26643 Informatie- en communicatietechnologie (ICT)

29911 Bestrijding georganiseerde criminaliteit

Nr. 1555 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 september 2026

Cybercriminaliteit wordt onvoorspelbaarder, geavanceerder en complexer. Zowel publieke als private organisaties zijn steeds vaker doelwit en een toenemend aantal incidenten, zoals hacks met datadiefstal, leiden tot massaal slachtofferschap van burgers en organisaties. Zelfs wanneer burgers hun apparaten goed beveiligen en alle beschikbare updates en beveiligingsmaatregelen nemen, kunnen zij slachtoffer worden van een hack bij een organisatie waar hun gegevens zijn opgeslagen. Gebruik van artificiële intelligentie (AI) door cybercriminelen vergroot het risico op slachtofferschap van cybercriminaliteit.

Cybercriminaliteit is een blijvende en groeiende dreiging voor onze samenleving, economie en nationale veiligheid. Om deze dreiging het hoofd te bieden voert Nederland een actief beleid van preventie, opsporing, verstoring en vervolging. Dit blijft in een snel veranderend digitaal landschap uitdagend. Het is dan ook van belang te blijven innoveren en kennis en expertise te ontwikkelen om effectief op te treden tegen cybercriminelen en de digitale infrastructuur die zij gebruiken.

Met deze brief informeer ik uw Kamer over de voortgang van de integrale aanpak van cybercrime en versterking van bevoegdheden in het digitale domein.

De volgende onderwerpen komen aan de orde:

i. Het beeld en de ontwikkeling van cybercriminaliteit;
ii. Opsporen, verstoren en vervolgen;
iii. Preventie;
iv. Versterking van de bevoegdheden in het digitale domein;

Als bijlage bij deze brief vindt u het Cybercrimebeeld 2026 van de politie en het Openbaar Ministerie (OM).

i. Beeld en ontwikkeling van cybercriminaliteit

In 2025 gaf volgens het Centraal Bureau van de Statistiek (CBS) 17 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.[1] In 6 procent van de gevallen was sprake van hacken (computervredebreuk).[2] Ruim een vijfde van de slachtoffers van online criminaliteit gaf aan dat het online delict heeft geleid tot emotionele, psychische en/of financiële problemen. Uit onderzoek blijkt dat de impact van online criminaliteit in veel gevallen gelijk is aan, en soms groter is dan die van traditionele (offline) criminaliteit.[3]

Ook de economische impact van cybercrime is aanzienlijk. Cyberaanvallen kunnen bedrijfsprocessen stilleggen, gegevens vernietigen of openbaar maken en daarmee tot directe schade leiden. Het CBS rapporteert dat in 2024 4 procent van de bedrijven te maken kreeg met een cyberincident door een aanval van buitenaf, bij 1 procent ging dit met kosten gepaard.[4]

Het Cybersecuritybeeld Nederland 2025 laat zien dat de digitale dreiging tegen Nederland onverminderd hoog blijft en verder is verbreed. Het dreigingslandschap wordt gekenmerkt door een grote diversiteit aan actoren, waarbij de grenzen tussen cybercriminelen, statelijke actoren en hacktivisten steeds verder vervagen.[5]

Het Cybercrimebeeld 2026 sluit daarop aan en laat vanuit de dagelijkse opsporingspraktijk van politie en Openbaar Ministerie zien hoe deze ontwikkelingen zich manifesteren in de criminaliteit.[6] De belangrijkste inzichten uit het Cybercrimebeeld zijn:

- Het daderlandschap wordt steeds diverser en diffuser. De grenzen tussen financieel gemotiveerde cybercriminelen, georganiseerde criminaliteit, hacktivisten en statelijke actoren vervagen. Cybercriminaliteit wordt steeds vaker ingezet als instrument voor hybride dreigingen, terwijl tegelijkertijd een nieuwe generatie jonge westerse cybercriminelen opkomt die zich beweegt in online netwerken zoals de Hacker Com[7].
- Achter vrijwel iedere cyberaanval schuilt een professionele internationale toeleveringsketen. Gespecialiseerde aanbieders van digitale infrastructuur,

