28684 Naar een veiliger samenleving

Nr. 522 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 april 2018

Cybercrime heeft vele gezichten. De gevolgen kunnen zeer ingrijpend zijn. Er zijn veel slachtoffers en het worden er niet minder. Criminelen richten zich onder meer op het inbreken in computers voor nieuwe vormen van diefstal en afpersing van burgers en bedrijven, op het platleggen van websites, op bedrijfsspionage en op handel op het *darkweb*. Een zo veelomvattend fenomeen vraagt om een integrale aanpak van preventie, het voorkomen van dader- en slachtofferschap, opsporing en vervolging tot het terugdringen van recidive. De overheid vervult daarbij verschillende rollen, zoals initiatiefnemer, ondersteuner, handhaver en zo nodig als maker van beleid en regelgeving. De aanpak van cybercrime raakt sterk aan de verbetering van cyber security, vooral waar het gaat over activiteiten gericht op de preventie van cybercrime.[1] De aanpak van cybercrime en de versterking van cybersecurity worden in samenhang met elkaar vormgegeven. Over de brede Nationale cybersecurity agenda wordt u apart geïnformeerd.

In december 2016 heeft de Tweede Kamer de gewijzigde motie van het lid Recourt aangenomen (Handelingen II 2016/17, nr. 31, item 19). In deze motie wordt het kabinet opgeroepen in samenspraak met de private sector te komen tot een integraal plan van aanpak voor cybercrime, waarbij aandacht is voor preventie tot en met vervolging (Kamerstuk 34 550 VI, nr. 87). Met deze brief informeer ik u, mede namens de minister voor Rechtsbescherming en de staatssecretaris van Economische Zaken en Klimaat, over de integrale aanpak van cybercrime en kom ik tegemoet aan het verzoek van de Kamer.

Cybercrime

De digitale revolutie biedt enorme schaalvoordelen en de mogelijkheid om overal ter wereld eenvoudig en snel contacten te leggen. De keerzijde daarvan is dat ook criminelen op grote schaal hun activiteiten via internet ontplooien. Zo was 1 op de 9 personen in 2017 slachtoffer van cybercrime.[2] Meer mensen zijn inmiddels slachtoffer van hacken dan van fietsendiefstal. Waar de criminaliteit over het geheel genomen daalt, geldt dat niet voor cybercrime.

Achter de term cybercrime gaat een grote variëteit aan verschijningsvormen schuil van zowel oude criminaliteit in digitale vorm als nieuwe criminaliteit. Het gaat bijvoorbeeld om het hacken van computers om geld naar criminele bankrekeningen over te schrijven, of het ongemerkt aanzetten van camera's en microfoons om mensen in hun eigen omgeving te kunnen bespioneren. Beroepscriminelen en statelijke actoren vormen al enkele jaren de grootste dreiging voor de veiligheid in de digitale wereld. Bovendien richten zij de meeste schade aan. Beroepscriminelen hebben het vooral gemunt op private organisaties en burgers voor de diefstal van gegevens die vervolgens kunnen worden doorverkocht of gepubliceerd.[3] In 2016 had 20 procent van de bedrijven met 10

[1] Het cybersecuritybeleid beoogt Nederland digitaal veilig te houden en richt zich op het geheel aan maatregelen om schade door verstoring, uitval of misbruik van ICT te voorkomen en, indien er toch schade is ontstaan, het herstellen hiervan, met bijzondere aandacht voor de vitale belangen van Nederland. De aanpak van cybercrime richt zich op het voorkómen en bestrijden van strafbare feiten en het beperken van slachtofferschap, daderschap en recidive. Daarbij gaat het om zowel high tech crime als veel voorkomende criminaliteit.

