidenten zoals hacks bij Odido en Clinical Diagnostics.

Ook de richtlijn strafvordering voor cybercrime en gedigitaliseerde criminaliteit van het OM wordt momenteel herzien. Daarbij is het OM vanzelfsprekend gebonden aan de wettelijke strafmaxima. De verwachting is dat dit traject kort na de zomer wordt afgerond.

Daarnaast vraagt het WODC aandacht voor de “heler-steler-regel”. Uit een klein deel van de vonnissen en interviews volgt dat geen veroordeling voor het helen van gegevens plaats heeft gevonden wanneer de verdachte de geheelde gegevens zelf door een misdrijf had verkregen. Dit naar analogie van de wijze waarop met de heling van goederen wordt omgegaan (de ‘heler-steler-regel’). De heler-steler-regel bepaalt dat iemand die een goed steelt, niet óók vervolgd kan worden voor heling van datzelfde voorwerp. De vraag rijst of hetzelfde gezegd kan worden voor het stelen en helen van gegevens. Net als de onderzoekers acht ik de jurisprudentie ten aanzien van dit vraagstuk van belang.

Online handelsfraude (artikel 326e Sr)

Artikel 326e heeft online handelsfraude een eigen strafbepaling gegeven. Deze bepaling is beter afgestemd op digitale handelspraktijken waarbij er via webshops, platforms en sociale media fraude wordt gepleegd. Een belangrijke veronderstelling van de wetgever was dat met de komst van artikel 326e Sr online handelsfraude (eenvoudiger) strafrechtelijk vervolgd kon worden en dan vooral grootschalige vormen van handelsfraude. In de evaluatie worden enkele aandachtspunten benoemd. Allereerst: door een tekort aan opsporingscapaciteit worden veel zaken niet opgepakt of geseponeerd. Daarnaast wijst het WODC op het gegeven dat ‘grootschaligheid’, waarbij sprake is van een enkele dader of dadergroep die veel delicten pleegt, in de praktijk weinig is vastgesteld. In slechts een klein aantal van de door de politie onderzochte zaken is daarvan sprake. De redenen zijn niet bekend geworden. Tot slot wordt er gewezen op de buitenlandcomponent. Daders en infrastructuur bevinden zich vaak in het buitenland, geldstromen verlopen via buitenlandse rekeningen en de politie en het OM zijn afhankelijk van internationale samenwerking. Dat

laatste ziet met name op het achterhalen van de identiteit van een verdachte.

Ik onderschrijf de bevinding dat de nieuwe strafbaarstelling vervolging en bewijsvoering eenvoudiger heeft gemaakt. Dit is van belang omdat online handelsfraude een toenemend maatschappelijk probleem is. Dat wordt in het coalitieakkoord ook onderkend.[2]

Wat betreft de genoemde grootschaligheid speelt een rol dat veel individuele slachtoffers, die elk te maken krijgen met relatief lage schadebedragen, weinig aangifte doen. De werkelijke aard en omvang blijft zo buiten beeld. Onderzoek van het CBS geeft echter aan dat oplichting en fraude in 2025 met 10,3% de grootste categorie binnen (ervaren) online criminaliteit blijven. Vooral aankoopfraude springt eruit, met 7,9% van de bevolking van 15 jaar en ouder als slachtoffer.

Bij de aanpak van dit probleem hebben zowel private als publieke partijen een rol. Binnen de integrale aanpak online fraude dragen publieke en private partners bij aan de samenwerking met webshops en platforms om online aan- en verkoopfraude op een effectieve en efficiënte manier te bestrijden. Zo worden interventies met het bedrijfsleven ontwikkeld, die bijdragen aan het voorkomen van (herhaald) slachtofferschap.[3]

Het Landelijk Meldpunt Internet Oplichting (LMIO) van de politie ontvangt alle aangiften van online handelsfraude. Naast het verzorgen van de intake, analyse, veredeling van aangiftes en voorbereiding van opsporingsonderzoeken heeft het LMIO zich tot doel gesteld om preventieve maatregelen te treffen of te stimuleren. Hiertoe zoekt het LMIO samenwerking met private partijen.