---

[1] CBS Veiligheidsmonitor 2025. Dit is hetzelfde percentage als in 2021. Vormen van online criminaliteit: online oplichting en fraude, hacken, online bedreiging en intimidatie, overige online delicten.
[2] Dit is een stijging ten opzichte van hetgeen in 2024 is aangegeven (4 procent). Maar: cijfers uit 2024 betreffen vraagstelling CBS online monitor en huidige cijfers zijn afkomstig uit de cijfers CBS Veiligheidsmonitor die een net iets andere vraagstelling heeft. De cijfers zijn dus niet helemaal naast elkaar te leggen. Daarnaast doen burgers en bedrijven niet altijd aangifte of melden cyberincidenten niet bij de bevoegde instanties. Hierdoor blijft een deel van cybercriminaliteit buiten de officiële statistieken.
[3] Jildau Borwell, 'Unravelling the impact of cybercrime – Understanding victim experiences and implications for police practice'.
[4] CSB Cybersecuritymonitor 2025.
[5] Cybersecuritybeeld Nederland 2025 | Nationaal Coördinator Terrorismebestrijding en Veiligheid
[6] Actie III.1.2.5 van de Nederlandse Cybersecurity Strategie (NLCS) + **https://fts.politie.nl/cybercrimebeeld/2026/** Cyberbeeld Nederland 2026
[7] Een dynamisch online netwerk van individuen die onder andere cryptovaluta stelen en grote organisaties afpersen met data-diefstal.

toegang tot slachtoffernetwerken, malware, AI en andere criminele diensten maken cybercriminaliteit toegankelijker, winstgevender en meer schaalbaar.
- Cryptovaluta vormen de financiële ruggengraat van de cybercriminele economie. Zij maken het mogelijk opbrengsten van cybercriminaliteit wereldwijd te verplaatsen, wit te wassen en opnieuw te investeren in nieuwe aanvallen.

Het Cybercrimebeeld maakt zichtbaar dat cybercriminaliteit zich ontwikkelt tot een internationaal ecosysteem van verweven dadernetwerken, criminele dienstverleners en mondiale geldstromen.

Ook Europol signaleert in het Internet Organised Crime Threat Assessment (IOCTA) 2026 dat in toenemende mate gebruik wordt gemaakt van 'cybercrime-as-a-service' en signaleert een centrale en groeiende rol van facilitatoren, zoals aanbieders van bulletproof hosting, proxydiensten, cryptodiensten en zogenoemde 'initial access brokers'. Cybercrime wordt daardoor steeds professioneler en laagdrempeliger; ook minder geavanceerde actoren kunnen op grotere schaal en met hogere impact aanvallen uitvoeren.

Ook info stealer-malware speelt een belangrijke faciliterende rol. Hiermee wordt grootschalig digitale toegang mogelijk gemaakt en verhandeld voor uiteenlopende vormen van criminaliteit, waaronder ransomware, (online) fraude en identiteitsmisbruik.[8]

Europol constateert verder dat cybercriminelen steeds vaker gebruikmaken van generatieve AI. Ook de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) stelt in haar jaarverslag dat steeds meer aanvallers gebruikmaken van automatisering om cyberaanvallen uit te voeren.[9] AI wordt onder meer ingezet voor het automatiseren en opschalen van phishingcampagnes, het genereren van geloofwaardige frauduleuze communicatie en het vervaardigen van deepfake-audio- en videomateriaal. De ontwikkeling van de geavanceerde AI-modellen maakt het mogelijk om op schaal kwetsbaarheden in software te vinden en aanvallen uit te voeren. Er bestaat een kans dat de AI-modellen in de toekomst in staat zijn om volledig autonoom cyberaanvallen uit te voeren.[10] Aan de andere kant kan AI ook worden gebruikt voor digitale verdediging; bijvoorbeeld door het patchen, monitoren, detecteren en ook de respons geautomatiseerd te laten verlopen.

De Autoriteit Persoonsgegevens (AP) waarschuwt dat phishing- en oplichtingsberichten sneller, grootschaliger en moeilijker te detecteren zijn als cybercriminelen AI gebruiken. De AP constateert in haar rapportage datalekken 2025 dat het aantal datalekmeldingen als gevolg van cyberaanvallen verder is toegenomen.[11] Bovendien is het aantal cyberaanvallen waarbij accounts zijn overgenomen (account take-over) zorgelijk gestegen. Hierbij krijgt een crimineel

---

[8] IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime - Internet Organised Crime Threat Assessment (IOCTA) 2026 | Europol
[9] AIVD Jaarverslag 2025
[10] Met *agentic* AI kunnen criminelen delen van het aanvalsproces in een keten automatiseren. AI *agents* voeren in verschillende onderdelen van een aanval zelfstandig uit. *Agents* worden op dit moment nog onder menselijke regie ingezet.
[11] Rapportage datalekken 2025 | Autoriteit Persoonsgegevens

toegang tot een account, bijvoorbeeld een mailbox. Zo'n take-over komt bijna altijd door phishing. Het AP ziet dit als een populaire manier voor criminelen om gegevens buit te maken en als startpunt voor grotere aanvallen.[12]

