26 643 Informatie- en communicatietechnologie (ICT)

29 911 Bestrijding georganiseerde criminaliteit

Nr. 1357 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 27 juni 2025

Cybercriminaliteit is een blijvende dreiging voor onze samenleving, economie en nationale veiligheid. Deze vorm van criminaliteit is complex, grensoverschrijdend en voortdurend in ontwikkeling. Nederland voert daarom een actief beleid van preventie, opsporing, verstoring en vervolging. Met deze brief informeer ik uw Kamer over de voortgang van de integrale aanpak van cybercrime en de versterking van de bevoegdheden in het digitale domein.[1] Daarbij komen de volgende onderwerpen aan de orde:

i. Het beeld en de ontwikkeling van cybercriminaliteit;
ii. Preventie;
iii. Opsporen, verstoren en vervolgen in het algemeen;
iv. Verkenning naar de aanpak van bad hosting (conform toezegging tijdens commissiedebat cybercrime in oktober 2024, Kamerstuk 26643, nr. 1246);
v. De resultaten uit de Veiligheidsagenda 2023-2026;
vi. De extra investeringen voor de bestrijding van cybercrime en gedigitaliseerde criminaliteit;
vii. Een update van verschillende trajecten ter versterking van de bevoegdheden in het digitale domein;
viii. Internationale trajecten

Tenslotte bevat deze brief mijn reactie op de motie Ceder-Six Dijkstra over de inspanningen om Telegram aan zijn wettelijke verplichtingen te houden en de motie Michon-Derkzen over het publiceren van de jaarlijkse resellerbrief.

[1] Cybercrime in enge zin betreft misdrijven die niet zonder tussenkomst van een computer of andere ICT-middelen gepleegd kunnen worden, zoals computervredebreuk of DDoS-aanvallen. Misdrijven die (deels) online plaatsvinden, maar ook enkel in het fysieke domein kunnen bestaan, worden aangeduid met de term gedigitaliseerde criminaliteit. Voorbeelden daarvan zijn online drugshandel en online fraude.

Als bijlagen bij deze brief vindt u een overzicht van de activiteiten in het kader van de preventie van cybercrime en een nadere beschrijving van de activiteiten in het kader van de verkenning naar de bad hosting-problematiek.

Over de voortgang van de integrale aanpak online fraude ontvangt uw Kamer een separate brief.

i. Algemeen beeld: ontwikkeling cybercriminaliteit en cijfers

In 2024 gaf volgens het CBS 16 procent van de Nederlanders van 15 jaar of ouder aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van een of meer vormen van online criminaliteit.[2] Dit zijn 2,4 miljoen mensen. 4 procent, zeshonderdduizend mensen, had te maken met hacken (computervredebreuk).[3]

Het Cybersecuritybeeld Nederland 2024 (CSBN 2024) laat zien dat cybercriminaliteit een structurele dreiging blijft die in complexiteit toeneemt. Cybercriminelen professionaliseren zich steeds verder en maken gebruik van geavanceerde aanvalsmethoden. Ransomware blijft een van de grootste dreigingen. Voor cybercriminelen blijft afpersing na data-exfiltratie (datadiefstal) of versleuteling van bestanden een aantrekkelijk verdienmodel. Het rapport signaleert een groeiende overlap tussen cybercriminaliteit en statelijke dreigingen. Criminele groepen opereren soms in dienst van of met toestemming van buitenlandse overheden om geopolitieke doelen te bereiken.[4]

Politie en OM constateren dat de drempel voor cybercriminaliteit is verlaagd. Waar voorheen technische expertise vereist was, kunnen tegenwoordig kant-en-klare tools en handleidingen eenvoudig online worden aangeschaft via platforms zoals Telegram, fora en het dark web. Dit stelt individuen in staat om met minimale investering en technische kennis cyberaanvallen uit te voeren.[5]

---

[2] CBS, Monitor Online Veiligheid 2024.
[3] Dit is een daling ten opzichte van de rapportage van het CBS in 2023 waar 6 procent aangaf te maken te hebben gehad met hacken.
[4] NCTV, Cybersecuritybeeld Nederland 2024.
[5] Politie, Cybercrimebeeld Nederland 2024.

Europol geeft in het Internet Organised Crime Threat Assessment 2024 (iOCTA 2024) aan dat AI steeds vaker wordt ingezet door criminelen. Ook in de EU Serious and Organised Crime Threat Assessment 2025 (EU SOCTA 2025) vermeldt Europol een aanzienlijke toename en evolutie van cybercriminaliteit waarbij AI een cruciale rol speelt. Criminelen gebruiken AI-gestuurde tools om aanvallen te automatiseren, beveiligingsmechanisme te omzeilen en phishing-tactieken te verbeteren.[6] Volgens Europol vergemakkelijkt het gebruik van digitale platforms en crypto-valuta illegale activiteiten waardoor criminele netwerken gemakkelijker kunnen opereren en financiële transacties kunnen uitvoeren. Het gebruik van het dark web en versleutelde communicatieplatforms biedt cybercriminelen bovendien anonimiteit en veilige kanalen om met elkaar te communiceren, te handelen en kennis te delen. Deze factoren dragen bij aan de complexiteit en schaal van cybercriminaliteit.