Het kabinet onderkent dat de buitenlandcomponent een belangrijk aandachtspunt is. Als slachtoffers geld hebben overgemaakt naar

---

[2] Aan de slag: Bouwen aan een beter Nederland | Publicatie | Rijksoverheid.nl

[3] Kamerstukken II, 2025-2026, 29911, nr. 490.

een buitenlandse rekening of webshop is de identiteit van de dader lastig te achterhalen. In de Europese *richtlijn ter voorkoming van witwassen en terrorismefinanciering* is opgenomen dat alle nationale gecentraliseerde automatische mechanismen van de lidstaten voor het achterhalen van identificerende gegevens bij bepaalde financiële dienstverleners (in Nederland het Verwijzingsportaal Bankgegevens) onderling worden verbonden via het koppelingssysteem voor registers van bankrekeningen (bank account registers interconnection system — BARIS) dat door de Europese Commissie wordt opgezet en beheerd.[4] De Commissie zorgt, in samenwerking met de lidstaten, uiterlijk op 10 juli 2029 voor een dergelijke verbinding. Dit systeem moet er toe leiden dat binnen de EU identificerende gegevens van rekeninghouders snel kunnen worden achterhaald. Op grond van de *richtlijn ter vergemakkelijking van het gebruik van financiële en andere informatie voor het voorkomen, opsporen, onderzoeken of vervolgen van bepaalde strafbare feiten* moet BARIS ook toegankelijk zijn voor autoriteiten die bevoegd zijn voor het voorkomen, opsporen, onderzoeken of vervolgen van een ernstig strafbaar feit (dus niet alleen witwassen of terrorismefinanciering) of het ondersteunen van een strafrechtelijk onderzoek naar een ernstig strafbaar feit, inclusief de identificatie, opsporing en bevriezing van vermogensbestanddelen in verband met een dergelijk onderzoek.[5]

Lokpuber (artikelen 248a en 248e Sr)

De aanpassingen van artikel 248a Sr (verleiding van een minderjarige) en artikel 248e Sr (grooming) hebben ervoor gezorgd dat de politie de figuur van de ‘lokpuber’ kan inzetten. Beoogd werd hiermee de inzet van een opsporingsambtenaar die zich online voordoet als een minderjarige, al dan niet in de vorm van een virtuele creatie van een minderjarige, mogelijk te maken. Een belangrijke veronderstelling van de wetgever was dat minderjarigen beter konden worden beschermd door deze artikelen. Sinds de inwerkingtreding van de Wet seksuele misdrijven (Stb. 2024, 59) op 1 juli 2024 is de inzet van de figuur van de lokpuber mogelijk voor de opsporing en vervolging van de verschillende vormen van seksuele benadering van een kind die in artikel 251 Sr strafbaar zijn gesteld. Dit betreft ook de nieuwe delictsvorm sexchatting. De in dit onderzoek gesignaleerde aandachtspunten zijn eveneens van nut voor de toepassing van de

[4] EU Richtlijn 2024/1640 van 31 mei 2024
[5] EU Richtlijn 2019/1153, gewijzigd bij richtlijn 2024/1654

inzet van de lokpuber in het kader van de opsporing en vervolging van dit delict.

De zaken die onderzocht zijn in het evaluatieonderzoek bevestigen dat de inzet van de lokpuber een effectief middel kan zijn in de bestrijding van het seksueel benaderen van een kind. Er zijn verschillende voorbeelden van zaken waarin een lokpuber is ingezet en het tot een veroordeling is gekomen. Daarmee worden de met de wetswijziging beoogde doelen gerealiseerd. De inzet van de lokpuber kan bijdragen aan het bewijs van grooming of verleiding van minderjarigen en zo aan betere bescherming van minderjarigen.[6]

Lokmiddelen zijn echter wel zware opsporingsmiddelen. Vanuit proportionaliteit en subsidiariteit zet de politie ze terughoudend in. Er wordt doorgaans pas voor gekozen wanneer andere methoden onvoldoende resultaat opleveren.

Het rapport noemt als belangrijkste reden voor de beperkte inzet de beperkte capaciteit in combinatie met een toename van brengzaken, waarin vaak al voldoende bewijs voorhanden is en inzet van een lokpuber dus niet noodzakelijk is. Brengdelicten zijn delicten met een direct aanwijsbaar slachtoffer die door burgers of bedrijven aan de politie worden gemeld (naar de politie ‘gebracht’). Dit beperkt ook de proactieve inzet in haaldelicten. Haaldelicten zijn strafbare feiten zonder een direct aanwijsbaar slachtoffer die ambtshalve door de politie worden geconstateerd. Als aandachtspunt wordt in het rapport verder de grens met uitlokking genoemd. Nadere jurisprudentie kan de grenzen van dit instrument verder verduidelijken, zodat de lokpuber helderder en eenduidiger kan worden toegepast.