Waar cybercriminelen voorheen primair gericht waren op het versleutelen van systemen, wordt onder andere door de politie en Europol een verschuiving gezien richting hacking, datadiefstal en afpersing op basis van buitgemaakte gegevens (hack-and-leak). Het getroffen bedrijf wordt vervolgens afgeperst met de eis om losgeld ('ransom') in cryptovaluta te betalen, in ruil voor het niet publiceren of verwijderen van de gestolen klantgegevens. Uit politieonderzoeken blijkt dat ook wanneer losgeld wordt betaald, geen garantie bestaat dat gestolen gegevens daadwerkelijk worden verwijderd, niet worden doorverkocht of opnieuw openbaar worden gemaakt. Dikwijls wordt gestolen data alsnog door de criminelen doorverkocht. Het stelen van gegevens is een zorgelijke ontwikkeling omdat dit vervolgcriminaliteit, zoals oplichting en verder misbruik mogelijk maakt. Sinds 2025 rekent de AP deze werkwijze ook als ransomware-aanvallen. In 2025 zag de AP 136 ransomware-aanvallen, in 2024 waren dat er 127.[13]

ii. Opsporen, verstoren en vervolgen

Vanuit het inzicht dat de brede bestrijding van cybercriminaliteit en complexe gedigitaliseerde criminaliteit een samenhangende aanpak vereist en het feit dat cybercrime kan resulteren in verschillende vormen van gedigitaliseerde vervolgcriminaliteit, waaronder (online) fraude, is door de politie een nieuwe visie en strategie online criminaliteit 2026-2030 ontwikkeld.

Binnen het OM vindt een vergelijkbare ontwikkeling plaats, waarbij de aanpak van online criminaliteit steeds verder wordt versterkt en verankerd in de organisatie. Online criminaliteit is de overkoepelende term die zowel cybercrime als gedigitaliseerde criminaliteit omvat[14]. In de verdere ontwikkeling van de strijd tegen online criminaliteit trekken de politie en het OM vanuit eigen taken en verantwoordelijkheden samen op.

Bestrijding van online criminaliteit is complex. Een goede informatiepositie is nodig. Om inzichten in netwerken en patronen te vergroten is het voor de opsporing cruciaal om datagedreven te werken zodat opsporingscapaciteit gericht kan worden ingezet. Met de investeringen die de overheid de afgelopen jaren heeft gedaan om de aanpak van cybercrime en gedigitaliseerde criminaliteit te versterken[15] wordt een landelijke voorziening voor cybercrime en een landelijke voorziening voor gedigitaliseerde criminaliteit ingericht om een zo effectief mogelijke en samenhangende aanpak te faciliteren.

Hoewel cybercrime en gedigitaliseerde criminaliteit met elkaar verbonden zijn, verschillen zij ten aanzien van de modus operandi en de wijze waarop zij effectief bestreden kunnen worden. Dit vraagt enerzijds om specifieke accenten, expertise

---

[12] 1742 in 2025 ten opzichte van 607 in 2024.
[13] Rapportage datalekken 2025 | Autoriteit Persoonsgegevens
[14] Een brief over de voortgang van de integrale aanpak online fraude heeft uw Kamer op 3 juli 2026 ontvangen. Derde voortgangsrapportage Integrale Aanpak Online Fraude | Tweede Kamer der Staten-Generaal, Kamerstukken II, 2025/26, 29911, nr. 511.
[15] Kamerstukken II, 2024-2025, 36600 VI nr. 32.

en interventies en anderzijds om een brede versterking van kennis en expertise op het gebied van online criminaliteit.

Het blijft van belang dat opsporingsmethoden aansluiten op veranderende en complexe dreigingen. Dit vraagt bij de politie en het OM om voortdurende ontwikkeling van kennis en expertise (bijvoorbeeld op het terrein van AI en cryptovaluta) en zowel een hoge mate van specialisatie om de (technologische) voorsprong van cybercriminelen te verkleinen, als kennisverbetering in brede zin, zodat een breder fundament van kennis in de organisaties geborgd is.

Zoals aangegeven in de beleidsbrief ben ik voornemens om verder te investeren in de politie voor de bestrijding van online criminaliteit.[16]

[16] Kamerstukken II, 2025/26, 36800 VI nr 142.

Veiligheidsagenda

In het Jaarverslag 2025 is reeds over de resultaten ten aanzien van de doelstellingen in de Veiligheidsagenda gerapporteerd.[17] Voor de volledigheid worden de resultaten voor cybercrime hier herhaald.