In de Rapportage Datalekken 2023 meldt de Autoriteit Persoonsgegevens (AP) meer dan 25.000 meldingen van datalekken, waarbij ongeveer 20 miljoen mensen werden getroffen. Van deze meldingen waren er ruim 1.300 het gevolg van cyberaanvallen zoals hacking, malware of phishing. Opvallend is dat organisaties in 70 procent van de gevallen de risico’s van dergelijke aanvallen te laag inschatten, waardoor slachtoffers niet tijdig werden geïnformeerd en zich onvoldoende konden beschermen tegen mogelijke vervolgmisdrijven.[7] Daarnaast rapporteerde de AP in haar eerste ransomware-rapportage dat in 2023 zeker 178 geslaagde ransomware-aanvallen plaatsvonden, die vaak meerdere organisaties tegelijkertijd troffen en persoonsgegevens van miljoenen Nederlanders raakten. Uit nader onderzoek naar de aanvallen bleek volgens de AP dat bij tweederde van de getroffen organisaties de basisbeveiliging niet op orde was.[8] Ook uit een analyse die mogelijk gemaakt is door project Melissa (het publiek-private samenwerkingsverband om ransomware te bestrijden) komt naar voren dat cybercriminelen nog steeds het vaakst via kwetsbaarheden in software en via account-takeover toegang verkrijgen.[9]

---

[6] EU-SOCTA, EU Serious and Organised Crime Threat Assessment 2025.
[7] Autoriteit Persoonsgegevens, Rapportage datalekken 2023.
[8] Autoriteit Persoonsgegevens, Rapportage ransomware 2023.
[9] Nationaal Cyber Security Centrum, Jaarbeeld Ransomware 2023.

ii. Preventie

Het verhogen van de cyberweerbaarheid van burgers, bedrijven en instellingen blijft een punt van aandacht. Met de Nederlandse Cybersecurity Strategie (NLCS) 2022-2028 streeft het kabinet naar een digitaal veilig Nederland waarin burgers en bedrijven ten volle kunnen profiteren van deelname aan de digitale samenleving. De strategie beschrijft deze stip op de horizon en de keuzes die het kabinet maakt om hier te komen.[10] De aanpak van cybercrime (in enge zin) maakt deel uit van die strategie. In het actieplan van de NLCS is de uitwerking van de strategie in acties opgenomen.

De afgelopen jaren zijn diverse cyberbewustwordingscampagnes, tools en kennisproducten voor organisaties ontwikkeld door het Nationaal Cybersecurity Centrum (NCSC) en het Digital Trust Center (DTC) om de digitale weerbaarheid in Nederland te versterken. Een voorbeeld hiervan is de ‘5-basisprincipes van digitale weerbaarheid’, ondernemers kunnen deze basisprincipes gebruiken als handvatten voor het ontwikkelen van een gezonde en degelijke cyberbeveiligingsstrategie.[11]

De ministeries van Justitie en Veiligheid, Binnenlandse Zaken en Koninkrijksrelaties, en Economische Zaken werken daarnaast nauw samen aan het vormgeven van communicatie richting burgers, bedrijven en andere overheden.[12] Een aantal voorbeelden zijn de campagnes “laat je niet interneppen”, “dubbel beveiligd is dubbel zo veilig” en “doe je updates”,[13] Alert Online en de tool Cyberweerbaarheid.[14] Naast campagnes en pilots vindt er ook publiek-private samenwerking plaats onder de vlag van het Actieprogramma Veilig Ondernemen,[15] waarbij de City Deal Lokale Weerbaarheid Cybercrime een belangrijke rol vervult voor het ontwikkelen van actuele interventies die bijdragen aan het

---

[10] NCTV, Nederlandse Cybersecuritystrategie 2022-2028.
[11] Nationaal Cyber Security Centrum, ‘5 basisprincipes van digitale weerbaarheid, wat kun je zelf doen?’ (5 basisprincipes van digitale weerbaarheid | Wat kun je zelf doen? | Nationaal Cyber Security Centrum)
[12] NLCS, pijler 4, actie 4 (voorlichtingscampagnes) en pijler 3 actie 3 (defensieve cybercapaciteiten)
[13] Doe je updates (veiliginternetten.nl)
[14] Cyberweerbaarheid - Het CCV (hetccv.nl)
[15] Actieprogramma Veilig Ondernemen 2023 t/m 2026 | Rapport | Rijksoverheid.nl

verhogen van de cyberweerbaarheid van verschillende doelgroepen.[16]

In de zomer van 2025 wordt door het NCSC in samenwerking met KPN een pilot gestart om de inzet van een effectief Anti Phishing Shield (APS) in Nederland te onderzoeken. Een Anti Phishing Shield (APS) is een systeem dat internetgebruikers herleidt naar een waarschuwingspagina in het geval zij een malafide website dreigen te bezoeken. Het Centrum voor Cybersecurity België (CCB) heeft een aantal jaar geleden een APS opgetuigd, waarbij in 2022 maar liefst 14 miljoen keer werd voorkomen dat een malafide website werd bezocht[17].

In bijlage 1 bij deze brief vindt u een overzicht van de verschillende preventieactiviteiten die zich concentreren op drie typen maatregelen:

- (potentiële) slachtoffers weerbaarder maken door hun basisveiligheid te vergroten (slachtofferpreventie);
- de daderpopulatie verkleinen door middel van gerichte interventies om daderschap te ontmoedigen en recidive te beperken (daderpreventie); en
- systemen en producten waar burgers en bedrijven gebruik van maken veiliger maken (situationele preventie).

iii. Opsporen, verstoren en vervolgen van cybercrime in het algemeen

Cybercrime ontwikkelt zich tot een steeds complexere en professionelere vorm van criminaliteit, waarbij de drempel om deel te nemen laag is en de impact op slachtoffers groot. Bovendien zijn de risico’s voor criminelen om gepakt of veroordeeld te worden relatief laag. Cybercriminelen opereren vaak vanuit landen waarmee samenwerking en rechtshulp moeilijk is.[18] Daarbij speelt ook geopolitiek een rol. Wanneer verhoudingen met andere landen (verder) verslechteren, zorgt dit ervoor dat opsporing en vervolging nog complexer is.[19] Door het grensoverschrijdend karakter van het internet versus de territoriaal gedefinieerde bevoegdheden van politie en justitie is het onderzoek naar cybercriminaliteit vaak

[16] City Deal Lokale Weerbaarheid Cybercrime - Het CCV (hetccv.nl)
[17] 14 miljoen kliks naar verdachte websites vermeden dankzij uniek Anti-Phishing Shield | Centrum voor Cybersecurity België
[18] Politie, Cybercrimebeeld Nederland 2024.
[19] NCTV, Cybersecuritybeeld Nederland 2024.

complex, terwijl het plegen van strafbare feiten niet door grenzen wordt gehinderd. Criminelen kunnen met één handeling vaak vele mogelijke slachtoffers maken, waardoor het plegen van deze delicten al snel loont. Cybercrime is tot slot steeds meer verweven geraakt met traditionele criminaliteit, mede doordat de offline en online wereld steeds meer samenkomen.