Preventie en vroege opsporing zijn belangrijk voor een effectieve aanpak van seksueel kindermisbruik. De veroordelingen in zaken waarin de lokpuber is ingezet onderstrepen dat dit instrument gebruikt kan worden om verdachte activiteiten vroegtijdig te signaleren en bewijs te verzamelen. Dat de lokpuber beperkt wordt ingezet doet niet af aan zijn toegevoegde waarde, zolang de politie goed bekend is met dit middel en het daadwerkelijk kan inzetten

[6] Kamerstukken II 2015/16, 34372, nr. 3, p. 69.

als dat nodig wordt geacht (p. 116). In dit verband staat in het rapport dat de inzet van digitale rechercheurs de bekendheid met dit instrument bevordert. Deze rechercheurs kijken mee met zaken en kunnen de inzet van een lokpuber aandragen als een mogelijkheid binnen het opsporingsonderzoek. Het kabinet acht deze werkwijze een goede stap voorwaarts.

Ontoegankelijk maken van gegevens (artikel 125p Sv)

Het met de Wet CCIII ingevoegde nieuwe artikel 125p Sv ziet op het ontoegankelijk maken van gegevens. Een belangrijke veronderstelling van de wetgever was dat door de introductie van artikel 125p Sv, een bevoegdheid om via een aanbieder gegevens ontoegankelijk te maken, strafbare feiten sneller beëindigd zouden kunnen worden of zelfs voorkomen. Op die manier zou de samenleving beter worden beschermd. De evaluatie laat zien dat artikel 125p Sv inderdaad wordt toegepast maar niet in veel gevallen. Zo voldoet het artikel niet altijd voor de opsporingspraktijk; het proces van afgifte van een machtiging van de rechter-commissaris en het horen van de aanbieder vooraf nemen veel tijd in beslag. Dit knelt indien er sprake is van spoed. Tegelijkertijd is de toets door de rechter-commissaris van belang omdat de inzet van deze bevoegdheid een effect kan hebben op de vrijheid van meningsuiting. Het alternatief is echter dat overgegaan wordt op andere bevoegdheden die minder procedurele eisen hebben, maar wel ingrijpender kunnen zijn.

Deze spanning tussen het belang van de opsporingspraktijk en het beschermen van grondrechten maakt het zoeken naar de juiste balans noodzakelijk. Ik verwelkom de conclusie van de evaluatie dat aanbieders vaak bereid zijn om op vrijwillige basis gegevens ontoegankelijk te maken. De introductie van artikel 125p Sv was ook nadrukkelijk bedoeld als sluitstuk van het systeem van zelfregulering door de sector.[7]

In veel verzoeken voor ontoegankelijkmaking gaat het om onmiskenbaar illegale content, bijvoorbeeld van online beeldmateriaal van seksueel kindermisbruik, waar geen discussie bestaat over de strafbaarheid ervan. Dit kan bij uitingsdelicten echter wel het geval zijn en dan is de toetsingsprocedure van

[7] Kamerstukken II 2015/–2016, 34372, nr. 3, p.61

belang. Om aan de problematiek van de opsporingspraktijk tegemoet te komen heeft het kabinet besloten om deze bevoegdheid in het nieuwe wetboek aan te passen en de hoorplicht door de rechter-commissaris facultatief te maken zodat maatwerk kan worden geleverd naar aanleiding van de aard van het materiaal waarvoor een verwijderbevel wordt gevraagd. De voorgestelde wijziging in artikel 2.7.57 van het nieuwe wetboek zal worden meegenomen door middel van de tweede aanvullingswet. Naar verwachting wordt dit wetsvoorstel in de komende maand in formele consultatie gegeven.

De wettelijke hackbevoegdheid (artikelen 126nba, 126uba en 126zpa Sv)

De wetgever heeft de hackbevoegdheid (artt. 126nba (binnendringen op afstand in een geautomatiseerd werk), 126uba (binnendringen in een geautomatiseerd werk ten behoeve van bestrijding georganiseerde criminaliteit) en 126 zpa Sv (binnendringen in een geautomatiseerd werk ten behoeve van bestrijding terroristische misdrijven) geïntroduceerd om computercriminaliteit en andere vormen van ernstige criminaliteit beter aan te kunnen pakken. In 2022 verscheen een eerdere WODC-evaluatie over deze bevoegdheid. De nadruk lag toen op de technische kant van de inzet. In de voorliggende evaluatie is vooral gekeken naar de tactische kant van de inzet van de hackbevoegdheid, namelijk op welke wijze de verzamelde gegevens binnen een opsporingsonderzoek worden gebruikt.