Cybercrime	Realisatie 2023	Realisatie 2024	Norm 2025	Realisatie 2025	Realisatie '25 tov norm '25
Aantal verdachten cybercrime regulier	336	351	400	370	93%
- Waarvan criminele samenwerkingsverbanden	50	61	80	57	
- Waarvan alternatieve of aanvullende interventies	36	22	100	44	
Aantal fenomeenonderzoeken	36	46	43	29	67%
- Waarvan alternatieve of aanvullende interventies	14	18	22	4	
Aantal high tech crime onderzoeken	17	20	20	20	100%

De opsporing van cybercrime stabiliseert op het niveau van 2024: de beoogde groei naar 400 verdachten in 2025 is met een realisatie van 370 niet gehaald. In 12% van de reguliere zaken is in 2025 gekozen voor een alternatieve of aanvullende interventie. Daarnaast kent 15% van deze zaken zijn oorsprong in onderzoek naar een crimineel samenwerkingsverband. In 2025 zijn 29 fenomeenonderzoeken en 20 hightechcrime-onderzoeken afgerond.

De achterblijvende resultaten hangen samen met een trend die al langer zichtbaar is: cybercrimezaken worden omvangrijker en technisch complexer, wat de doorlooptijden verlengt. Die toegenomen complexiteit manifesteert zich zowel in de reguliere onderzoeken als in de fenomeen- en hightech onderzoeken. Tegelijkertijd neemt in de fenomeen- en hightech-onderzoeken de afhankelijkheid van internationale rechtshulp en afstemming met buitenlandse partners verder toe, wat extra tijd en capaciteit vergt. Daarbij kwamen in 2025 enkele impactvolle hacks aan de orde die, vanwege hun urgentie en brede effecten op burgers en op de maatschappij als geheel, in overleg met het gezag hebben geleid tot herprioritering en aanpassing van de capaciteitsinzet binnen de cybercrimeteams.

Cybercrime, als onderdeel van het overkoepelende thema online criminaliteit, is ook in de nieuwe Veiligheidsagenda 2027-2030 als thema opgenomen. In het najaar wordt uw Kamer geïnformeerd over de nieuwe Veiligheidsagenda.

[17] Jaarverslag en slotwet van het Ministerie van Justitie en Veiligheid (VI) 2025

Brede bestrijding cybercrime

De politie en het OM werken samen aan de brede bestrijding van cybercrime. De focus ligt op de identificatie en vervolging van verdachten (“aanhouden, tenzij”), en wordt aangevuld met het duurzaam verstoren van (high tech) cybercriminele netwerken en criminele geld/cryptostromen, het notificeren van slachtoffers en de preventie van cybercrime, vaak in samenwerking met publieke en private partners. Het uitgangspunt blijft dat crimineel handelen niet mag lonen.

Grote internationale acties waarbij wordt ingezet op brede bestrijding laten zien dat het lukt om cybercriminelen een belangrijke slag toe te brengen. Binnen bijvoorbeeld Operation Endgame werken sinds 2024 internationale opsporingsdiensten en private partijen samen om wereldwijd cybercrime breed te bestrijden. Sinds de start:

- is er ingezet op duurzame verstoring (onder andere zijn meerdere botnets ontmanteld, infostealers offline gehaald, in Nederland zijn servers in verschillende datacenters offline gehaald waardoor de cybercriminelen geen toegang meer hebben tot hun systemen);
- zijn cybercriminelen op de EU sanctielijst geplaatst en op de Europe's Most Wanted-lijst gezet;
- kunnen mensen die slachtoffer zijn geworden van een infostealer via www.politie.nl/checkjehack nagaan of hun inloggegevens voorkomen in de buitgemaakte set, en krijgen ze meer handvatten wat ze vervolgens moeten doen om vervolgcriminaliteit te voorkomen;
- is er ingezet op preventie (onder andere op de website www.operation-endgame.com worden acties aangekondigd, onder het motto “Think about (y)our next move”, worden verdachten direct aangesproken op hun actie, en Operation Endgame geeft criminelen en getuigen de mogelijkheid om contact op te nemen met de politie).