Cybercrime vereist dan ook een brede aanpak. Strafrechtelijke handhaving blijft essentieel, maar wordt aangevuld met verstoringsmaatregelen zoals het offline halen van criminele infrastructuren, het onderbreken van het criminele verdienmodel en het inzetten van alternatieve interventies. Uit wetenschappelijk onderzoek blijkt dat een gecombineerde aanpak en onvoorspelbare inzet van diverse interventies (waaronder sancties, arrestaties, de inzet van de-cryptors[20] en het uitschakelen van servers die worden gebruikt voor data exfiltratie) bijdraagt aan de effectiviteit van de rechtshandhaving bij de bestrijding van ransomware.[21]

Zowel bij het OM als bij de politie wordt op basis van trends en ontwikkelingen van de afgelopen jaren gewerkt aan aanpassingen en vernieuwingen om cybercriminaliteit aan te pakken. Naast de brede aanpak van cybercrime wordt daarbij ook gekeken naar de verwevenheid van verschillende vormen van online criminaliteit en offline criminaliteit. Daarbij is onder andere aandacht voor de organisatie van politie-eenheden en van parketten, de kennis en vaardigheden van medewerkers, de manier waarop aangiftebereidheid kan worden vergroot en mogelijkheden om de drempel om aangifte te doen te verlagen. Ook is aandacht voor het werken op grond van intelligence gestuurde instroom van zaken en een bredere inzet van digitale opsporingsmethoden in onderzoeken.

Publiek-private samenwerking

Nauwe publiek-private samenwerking blijft voor de bestrijding van cybercrime essentieel. Noemenswaardig in dit verband is het eerder benoemde project Melissa, het samenwerkingsverband tussen publieke (politie, OM en NCSC) en private cybersecurity partijen om ransomware te bestrijden. De partijen wisselen

[20] Bijvoorbeeld via NoMoreRansom (Home | The No More Ransom Project)
[21] Double-Extortion Ransomware: A Study of Cybercriminal Profit, Effort, and Risk, Tom Meurs (universiteit Twente)

structureel informatie over ransomware met elkaar uit en signaleren trends en ontwikkelingen. Gezamenlijk kan hierdoor een beter beeld van de problematiek van ransomware worden verkregen van waaruit (preventieve) maatregelen en interventies voortkomen. Zo bleek uit een gezamenlijke analyse binnen project Melissa dat een ransomware-groepering misbruik had gemaakt van een bepaalde kwetsbaarheid. Het scannen op kwetsbare servers en het informeren van potentiële slachtoffers hielp de mogelijke impact in Nederland en wereldwijd te verminderen. Vanuit het samenwerkingsverband wordt bijgedragen aan diverse lopende onderzoeken,[22] en binnenkort verschijnt een publicatie met handelingsperspectief over secundair slachtofferschap. Steeds meer partijen tonen interesse om deel te nemen aan het samenwerkingsverband. Een recente evaluatie van het project door de universiteit Leiden laat zien dat de focus van het samenwerkingsverband, de strenge voorwaarden waaronder partijen kunnen deelnemen, de kennis en het onderlinge vertrouwen van de deelnemers hebben bijgedragen aan het succes.[23] De evaluatie biedt handvatten voor het opzetten en verder verbeteren van publiek-private samenwerking. De ervaringen uit project Melissa worden meegenomen in de ontwikkeling van Cyclotron, een programma onder de NLCS waarin via publiek-private samenwerking wordt beoogd de cyberweerbaarheid van alle organisaties te verhogen door publiek-private samenwerking te verbeteren.[24]

Sancties

De inzet van sancties wordt door het OM en de politie gezien als aanvullend verstoringsmiddel. Eind juni 2024 zijn voor het eerst cybercriminelen op de Europese sanctielijst geplaatst. Als gevolg van deze sancties zijn de tegoeden in de EU van deze individuen bevroren, is inreizen naar de EU niet meer mogelijk, en wordt het aangaan van transacties met hen verboden. Dat houdt in dat samenwerken en (indirect) zakendoen met deze cybercriminelen voor burgers en bedrijven in de EU verboden is, bijvoorbeeld bij het

---

[22] Zoals Operation Endgame en het vervolg daarop, zie: Internationale politiediensten pakken met Operation Endgame door in bestrijding ransomware | politie.nl

[23] Samenwerken tegen Ransomware Evaluatie Melissa by Universiteit Leiden - Issuu

[24] Programma Cyclotron | Nationaal Coördinator Terrorismebestrijding en Veiligheid

aanbieden van hostingdiensten.[25] De plaatsing op de sanctielijst kwam tot stand op voordracht van Nederland en door intensieve samenwerking tussen de politie, het OM en de ministeries van Buitenlandse Zaken en Justitie en Veiligheid. Voor het instellen van EU-sancties is steun van alle EU-lidstaten een voorwaarde. Recentelijk zijn de sancties verlengd.[26]

Financiële stromen

Ook in het geval van het aanpakken van cybercrime is het van belang om de financiële stromen richting criminelen in kaart te brengen, dit geldt ook voor cryptovaluta. Het afpakken of bevriezen van cryptovaluta blijkt nog erg lastig: een verdachte moet verbonden kunnen worden aan een specifieke rekening met cryptovaluta en voor bevriezing is vaak internationale rechtshulp nodig.