[2] Veiligheidsmonitor 2017

of meer werknemers te maken met de gevolgen van cybercrime.[4] Vooral voor kleine ondernemingen kan het risico groot zijn. Een ransomware-aanval kan bijvoorbeeld klantgegevens ontoegankelijk maken en de bedrijfsvoering onmogelijk maken, met grote financiële gevolgen. Op internet is een markt ontstaan van criminele dienstverlening, ook wel aangeduid met de term *cybercrime-as-a-service*. Hierdoor is het voor cybercriminelen niet langer nodig uitgebreide technische kennis te hebben om toch met gebruik van technologie succesvol te zijn. Zo kan één kwaadwillend individu bijvoorbeeld met een DDOS-aanval de toegang tot diensten van een bedrijf of overheidsorganisatie blokkeren. De verschillen tussen *high tech* cybercrime, *advanced persistent threats* en veel voorkomende criminaliteit worden daardoor minder scherp.[5]

Meerdere typen daders
Er lijken diverse typen daders actief. Bij sommigen gaat het meer om de kick van de geavanceerde hack dan om het financieel gewin. Het is de vraag of gebruikelijke interventies bij alle daders van cybercrime bruikbaar zijn.[6] Daders van cyberdelicten, ook met ernstige gevolgen, zijn veelal jonger dan bij zogenaamde traditionele criminaliteit. Het gaat dan bijvoorbeeld om *scriptkiddies,* waarbij het risico bestaat dat ze een criminele carrière ontwikkelen en doorgroeien naar doorgewinterde cybercriminelen.

Slachtoffers - doorlopend en overal potentieel doelwit
De doorlopende verbinding van een ieder met het internet maakt dat er op elk moment veel potentiële slachtoffers zijn. Zo hebben de meeste mensen hun telefoon altijd aan staan, en zijn daarmee altijd bereikbaar voor criminelen. Gezien de enorme hoeveelheid, soms zeer persoonlijke, gegevens die op een telefoon staan, of via de telefoon kunnen worden buitgemaakt, kunnen de gevolgen voor slachtoffers groot zijn. Door een telefoon te hacken kunnen bijvoorbeeld privéfoto's worden overgenomen, die vervolgens gebruikt kunnen worden voor afpersing. Van veel bedrijven is de internetpagina altijd bereikbaar, en daarmee kwetsbaar voor hacks en DDoS-aanvallen. Het internet biedt aan criminelen kansen voor schaalvergroting. Door bijvoorbeeld de verspreiding van *ransomware* kunnen wereldwijd slachtoffers voor afpersing worden gevonden. Gegevens in allerlei soorten databanken zijn een waardevol doelwit om nieuwe criminele activiteiten te kunnen ontplooien. Voor specifieke, waardevolle doelen geldt dat meer geavanceerde criminele werkwijzen worden toegepast. Slachtoffers blijken echter vaak onwetend over de gevaren en de, vaak redelijk eenvoudige, maatregelen die ze kunnen nemen. Zo worden veiligheidsupdates vaak niet tijdig geïnstalleerd of men laat zich weinig gelegen liggen aan de mogelijke gevaren.[7]

Opsporing lastig
De anonimiteit en snelheid van de ontwikkelingen in de digitale wereld vormen voor de opsporing een bijzondere uitdaging. Contact leggen over het internet kan anoniem en versleuteld. De technologie om de privacy van gebruikers te beschermen wordt ook gebruikt door criminelen om hun identiteit beter af te schermen. Op het *darkweb* zijn diverse criminele marktplaatsen actief die de handel in bijvoorbeeld wapens en verdovende middelen faciliteren. Bovendien worden continu nieuwe digitale producten en diensten ontwikkeld, ook voor criminele doeleinden.

---

[3] Cyber Security Beeld Nederland 2017

[4] CBS.nl 25 september 2017

[5] Internet Organised Crime Threat Assessment (iOCTA), Europol 2016

[6] Kamerstukken 28741 en 28 684, nr. 33

[7] iOCTA 2016

Kenmerkend voor het internet is bovendien dat het geen territoriale grenzen kent. Veel daders van vooral georganiseerde cybercriminaliteit bevinden zich niet in Nederland, terwijl hier wel slachtoffers worden gemaakt of de Nederlandse digitale infrastructuur voor criminele doeleinden wordt gebruikt. Dader en slachtoffer hoeven elkaar evenmin fysiek te treffen. De plaats-delict is daarmee vaak op meerdere fysieke locaties tegelijk en vaak in meerdere landen. De internationale procedures voor de opsporing zijn hier onvoldoende op toegesneden.