De evaluatie laat wederom zien dat de hackbevoegdheid een waardevolle bevoegdheid is voor de politie.[8] In 60% van de gevallen wordt sturingsinformatie of bewijs verkregen. In 40% van de gevallen wordt geen relevante opbrengst verkregen.

Een van de aandachtspunten is dat de inzet van de hackbevoegdheid arbeidsintensief is, onder andere door 1) wettelijk verplichte procedures, zoals de procedure die moet worden gevolgd om tot inzet te komen, en 2) analyse achteraf van de grote hoeveelheid data die uit de inzet van de bevoegdheid is verkregen.

[8] En in voorkomende gevallen voor andere opsporingsdiensten zoals KMar, FIOD en BOD’en.

De te volgen procedure kan inderdaad arbeidsintensief zijn vanwege de hoge eisen die gesteld worden aan die inzet. Dat acht ik noodzakelijk omdat de inzet van het middel ingrijpend van aard kan zijn.

De analyse van de grote hoeveelheid gegevens, verkregen uit de inzet van de bevoegdheid, is een van de aspecten die meegewogen worden door de officier van justitie wanneer hij overweegt om de hackbevoegdheid in te zetten. De hoeveelheid gegevens kan bijvoorbeeld worden verkleind door beperking in scope en tijdsduur.

Ook de keuring van technische hulpmiddelen die worden gebruikt bij de inzet, is een arbeidsintensief proces. Uit de hierboven genoemde eerdere evaluatie is gebleken dat het niet realistisch is om alleen te werken met vooraf goedgekeurde technische hulpmiddelen. Mijn ambtsvoorganger heeft in de reactie op die evaluatie aangegeven dat de wijze waarop met de keuring van technische hulpmiddelen omgegaan wordt, zal worden aangepast.[9] Een wijziging van de geldende regelgeving is hiervoor in voorbereiding en wordt meegenomen in de nieuwe uitvoeringsbesluiten onder het nieuwe Wetboek van Strafvordering.

Het WODC vraagt in dit kader aandacht voor de toetsing van de ingezette technische hulpmiddelen door de zittingsrechter, de keuring daarvan, en de betekenis hiervan voor het bewijs. De toetsing door de zittingsrechter is belangrijk voor de rechtsstatelijkheid van de inzet van middelen. Het WODC lijkt te constateren dat, bij gebrek aan informatie hierover in vonnissen, het in de praktijk nauwelijks voorkomt dat de rechter deze toetsing verricht en dat daarmee de rechtsstatelijkheid van de inzet van middelen in het geding kan komen. Het kabinet onderschrijft dat de mogelijkheid van rechterlijke toetsing essentieel is. Het ontbreken

---

[9] Het uitgangspunt dat alleen goedgekeurde hulpmiddelen worden ingezet wordt gewijzigd. Alle in dit kader gebruikte technische hulpmiddelen worden ter keuring aangeboden bij een keuringsdienst. Daarmee wordt inzicht verkregen in de mate waarin dit hulpmiddel aan de eisen voldoet en kan de officier van justitie bepalen of aanvullende verificatiemaatregelen moeten worden genomen als aan een eis niet, of niet volledig, wordt voldaan. Op die manier krijgen de rechter, verdediging en officier van justitie inzicht in de bewijswaarde in de rechtszaal van de verkregen informatie.

van informatie in vonnissen betekent naar het oordeel van het kabinet echter niet dat deze toetsing niet plaatsvindt. De inzet van een technisch hulpmiddel staat altijd in het proces-verbaal. De rechter kan op basis daarvan, of na bespreking ter zitting, een oordeel vellen. Het niet weergeven daarvan in het vonnis betekent niet dat er geen aandacht aan is geschonken door de rechter.

Tot slot beschrijft het WODC de rol van commerciële middelen voor het binnendringen van geautomatiseerde werken. Zij vraagt zich af of deze inzet nog wel benoemd kan worden als een ‘uiterst middel’ omdat dit gebruik inmiddels eerder regel dan uitzondering is. Ik benadruk in dit kader dat de inzet van een commercieel middel een uiterst middel is, afgezet tegen de mogelijkheid om niet-commerciële middelen met vergelijkbare functionaliteit te gebruiken.

Het gaat dus om subsidiariteit, niet om proportionaliteit. Niet-commerciële middelen blijven de voorkeur hebben. In de praktijk zijn er doorgaans echter geen niet-commerciële middelen beschikbaar en wordt in die gevallen inderdaad gebruik gemaakt van de commerciële variant.

De minister van Justitie en Veiligheid,
D.M. van Weel