Sinds december 2024 is de EU Transfer of Funds verordening van kracht. Deze verordening zorgt ervoor dat crypto-activadienstverleners in de EU de identiteit van een houder van een *cryptowallet* (rekening) moeten kennen en informatie over de initiator en de begunstigde van een crypto-transactie moeten meesturen. Ondanks dat in internationaal verband het belang van het kennen van de identiteit achter een *cyptowallet* is onderkend[27] is deze aanbeveling nog niet wereldwijd geïmplementeerd.[28]

In de praktijk blijken crypto-dienstverleners regelmatig gevestigd in landen waarmee geen of moeizame rechtshulp mogelijk is, en wordt er vaak niet of nauwelijks gereageerd op verzoeken. Daarnaast bemoeilijkt het gebruik van crypto-mixingdiensten de attributie van transacties aanzienlijk en is specialistische kennis vereist om hier effectief op te kunnen acteren.

---

[25] EU sanctioneert voor het eerst cybercriminele kopstukken | Nieuwsbericht | Rijksoverheid.nl
[26] Cyber-attacks: Council extends sanctions and legal framework - Consilium
[27] www.fatf-gafi.org/en/topics/virtual-assets.html
[28] Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs

In een samenwerking tussen onder andere de politie, de Fiscale inlichtingen- en opsporingsdienst (FIOD) en de Verenigde Staten zijn het afgelopen jaar twee criminele crypto-exchange-diensten aangepakt en is een vermogen van 7 miljoen euro aan cryptovaluta afgepakt. Deze actie resulteerde bovendien in een sterker begrip van de financiële aspecten van het cybercriminele ecosysteem. Cryptovaluta en de financiële aspecten van cybercrime worden in toenemende mate een vast onderdeel in onderzoeken. Daarbij moet worden opgemerkt dat expertise op dit vlak schaars is.

In het kader van de internationale aanpak van het gebruik van cryptovaluta bij criminaliteit wordt momenteel binnen het kader van het Cybercrimeverdrag van de Raad van Europa (Verdrag van Boedapest) onderzocht op welke manier de instrumenten van dit Cybercrimeverdrag in kunnen worden gezet. De resultaten van deze inventarisatie worden eind 2025 verwacht.

Slachtoffernotificatie

Tenslotte is het actief informeren en ondersteunen van slachtoffers door het bieden van handelingsperspectief cruciaal om schade te beperken en herhaald slachtofferschap te voorkomen. Dit geldt voor slachtoffers op individueel niveau en zorgt er bij sommige vormen van criminaliteit (bijvoorbeeld botnets) voor dat de criminele tools en netwerken minder effectief zijn. Slachtoffernotificatie dient daarmee ook de nationale veiligheid, omdat de slagkracht van criminele netwerken wordt verminderd bij de-installatie van malware.[29]

Het is belangrijk dat iedereen die in Nederland (mogelijk) slachtoffer of doelwit is van een cyberaanval gewaarschuwd kan worden. Hiermee zijn organisaties, publiek en privaat, vitaal en niet-vitaal en groot en klein, en burgers beter in staat acties te ondernemen en daarmee hun digitale weerbaarheid te vergroten. Binnen het cyberweerbaarheidsnetwerk (CWN) zorgt het NCSC er, samen met partners, voor dat iedereen genotificeerd kan worden. Hiermee wordt een belangrijke stap gezet om de opgave voor een digitaal veilig Nederland te realiseren.

[29] NCTV, Cybersecuritybeeld Nederland 2024.

Daarnaast heeft de politie via het EU International Security Fund (ISF) een bijdrage ontvangen om de komende twee jaar tot een internationaal systeem ter preventie van secundair slachtofferschap van cybercrime te komen, onder andere door bestaande systemen van Check je hack[30] en No More Leaks[31] die door de politie zijn ingericht verder te ontwikkelen, zodat wereldwijd mensen kunnen worden gewaarschuwd voor diefstal en handel van hun gebruikersgegevens.

Successen

De politie en het OM boeken ondanks de toenemende complexiteit successen in de brede aanpak van cybercrime. In een gezamenlijke actie, bekend als Operation Endgame,[32] voerden Europese politiediensten in 2024, gecoördineerd door Eurojust en Europol, een grote internationale politie-operatie tegen ransomware-netwerken uit. In verschillende landen werden botnets die een sleutelrol speelden in de wereldwijde cybercriminaliteit, ontmanteld. Criminele organisaties verspreidden al jaren malware via honderden miljoenen phishingmails en vormden zo een omvangrijk en complex netwerk waarmee computersystemen van slachtoffers misbruikt konden worden. Naar schatting loopt de financiële schade die deze criminelen aangericht hebben bij bedrijven en overheidsinstellingen in de honderden miljoenen euro’s. Miljoenen particulieren zijn ook slachtoffer geworden, omdat hun systemen waren geïnfecteerd en ze onderdeel werden van deze botnets. De gezamenlijke actie resulteerde in het uitschakelen van meer dan 100 servers, de arrestatie van vier hoofdverdachten en de plaatsing van twee cybercrimelen op de EU-sanctielijst, zoals hiervoor vermeld. Het vervolg van het onderzoek richtte zich op de gebruikers van de botnets die eveneens strafbaar zijn. Dit resulteerde onder andere in een arrestatie in Nederland van een man die ervan verdacht wordt via Telegram malware te hebben aangekocht. In een vervolg van Operation Endgame zijn in mei 2025 opnieuw verschillende botnets en infostealers uit de lucht gehaald, zijn wereldwijd 300 servers uitgeschakeld en is 3,5 miljoen euro aan cryptovaluta in beslag genomen. Tevens zijn nieuwe verdachten op de Europol Most-wanted lijst geplaatst.[33]