De huidige bevoegdheden en capaciteiten zijn onvoldoende om een vuist te maken tegen cybercrime. Dankzij de inzet van velen worden belangrijke successen geboekt, maar desondanks gaan nog te veel criminelen vrijuit. Dat moet veranderen. Het internet mag geen vrijplaats worden voor criminelen en misdaad mag niet lonen.

Uitgangspunten
Gezien de snelheid van de ontwikkeling van cybercrime, het gebrek aan lokale binding en de belangrijke rol van private partijen zijn flexibiliteit, integraliteit en samenwerking leidende uitgangspunten van de aanpak.

Flexibiliteit en integraliteit
Criminele werkwijzen blijven zich in een hoog tempo ontwikkelen. Bovendien worden innovatieve en technologisch complexe criminele werkwijzen snel bekend bij - en beschikbaar voor - minder technisch onderlegde criminelen, bijvoorbeeld door deze werkwijzen aan te bieden als *cybercrime-as-a-service*. Voor de aanpak betekent dit dat flexibiliteit geboden is. Een te specifieke, rigide planning van maatregelen voor de lange termijn is weinig effectief. Snel kunnen reageren op de wisselende werkwijzen is nodig. Voor de aanpak van cybercrime is het bijvoorbeeld nodig om nieuwe criminele werkwijzen snel te onderkennen, interventies erop uit te werken en, indien deze succes hebben, snel breed uit te dragen binnen de politie, het Openbaar Ministerie en richting andere samenwerkingspartners. Daarnaast wordt cybercrime integraal benaderd door te kijken welke acties (preventie, opsporing, vervolging, verstoring, of een combinatie daarvan) het crimineel verdienmodel het meest effectief kunnen verstoren. Zo kan bijvoorbeeld flexibele publieksvoorlichting, onder meer via sociale media, helpen om bij de opkomst van nieuwe werkwijzen snel het publiek te informeren, zodat potentiële slachtoffers maatregelen kunnen nemen om het criminelen moeilijker te maken.

Samenwerking
De maatschappelijke opgave voor de overheid is het terugdringen van cybercrime, het verminderen van de gevolgen ervan en het aanpakken van de daders. De overheid kan dat niet zonder samenwerking met het bedrijfsleven, burgers en maatschappelijke organisaties. In zo'n integrale aanpak hebben overheden, bedrijven, burgers en maatschappelijke organisaties ieder hun eigen verantwoordelijkheid. Het internet en de dienstverlening daarop zijn voor het overgrote deel niet in handen van de overheid. De aanpak van cybercrime vergt daarom intensieve samenwerking met private partijen die voor het internet essentiële diensten verlenen. Het zijn grotendeels private partijen die kennis en mogelijkheden hebben om cybercrime te voorkomen, snel te onderkennen, barrières op te werpen en te verstoren. Bovendien hebben de private partijen veelal de gegevens in beheer die nodig zijn voor de opsporing.

Het ministerie van Justitie en Veiligheid zoekt ook actief de samenwerking met andere ministeries en medeoverheden. Het ministerie van Economische Zaken en Klimaat draagt bijvoorbeeld zorg voor het opzetten van een Digital Trust Centre voor (niet-vitaal) ondernemend Nederland en – samen met de NCTV en ECP - de voorlichtingsportal veiliginternetten.nl. Ook lokale overheden kunnen een

belangrijke bijdrage leveren aan het tegengaan van cybercrime. Zij zijn bijvoorbeeld vaak beter in staat samen te werken met lokale private organisaties.

Vanwege de grenzeloosheid van het internet is daarnaast internationale politiële en justitiële samenwerking onontbeerlijk. In de praktijk blijkt het gebruik van de in het internationaal verkeer gangbare vormen van samenwerking vaak te langzaam en te bewerkelijk voor een effectieve opsporing. Bovendien maken ook criminelen gebruik van anonimiseringstechnieken zoals VPN[8] en TOR[9], en encryptie. Veelal is het dan niet goed mogelijk te bepalen waar (op welke servers in welk land) gegevens zich bevinden en daarmee met welk land samenwerking kan worden gestart om de opsporing ter hand te nemen. De rechtshandhaving op het internet staat daardoor onder druk. Nederland is actief voor het versterken van de samenwerking en het vinden van nieuwe methoden om de effectiviteit van de internationale opsporing te verbeteren. Aanpassing van de internationale juridische kaders kan de samenwerking ondersteunen.

Vier sporen
De huidige aanpak van cybercrime richt zich vooral op het opsporen, vervolgen en verstoren van strafbare feiten, preventie (vooral door bewustwording), en het versterken van de wet- en regelgeving. Deze aanpak wordt voortgezet en geïntensiveerd. Daarnaast worden er nieuwe elementen aan toegevoegd, zoals preventieve maatregelen voor potentiële daders en slachtoffers, een mogelijk andere vorm van ondersteuning van slachtoffers en een aanpak van daders ter voorkoming van recidive. Daarnaast is meer kennis nodig voor beleidsvorming op de langere termijn. De integrale aanpak van cybercrime bestaat uit vier sporen:

1. Er wordt geïnvesteerd in preventie.
2. De opsporing wordt versterkt, criminele activiteiten worden verstoord en daders worden aangepakt.
3. De ondersteuning van slachtofferschap wordt toegesneden op cybercrime.
4. De wetenschappelijke kennis over cybercrime wordt vergroot.

Preventie
Burgers en organisaties zijn in beginsel zelf verantwoordelijk voor het nemen van maatregelen om de eigen veiligheid te vergroten. Dat geldt ook in het digitale domein. De overheid helpt hen daarbij, bijvoorbeeld door basiskennis over digitale veiligheid breed beschikbaar te maken en de veiligheid van hard- en software te stimuleren. De overheid heeft hierbij ook aandacht voor de verschillen in behoeften en mogelijkheden van mensen: wat burgers op het punt van digitale veiligheid zelf aan kunnen, en waar ze kwetsbaar zijn, varieert en vraagt soms specifieke aandacht. Hierbij komt de noodzaak tot samenwerking met diverse partners binnen en buiten de overheid duidelijk naar voren. Private partijen hebben veelal de beste mogelijkheden om de veiligheid in technische zin te versterken en burgers, hun klanten, te helpen. Gemeenten van hun kant zijn vaak goed in staat kleine en middelgrote organisaties en burgers actief te benaderen.

Om cybercrime te beperken is het van belang dat potentiële slachtoffers weten hoe zij zichzelf beter kunnen beschermen. Veel ICT-professionals en grote organisaties zijn goed bekend met mogelijke beschermingsmaatregelen. Dat is mede te danken aan de bewustwordingsactiviteiten op het gebied van cyber security, zowel vanuit de overheid als vanuit het bedrijfsleven. Individuen en kleine en middelgrote ondernemingen zijn vaak onvoldoende bekend met de risico's van cybercrime en met de relatief eenvoudige maatregelen die zij zelf kunnen nemen om zich beter te beschermen. In samenwerking met het ministerie van Economische Zaken en Klimaat en met private partijen wordt gewerkt aan het

[8] Een Virtual Private Network (VPN) is een geïsoleerde, versleutelde verbinding tussen een apparaat en een bepaalde server op het internet.
[9] Een open netwerk voor anonieme communicatie waarbij het vaststellen van de herkomst en bestemming van berichten door derden wordt tegengegaan.

ondersteunen van deze groep (consumenten en bedrijfsleven). Extra aandacht voor het effectief bereiken van specifieke groepen is daarvoor nodig. Daarnaast wordt gewerkt aan het verbeteren van de veiligheid van hard- en software.