---

[30] Check je hack | politie.nl
[31] No More Leaks | politie.nl
[32] https://operation-endgame.com
[33] https://eumostwanted.eu

In een andere internationaal gecoördineerde actie van opsporingsdiensten, bekend als Operation Magnus, is de technische infrastructuur van *infostealers* ontmanteld. Een *infostealer* is een vorm van malware die specifiek is ontworpen om gevoelige gegevens te stelen van de computer van nietsvermoedende slachtoffers. De buitgemaakte gegevens kunnen door de criminelen verkocht worden of gebruikt worden voor onder andere identiteitsdiefstal, financiële fraude en ransomware. In het onderzoek zijn duizenden afnemers van de *infostealers* in beeld gekomen die op hun beurt zelfstandig slachtoffers hebben gemaakt. Op basis van het veilig gestelde klantenbestand vindt vervolgonderzoek naar de afnemers van deze dienst plaats.

Met behulp van de internationale opsporingsdiensten is bewerkstelligd dat meerdere Telegram-accounts waar de *infostealers* werden aangeboden uit de lucht zijn gehaald waarmee de verkoop van deze *infostealers* is platgelegd. Daarnaast is de politie met gebruikmaking van de hackbevoegdheid met een technisch hoogstandje in staat geweest de infrastructuur van de beide *infostealers* offline te halen. Hierdoor functioneert de malware niet meer en is het niet meer mogelijk om hiermee nieuwe data van geïnfecteerde slachtoffers te stelen.

iv. Verkenning aanpak bad hosting

De Nederlandse hostingsector is groot en divers. Het heeft een goede naam door de snelle internetverbindingen in Nederland, de hoeveelheid datacenters en servers en de goede service die geleverd wordt. Naast de vele voordelen die dat biedt voor legale activiteiten betekent dat helaas ook dat criminaliteit ermee kan worden gefaciliteerd. Dit wordt door de hostingsector ook erkend en in het kader van zelfregulering zijn afspraken gemaakt om de sector zo schoon mogelijk te krijgen en te houden. Maar net als in de offlinewereld zijn er ook partijen die zich van dergelijke afspraken weinig aantrekken: er zijn malafide hostingbedrijven die bewust criminaliteit faciliteren (bulletproof hosting) dan wel onwetende hostingbedrijven die zeer weinig maatregelen nemen ter preventie van criminaliteit (bad hosting).

Hostingproviders weten vaak niet precies welke klanten hun diensten misbruiken voor criminele activiteiten. Bovendien kunnen klanten de dienstverlening doorverkopen. Er is dan sprake van

zogenaamde *resellers*. Dit doorverkopen is niet verboden. Dit kan de opsporing en vervolging echter wel extra complex maken; een klant kan immers doorverkopen aan een klant, die het weer verder kan verkopen aan een andere klant en zo verder. Door vergevorderde reseller-constructies kunnen klanten gemakkelijk anoniem blijven en/of zich in het buitenland bevinden of zich naar het buitenland verplaatsen.

Tijdens het commissiedebat Cybercrime van 24 oktober 2024 heb ik toegezegd om verder te verkennen wat er aan de problematiek van bad hosting en resellers kan worden gedaan. Deze verkenning heeft plaatsgevonden langs zes sporen: wet- en regelgeving, internationale samenwerking, reseller-problematiek, financiële opsporing, zelfregulering en overzicht van de sector. Voor deze verkenning is met verschillende partijen gesproken, zowel publiek als privaat. De verschillende activiteiten die in de verkenning zijn benoemd staan verder beschreven in bijlage 2 bij deze brief. Uit de verkenning vloeien een aantal kansrijke mogelijke oplossingen die ik het komende jaar graag verder uit wil werken. Hier zal uw Kamer in 2026 verder over worden geïnformeerd. Oplossingsrichtingen die kansrijk worden geacht en in de komende tijd concreet zullen worden uitgewerkt staan hieronder kort beschreven.

‘Ken je klant’-beleid, ook wel ‘Know-your-customer’-beleid of KYC-beleid genoemd, wordt als een van de oplossingen gezien om bulletproof en bad hosting beter aan te kunnen pakken. Het principe is al terug te vinden in de reeds lang bestaande Gedragscode Abusebestrijding. Partijen in de hostingsector die hierbij zijn aangesloten voeren dit al grotendeels uit. Het kabinet wil echter verder onderzoeken waar Know your customer-beleid wettelijk verankerd zou kunnen worden; bijvoorbeeld in lijn met de Wet ter voorkoming van witwassen en financieren van terrorisme (H2, clientonderzoek) of de Wet economische delicten.

Bad hosting en de reseller-problematiek is een grensoverschrijdend probleem; klanten van Nederlandse hostingdiensten kunnen immers overal vandaan komen. Daarom wil het kabinet inzetten op meer Europese en internationale samenwerking. Voorbeelden van concrete acties hierop zijn het inzetten op Europees niveau van de Gedragscode Abusebestrijding, het verder stimuleren van het Cleannetworksproject en dit op Europees niveau onder de aandacht brengen. Dit stimuleert dat de sector binnen de gehele EU aan dezelfde voorwaarden voldoet. Dat helpt bij het uitwisselen van

informatie in opsporingsonderzoeken en voorkomt oneerlijke concurrentie voor de Nederlandse sector.

Om beter zicht te krijgen op de hostingsector en de verschillende type diensten die hier onder vallen zal het kabinet bezien of het mogelijk is om de codes van de CBS Standaard Bedrijfsindeling (SBI codes) voor de sector aan te passen. Hierdoor wordt het makkelijker om een type dienst en/of activiteit te classificeren, wat het ook eenvoudiger maakt voor handhavende en toezichthoudende organisaties om zicht te hebben op de verantwoordelijkheid en aansprakelijkheid van een partij.

Publiceren jaarlijkse resellerbrief (motie Michon-Derkzen)
Jaarlijks verstuurt de politie een brief aan Nederlandse hostingproviders waarin zij adviseert een eventuele overeenkomst met bepaalde resellers te herzien. De lijst van resellers wordt opgesteld op basis van openbare bronnen waaruit af te leiden valt dat de resellers zichzelf afficheren als criminele dienstverleners. Er is gebleken dat hostingbedrijven actie ondernemen naar aanleiding van de brief en dit is daarmee een efficiënt middel gebleken.[34]

Door de Tweede Kamer is met de motie Michon-Derkzen opgeroepen om te onderzoeken of het wenselijk is dat de jaarlijkse brief van de politie openbaar wordt gemaakt.[35] Er zijn hostingbedrijven die zich niet bewust zijn van malafide klanten maar wel actie ondernemen. Daarom kan het openbaar maken van de lijst een negatief beeld geven van partijen die het wel goed doen en wordt daarmee het risico op onterechte reputatieschade van deze partijen vergroot. Dat laat onverlet dat men binnen de sector zelf de brief openbaar kan maken om positieve reacties erop juist te benadrukken. In het kader van het versterken van de internationale samenwerking zal er worden gekeken of de politie de lijst kan delen met andere opsporingsdiensten zodat ook zij een beter beeld hebben van de reseller-problematiek.

v. Veiligheidsagenda 2023-2026 - resultaten cybercrime
Bij de bestrijding van cybercrime zijn ten aanzien van de doelstellingen uit de Veiligheidsagenda in 2024 mooie resultaten gehaald. De doelstellingen zien op reguliere onderzoeken uitgevoerd op regionaal niveau, fenomeenonderzoeken die gericht zijn op de brede bestrijding van eenheidsoverstijgende cybercrime-

[34] CBS, Online Veiligheid en Criminaliteit 2024 (https://www.cbs.nl/nl-nl/longread/rapportages/2025/onlineveiligheid-en-criminaliteit-2024/7-online-criminaliteit-totaal)
[35] Kamerstukken II, 2024-2025, 26643, nr. 1250.

fenomenen en dadergroepen, en onderzoeken van het Team High Tech Crime (zie in figuur 1 de doelstellingen 2023- 2026).

In 2024 is ten aanzien van reguliere onderzoeken het streefaantal van 350 gehaald: er zijn 351 verdachten naar het OM ingezonden. In 6 procent van de reguliere cybercrimezaken was sprake van een alternatieve of aanvullende interventie. 17 procent van de reguliere cybercrimezaken is uit een onderzoek naar een crimineel samenwerkingsverband voortgekomen. Ook voor de complexere onderzoeken zijn de doelstellingen behaald. Aan het einde van 2024 waren 46 fenomeenonderzoeken en 20 high tech crime-onderzoeken tactisch afgerond.

Figuur 1 - Veiligheidsagenda 2023-2026, doelstellingen cybercrime

Afspraken:

	2023	2024	2025	2026
Aantal verdachten van cybercrime regulier	310	350	400	450
Waarvan csv's	10%	10%	20%	20%
Waarvan alternatieve interventies	25%	25%	25%	25%
Aantal fenomeenonderzoeken	41	41	43	45
Waarvan alternatieve interventies	50%	50%	50%	50%
Aantal high tech crime onderzoeken (inclusief alternatieve interventies)	20	20	20	20

Figuur 2 - Veiligheidsagenda 2023-2026, resultaten cybercrime (realisatie 2023, doelstelling 2024, realisatie 2024)

Cybercrime	realisatie 2023	doelstelling 2024	realisatie 2024	Realisatie tov doelstelling 2024
Aantal cybercrime regulier wv alternatieve interventies wv csv	336 36 50	350 88 35	351 22 61	100%

Fenomeenonderzoeken wv alternatieve interventies	36 14	41 20	46 18	112%
Aantal high tech crime onderzoeken	17	20	20	100%

vi. Extra investeringen voor politie en keten

Uw Kamer is in november 2024 geïnformeerd over de investeringen van dit kabinet.[36] Voor de aanpak van cybercrime en gedigitaliseerde criminaliteit wordt een bedrag van 52,6 miljoen euro geïnvesteerd in de politie en de strafrechtketen.

Een effectieve aanpak van cybercrime en gedigitaliseerde criminaliteit vergt een intelligence-gestuurde en datagedreven aanpak op basis van (inter)nationaal inzicht en overzicht. Het kabinet investeert daarom onder andere in landelijke voorzieningen bij de politie voor de aanpak van cybercrime en gedigitaliseerde criminaliteit ten behoeve van de regionale eenheden en de Eenheid Landelijke Opsporing en Interventies (voor onderzoeken van het Team High Tech Crime), en in extra uitvoeringscapaciteit voor de aanpak van gedigitaliseerde criminaliteit in de eenheden. De landelijke voorziening voor cybercrime heeft als doel meer samenhang te brengen in de aanpak, van regionaal tot internationaal. Vanuit de landelijke voorziening worden strategie, intelligence en operationele inzet bijeengebracht. Voor de versterking en doorontwikkeling van de bestrijding van cybercrime zal onder andere worden geïnvesteerd in personeel met specifieke kennis en vaardigheden en een hoger opleidingsniveau.

vii. Versterking van de bevoegdheden in het digitaal domein

Update evaluatie Wet Computercriminaliteit III

In 2022 is het eerste deel van de evaluatie van de Wet Computercriminaliteit III (CCIII) over de uitvoering van de hackbevoegdheid afgerond. In de beleidsreactie van december

[36] Kamerstukken II, 2024-2025, 36600, nr. 32.