Opsporing, vervolging, sanctionering en verstoring
Strafrechtelijke handhaving is een kerntaak van de overheid, ook in het digitale domein. Het versterken van de strafrechtelijke aanpak blijft nodig ter bescherming van (potentiële) slachtoffers en om te zorgen dat misdaad niet loont. Het Team High Tech Crime van de Landelijke Eenheid van de politie is inmiddels 120 personen sterk. Daarnaast werkt de politie aan de opbouw van cybercrimeteams in de regionale eenheden. Het Openbaar Ministerie beschikt bij het Landelijk Parket en de regionale parketten over gespecialiseerde capaciteit voor de opsporing en vervolging van cybercrime. De huidige aard en omvang en de verwachte impact van cybercriminaliteit vragen echter extra capaciteit en versterking van de expertise in de strafrechtketen, en om adequate bevoegdheden. Waar het identificeren en aanhouden van cybercriminelen lastig blijkt, zullen - ook met de inzet van de nieuwe wettelijke bevoegdheden uit de Wet Computercriminaliteit III - criminele activiteiten worden verstoord, bijvoorbeeld door het binnendringen en offline halen van servers. Naast de zaaksgerichte oriëntatie is verstoren zo onderdeel van de handhavingsstrategie tegen cybercrime. Waar nodig worden voorstellen ontwikkeld om de juridische kaders aan te passen, zowel nationaal als internationaal. Daarnaast wordt in overleg met private partijen gezorgd dat criminelen niet te gemakkelijk bonafide dienstverleners voor hun activiteiten kunnen misbruiken. Om recidive te beperken is bovendien van belang dat de interventies voor daders van cybercrime zijn toegesneden op de risicofactoren van deze daders.

Aandacht voor slachtoffers
Slachtofferschap van cybercriminaliteit is helaas niet uit te sluiten. De overheid kan slachtoffers ondersteunen en helpen herhaald slachtofferschap te voorkomen. Er wordt ingezet op ondersteuning om de impact van cybercriminaliteit te minimaliseren. Bij veel vormen van cybercrime zijn mensen of organisaties zich vaak niet bewust dat hun systemen door criminelen zijn gecompromitteerd of worden gebruikt voor criminele activiteiten. Het informeren van slachtoffers (slachtoffernotificatie) is dan zowel voor hen zelf van belang als ter voorkoming van nieuwe slachtoffers. Door het snel informeren van slachtoffers kan de schade worden beperkt. Bovendien kan dit verstorend werken voor de criminele activiteit. Door versterking van het aangifteproces wordt daarnaast gezorgd dat de politie eenvoudiger bereikbaar is voor slachtoffers van cybercrime.

Wetenschappelijk onderzoek
Cybercrime bestaat al enige tijd, en er wordt ook onderzoek naar gedaan. Er zijn echter minder wetenschappelijke inzichten dan gewenst, vooral als het gaat om daderschap en slachtofferschap van veel voorkomende vormen van cybercrime. Daarom is gestart met een breed wetenschappelijk onderzoeksprogramma. Het ministerie van Justitie en Veiligheid is opdrachtgever voor deze onderzoeken.

Financiële aspecten
In de Rijksbegroting voor 2018 is een structurele intensivering opgenomen voor de politie van € 6 miljoen structureel. Dit bedrag wordt aangewend voor een beperkte uitbreiding van de capaciteit en verbetering van ICT-middelen voor digitale opsporing. Voor het Openbaar Ministerie is een intensivering opgenomen van € 1 miljoen structureel, die zal worden aangewend voor een beperkte uitbreiding van de capaciteit. Daarnaast is een bedrag van € 3,5 miljoen voorzien voor de opbouw van een Digital Trust Center. Het regeerakkoord Vertrouwen in de Toekomst bevat een investering voor cyber security voor diverse departementen. Voor het ministerie van Justitie en Veiligheid gaat het om een

bedrag oplopend tot € 16 miljoen structureel. Een investering van € 10 miljoen structureel voor de uitvoering van de wet Computercriminaliteit III maakt daar deel van uit. Het resterende bedrag wordt onder meer geïnvesteerd in maatregelen ten behoeve van de cyberveiligheid, wat ook een preventief effect heeft op cybercrime. Naast deze specifieke posten wordt er geïnvesteerd in de betrokken organisaties. Zo bevat het regeerakkoord investeringen in de politie en de strafrechtketen. De hiervoor gereserveerde bedragen worden voor een deel aangewend voor de versterking van de aanpak van cybercrime en de keteneffecten daarvan.