2023 is uw Kamer daarover geïnformeerd.[37] Op 4 september 2024 is deze aan de orde geweest in het commissiedebat over Strafrechtelijke onderwerpen (Kamerstuk 29279, nr. 875).

In de brief over de integrale aanpak van cybercrime van 28 juni 2024 is specifiek op het onderdeel toezicht nader ingegaan.[38] Daarin heeft mijn voorganger uw Kamer geïnformeerd over het voornemen dat de Inspectie van Justitie en Veiligheid overgaat op systeemtoezicht op de uitvoering van de hackbevoegdheid door de politie. Om toezicht te kunnen houden is een kwaliteitssysteem bij de politie nodig.. De politie heeft dit het afgelopen jaar in dialoog met de Inspectie ontwikkeld. Het zal in de loop van de tijd worden uitgebreid en aangepast op basis van opgedane ervaring. Het doel is dat het kwaliteitssysteem aansluit bij de operationele behoeften en de uitvoering van systeemtoezicht. De implementatie van het kwaliteitssysteem bij de politie zal rond de zomer beginnen.

Daarnaast is, ter uitvoering van de genoemde beleidsreactie, ook op andere vlakken voortgang geboekt. Voor een deel van de aanpassingen is geen wijziging in wet- en regelgeving nodig. Deze beleidswijzigingen zijn voor een groot deel geïmplementeerd, zoals het afschaffen van het licentiemodel voor binnendringsoftware en het versterken van de interne organisatie van het OM ten behoeve van het toetsingstraject dat doorlopen wordt rond de voorbereiding en de inzet van de bevoegdheid. Voor de uitvoering van de andere aanpassingen is wel wijziging van de wet- en regelgeving noodzakelijk. Deze zijn in voorbereiding. Het gaat om aanpassingen van lagere regelgeving en om aanpassingen die in de wet moeten worden opgenomen. Voor de aanpassingen die geregeld moeten worden in de wet zal worden aangesloten bij het traject dat leidt tot de modernisering van het Wetboek van Strafvordering.

In het tweede deel van de evaluatie worden de overige delen uit de Wet CCIII behandeld. De planning is dat deze evaluatie in het najaar is afgerond.

Toegang tot elektronisch bewijs: implementatie e-evidence

[37] Kamerstukken II, 2023-2024, 34372, nr. 31.
[38] Kamerstukken II, 2023-2024, 26643, nr. 1204.

Ten behoeve van de implementatie van het Europese e-evidence pakket wordt op korte termijn een wetsvoorstel in procedure gebracht ten behoeve van de omzetting van de richtlijn (EU 2023/1544) met voorwaarden en verplichtingen voor digitale dienstverleners. Het gaat hier om registratieverplichtingen voor bedrijven die (elektronische) diensten verlenen zoals omschreven in de definitie van dienstaanbieder in de richtlijn en die daarom over gegevens beschikken die nodig zijn als sporen en bewijs in opsporingsonderzoeken. De richtlijn bevat ook vereisten over wanneer, waar én hoe een dienstverlener kan worden benaderd door justitiële autoriteiten uit een andere EU-lidstaat voor het bewaren en/of verstrekken van digitaal bewijs. De richtlijn is ondersteunend aan de verordening (EU 2023/1543) die de grondslagen en voorwaarden geeft voor het grensoverschrijdend uitvaardigen en handhaven van bevelen voor het bewaren en/of verstrekken van digitaal bewijs. De richtlijn creëert een gelijk speelveld voor alle bedrijven die vallen onder het bereik van de verordening en de richtlijn. Het maakt daarbij niet uit of de bedrijven zijn gevestigd in of buiten de EU. Belangrijk is dat zij hun diensten in de EU – in meer dan één lidstaat – aanbieden. De lidstaten moeten ervoor zorgen dat bedrijven uitvoering geven aan de vereisten van de richtlijn en moeten toezien dat de richtlijn op een consistente en evenredige wijze wordt toegepast. Als centrale autoriteit hiervoor, als toezichthouder, stelt Nederland de Autoriteit Consument en Markt (ACM) aan. De ACM bereidt zich op haar nieuwe taak voor.

Voor de toepassing van de verordening loopt daarnaast een specifiek programma met daarin projecten bij de organisaties die te maken krijgen met de uitvoering van de verordening, zoals het OM, de politie en de Justitiële Informatiedienst (Justid). Zij bereiden de werkprocessen voor, inclusief de inrichting van de organisatie en het creëren van de nodige kennis en vaardigheden. Deze werkprocessen zijn nodig voor het grensoverschrijdend uitvaardigen en handhaven van bevelen voor het bewaren en verstrekken van digitaal bewijs- en bewaringsbevelen en het verstrekken van de gegevens in Nederland. Hiervoor moet een digitale infrastructuur worden ingericht.

Het e-evidence pakket treedt op 18 augustus 2026 in werking. In de verordening zijn belangrijke rollen weggelegd voor justitiële autoriteiten. Ten eerste kunnen zij een verstrekkings- of bewaringsbevel uitvaardigen om gegevens die berusten bij een

provider in een andere EU-lidstaat op te vragen (rol 1). Daarnaast kunnen zij worden genotificeerd over bevelen die zien op verkeersgegevens en op inhoudelijke gegevens om ten aanzien van die bevelen te kunnen beoordelen of daartegen in de verordening weigeringsgronden moeten worden ingeroepen (rol 2). Tot slot zijn zij de autoriteiten die op verzoek van een ander uitvaardigend land een verstrekkingsbevel tenuitvoerleggen als het geadresseerde bedrijf in eerste aanleg niet binnen 10 dagen heeft gereageerd (rol 3). Nederland (JenV) wijst voor rol 1, 2 en 3 het OM aan als justitiële autoriteit, waarbij in rol 1 soms ook actie van een rechter nodig is als degene die bepaalde categorieën van bevelen van een officier van justitie moet bekrachtigen.