Afsluiting

Het internet blijft zich snel ontwikkelen, vaak op een weinig planmatige wijze. Het is daarom lastig te voorspellen hoe de criminaliteit zich zal ontwikkelen. Daarnaast zijn private partijen van groot belang voor een effectieve aanpak. Flexibiliteit, integraliteit en samenwerking zijn onze uitgangspunten. Maatregelen worden de komende periode samen met private partijen uitgewerkt, en vaak zal aanpassing nodig zijn op basis van veranderingen in de uitingsvormen van cybercrime, of op basis van onderzoek of overleg met publieke en private partners. De maatschappelijke opgave om cybercrime tegen te gaan is niet in de tijd begrensd. De komende jaren is te verwachten dat nieuwe maatregelen nodig worden, of de wijze van uitvoering moet worden aangepast. Het ministerie van Justitie en Veiligheid blijft in gesprek met diverse publieke en private partijen over hun visie op cybercrime en de beste manieren om die gezamenlijk te lijf te gaan. Alleen met een flexibele, gezamenlijke inspanning kan de criminaliteit van de toekomst worden aangepakt.

De minister van Justitie en Veiligheid,

F.B.J. Grapperhaus

Bijlage – maatregelen per spoor

Preventie
Flexibele, snel inzetbare preventiecampagnes
Bij de opkomst van nieuwe criminele werkwijzen dient snel een breed publiek over mogelijke tegenmaatregelen te worden geïnformeerd. Afhankelijk van de specifieke criminele werkwijze worden de tegenmaatregelen en communicatieboodschappen aangepast. Samen met private partijen wordt op basis van (gedrags)wetenschappelijke inzichten bezien welke kernboodschappen het meest effectief zijn voor een breed publiek of waar een campagne op een specifieke doelgroep meer aangewezen is. Dat vergt ook nauwe afstemming en het stroomlijnen van kernboodschappen.

Ondersteuning veiligheid mkb-ondernemingen
Het bedrijfsleven wordt steeds vaker digitaal aangevallen en specifieke ondersteuning is gewenst. De nader gewijzigde motie van de leden Hijink en Tellegen[10] roept op tot de oprichting van een Digital Trust Centre (DTC) om het bedrijfsleven weerbaarder te maken. Het doel van het DTC is om ondernemend Nederland in staat te stellen zich weerbaarder te maken tegen cyberaanvallen. Overigens is in 2016 in opdracht van het Nationaal Platform Criminaliteitsbeheersing gestart met branchegerichte onderzoeken en zijn gratis veiligheidschecks aangeboden aan ondernemers.

Ondersteuning gemeenten en regionale Platforms Veilig Ondernemen
Gemeenten hebben vaak goed zicht op de lokale prevalentie van criminaliteit en de mogelijkheden om deze aan te pakken. Het ministerie van Justitie en Veiligheid ondersteunt pilot-initiatieven van gemeenten en Platforms Veilig Ondernemen die naar verwachting ook in andere regio's en gemeenten, toegesneden op de lokale situatie, toepasbaar zijn.

Digitaal veilige hard- en software
Het is belangrijk dat producten digitaal veilig zijn. Het ministerie van Economische Zaken en Klimaat stelt in samenspraak met het ministerie van Justitie en Veiligheid een *roadmap* digitaal veilige hard- en software op. Deze *roadmap* wordt naar verwachting in het voorjaar van 2018 aan de Tweede Kamer aangeboden.[11]

Opsporing, vervolging, sanctionering en verstoring
Versterking aanpak van de politie en in de strafrechtketen
Tijdens de vorige regeerperiode is de politie gestart met de opbouw van cybercrimeteams in de regionale eenheden van de politie. Deze regering investeert daarbovenop in de politie en de overige partners in de strafrechtketen. Het gaat daarbij om de uitbreiding van capaciteit en expertise op het gebied van informatievoorziening, preventie en verstoring, en het versterken van de samenwerking met private partijen. De investering in capaciteit gaat gepaard met versterking van de ICT-ondersteuning.