Optreden tegen illegale inhoud

Door de leden Ceder en Six Dijkstra is de regering in een motie opgeroepen om zich in te spannen om Telegram nationaal en internationaal aan haar verplichtingen te houden om op te treden tegen illegale inhoud.[39] Graag maak ik van de gelegenheid gebruik om u hier nader over te informeren. De regels voor het monitoren en modereren van online illegale inhoud zijn vastgelegd in de Digitaledienstenverordening. Voor Nederland is de Autoriteit Consument en Markt (ACM) hiervoor de toezichthouder en handhaver als Digitaledienstencoördinator; haar taken kan zij sinds de inwerkingtreding van de uitvoeringswet Digitaledienstenverordening (2025) volledig uitvoeren. Het toezicht op, en de handhaving ten aanzien van Telegram zijn belegd bij de Belgische Digitaledienstencoördinator (Belgisch Instituut voor Postdiensten en Telecommunicatie, BIPT), omdat Telegram in België haar wettelijke vertegenwoordiging heeft. Telegram lijkt tegenwoordig te handelen naar de wettelijke verplichting op te treden tegen illegale inhoud. Een voorbeeld hiervan is de casus van bangalijsten op Telegram. Nederlandse gedupeerden hebben onder aanvoering van Offlimits een handhavingsverzoek ingediend om bangalijsten offline te halen van Telegram. Telegram gaf volgens de melders geen gehoor aan hun meldingen. De ACM heeft in de communicatie tussen Offlimits en de Belgische Digitaledienstencoordinator een bemiddelende rol gespeeld, geïnitieerd binnen de Europese Digitaledienstenraad. Telegram heeft de betreffende bangalijsten inmiddels verwijderd. Bovendien heeft Telegram toegezegd dat Offlimits via een apart kanaal de

[39] Kamerstukken II, 2024-2025, 36 600 VII, nr. 76.

mogelijkheid krijgt meldingen door te geven, zodat Telegram snel illegale content offline kan halen.

viii. Internationale trajecten

VN Cybercrime verdrag

In december 2024 is een nieuw VN-verdrag op het gebied van cybercrime overeengekomen. Het verdrag biedt mogelijkheden voor samenwerking op het gebied van cybercrime met landen die niet zijn aangesloten bij Cybercrimeverdrag van de Raad van Europa (Verdrag van Boedapest). Momenteel wordt door de Europese Commissie bezien wat de mogelijke juridische gevolgen zijn van ratificatie van dit verdrag ten opzichte van bestaande wet- en regelgeving. Deze analyse zal tevens worden afgezet tegen de bestaande Nederlandse wet- en regelgeving omtrent cybercrime en de huidige regelingen voor internationale samenwerking voor het verkrijgen van elektronisch bewijs. Aan de hand daarvan zal het kabinet haar positie bepalen ten opzichte van mogelijke ratificatie.

EU-VS onderhandelingen elektronisch bewijs

Veel van de grote technologiebedrijven die elektronisch bewijs hebben dat van belang is voor de opsporing, zijn Amerikaans. Door verplichte vestiging of vertegenwoordiging van dergelijke bedrijven in de EU en de verplichting om gevolg te geven aan vorderingen voor elektronisch bewijs, maken de recente EU-e-evidence regels het gemakkelijker om van deze bedrijven elektronisch bewijs te verkrijgen. Echter, voor situaties waarbij er sprake is van botsende regelgeving tussen het Europese en het Amerikaanse recht (bijvoorbeeld op het terrein van bescherming van persoonsgegevens), kan een specifieke overeenkomst tussen de EU en de VS juridische zekerheid bieden. Dat is niet alleen voor de opsporing, maar ook voor de betrokken bedrijven van belang. De Europese Commissie voert onderhandelingen voor een dergelijke overeenkomst in nauw overleg met de Raad. De laatste onderhandelingsronde vond plaats in november 2024. Sinds het aantreden van de nieuwe Amerikaanse regering is er nog geen nieuwe onderhandelingsronde gepland.

Counter Ransomware Initiative

Het Counter Ransomware Initiative is een samenwerkingsverband van meer dan 70 landen en organisaties om kennis van en ervaring met de bestrijding van ransomware uit te wisselen en te bezien op welke wijze de internationale samenwerking tegen ransomware kan worden versterkt.[40] Tijdens de jaarlijkse bijeenkomst in oktober 2024 is een *guidance* aangenomen die organisaties bij een ransomware-aanval handvatten biedt, zodat betaling van losgeld zoveel mogelijk wordt voorkomen en ransomware-aanvallen bij autoriteiten worden gemeld. Het Nederlands Verbond van Verzekeraars is mede-ondertekenaar van de *guidance*.[41]

Tot slot

Eerdere investeringen en de inzet van vele partijen hebben geleid tot meer kennis en capaciteit, vele initiatieven die burgers en bedrijven beschermen en ondersteunen, en een versterking van de aanpak van cybercrime. De aanvullende maatregelen, waaronder structurele investeringen, versterken de aanpak verder. Tegelijkertijd blijft de criminaliteit in het digitale domein zich ontwikkelen en blijft opsporing complex. De aandacht voor deze uitdagingen blijft daarom ook in de komende jaren onverminderd noodzakelijk.

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

[40] About Us | International Counter Ransomware Initiative
[41] Nieuwe richtlijn ransomware