Bewustwording hostingproviders
De private sector is in overleg met het ministerie van Economische Zaken en Klimaat gestart met het project Abuse 2.0. Dit project is gericht op het verbinden van marktpartijen om diverse vormen van cybercrime sneller te onderkennen en met elkaar te delen, zodat private partijen zelf maatregelen kunnen nemen. De aangesloten bedrijven lopen zo minder kans cybercrime te faciliteren.

Verstoring crimineel verdienmodel

[10] Kamerstuk 26643 nr. 473, 13 juni 2017

[11] Kamerstuk 26643 nr. 507, 7 december 2017.

Om criminaliteit niet te laten lonen, ook als geen reëel zicht is op een veroordeling, wordt ingezet op het verstoren van het criminele verdienmodel. Daarvoor worden opkomende criminele werkwijzen geanalyseerd, vaak in publiek-privaat verband, en wordt bezien welke interventies kunnen worden ingezet om het criminelen zo lastig mogelijk te maken.

Versterking nationale wetgeving
Het wetsvoorstel Computercriminaliteit III (Kamerstuk 34 372) is momenteel aanhangig in de Eerste Kamer. Voor de uitvoering is vanaf 2019 € 10 miljoen per jaar beschikbaar. De wet wordt twee jaar na de inwerkingtreding geëvalueerd. Daarnaast wordt de komende periode bezien of aanvullende wettelijke maatregelen nodig zijn.

Internationale samenwerking
Voor de opsporing in de digitale wereld is internationale samenwerking essentieel. In het kader van de EU en in het kader van de Raad van Europa wordt gewerkt aan het verbeteren van de procedures voor internationale samenwerking, waaronder de rechtshulp.

Versterking internationale juridische kaders
Nederland heeft de afgelopen jaren een voortrekkersrol gespeeld bij de verbetering van de internationale kaders voor de opsporing op internet en zal zich hiervoor blijven inzetten, zowel in de Europese Unie als in de Raad van Europa. Deze kaders moeten bijdragen aan snellere en effectieve toegang tot elektronische gegevens.

Aanpak jonge (potentiële) daders en beperking recidive
Samen met onder meer de politie, Halt en de Raad voor de Kinderbescherming wordt verkend met welke interventies jonge (potentiële) daders op het rechte pad kunnen worden gebracht of gehouden. Daarnaast wordt met onder meer de reclassering bezien of daders van cybercrime een andere benadering vergen om de kans op recidive te verminderen, bijvoorbeeld door andere begeleidingsvormen tijdens het toezicht.

Verbetering aangifteproces
De aangiftebereidheid van cybercrime is lager dan bij traditionele criminaliteit. De politie is voornemens voor bepaalde vormen van cybercrime digitale aangifte mogelijk te maken, zodat de drempel voor slachtoffers om aangifte te doen omlaag gaat.

Aandacht voor slachtoffers
Slachtoffernotificatie en schadebeperking
Binnen de versterking van de organisaties in de strafrechtketen is aandacht voor verbetering van de communicatie met slachtoffers. Het kan daarbij gaan om individuele burgers of om organisaties die slachtoffer zijn geworden. Het actief notificeren van slachtoffers en het bieden van handelingsperspectief kan schade beperken en tegelijk een sterk verstorend effect hebben op criminele activiteiten. Bijvoorbeeld bij *botnets* of *ransomware* kunnen slachtoffers door hun eigen systemen op te schonen er voor zorgen dat vanuit hun systemen geen nieuwe slachtoffers worden benaderd. De website www.nomoreransom.org is hiervan een goed voorbeeld.

Wetenschappelijk onderzoek
Voor de versterking van de wetenschappelijke kennis over cybercrime en de beleidsvorming in de toekomst worden in ieder geval de volgende onderzoeken uitgevoerd.
- Aard en omvang van cyber- en gedigitaliseerde criminaliteit
- Slachtofferschap van cyber- en gedigitaliseerde criminaliteit

- Verstoren van cyber- en gedigitaliseerde criminaliteit
- Strafrechtelijke aanpak van cyber- en gedigitaliseerde criminaliteit