Publiek-private samenwerking

Nauwe samenwerking tussen publieke en private partners blijft bij de bestrijding van cybercrime essentieel. Project Melissa, onderdeel van het programma Cyclotron, is een voorbeeld van een effectief publiek-privaat samenwerkingsverband voor de bestrijding van cybercrime; publieke (politie, OM en NCSC) en private cybersecurity partijen wisselen structureel kennis en informatie over ransomware met elkaar uit en signaleren trends en ontwikkelingen.[18] Gezamenlijk kan hierdoor een beter beeld van de problematiek worden verkregen van waaruit (preventieve) maatregelen en interventies voortkomen.[19] Ook publiceerde het samenwerkingsverband *best practices* om de impact van datadiefstal te beperken.[20]

Sancties

[18] Jaarbeeld Ransomware 2025 | NCSC
[19] Operationeel is er samengewerkt in onderzoeken (o.a. Operation Endgame), waarbij, gebruikmakend van ieders specifieke expertise en perspectief, gezamenlijk analyses zijn gemaakt van criminele infrastructuur.
[20] Best practices secundair slachtofferschap_v2_2_digitaal.pdf

Cybercriminelen opereren vaak vanuit landen waarmee samenwerking en rechtshulp moeilijk is. Het blijft in die gevallen daarom lastig om verdachten van (high tech) cybercrime in Nederland te berechten. Om die reden heeft het kabinet in het regeerakkoord de ambitie uitgesproken om cybercriminelen vaker op de EU sanctielijst te plaatsen.

Sinds enkele jaren is het mogelijk om sancties op te leggen aan personen of entiteiten die betrokken zijn bij ernstige cyberaanvallen die de EU, haar lidstaten of derde landen en organisaties bedreigen. Op initiatief van Nederland gebeurde dat in 2024 voor het eerst bij cybercriminelen. Inschatting van het OM en de politie is dat de concrete impact van dergelijke cybersancties op criminelen substantieel is. Ze veroorzaken onrust binnen cybercriminele groepen waardoor de effectiviteit van die groepen in ieder geval op korte termijn aanzienlijk wordt verminderd. Daarnaast mogen organisaties binnen de EU geen diensten aanbieden aan gesanctioneerde partijen.

In juli 2026 zijn twee individuen en twee organisaties nieuw op de Europese lijst geplaatst. De Nederlandse politie en het OM hebben hier in belangrijke mate aan bijgedragen. De gesanctioneerde organisaties faciliteerden criminaliteit door infrastructuur te leveren als zogenoemde bulletproof hosters. Zij boden cybercriminelen een schijnbaar veilige haven om ongestoord malware te verspreiden, phishing uit te voeren en botnets te ontwikkelen en aan te sturen. Hierdoor droegen zij bij aan de ransomware- en phishing aanvallen die op grote schaal binnen de EU zijn uitgevoerd, waardoor aanzienlijke financiële schade is opgelopen. Sanctionering geeft een duidelijke boodschap aan organisaties in de hele EU: doe geen zaken met gesanctioneerde bedrijven of personen. Lever geen (internet)diensten, zoals bijvoorbeeld hostingdiensten, aan gesanctioneerde bedrijven of personen. Dat is strafbaar en brengt de eigen organisatie en de samenleving schade toe. Organisaties worden opgeroepen om sanctielijsten actief te controleren.

Aanpak van facilitatoren

Cybercriminelen maken veelvuldig gebruik van infrastructuur en diensten die niet per definitie crimineel zijn, maar die zonder deze diensten veel moeilijker uitvoerbaar zouden zijn.

Misbruik van hostingdiensten vormt een belangrijk onderdeel van meerdere vormen van online criminaliteit. Alhoewel het overgrote deel van de Nederlandse hostingsector zelf maatregelen neemt tegen het gebruik van hun diensten door criminelen, is er een deel dat onbewust (bad) of bewust (bulletproof) malafide activiteiten faciliteert. Bij brief van 3 juli 2026 is uw Kamer geïnformeerd over de inspanningen van het kabinet om deze problematiek aan te pakken.[21] Uit de eerdere verkenning naar de aanpak van bad hosting kwam o.a. naar voren dat een wettelijke verplichting van het Know Your Customer principe een goede maatregel kan zijn om bad hosting tegen te gaan. Het kabinet zet in op een

[21] Kamerstukken II, 2025/26, 26643 nr 1544.

Europese aanpak van bad hosting en versterkte samenwerking op internationaal niveau.

Naast hostingdiensten worden ook andere diensten misbruikt. Een virtual private network (VPN) zorgt ervoor dat het netwerkverkeer van de gebruiker wordt versleuteld en dat zijn IP-adres wordt afgeschermd. Op deze manier weet een internetprovider of een netwerkbeheerder niet welke websites een gebruiker bezoekt of waar een website bezoek vandaan komt. Criminele VPNs richten zich specifiek op cybercriminelen en bieden hun de gelegenheid hun identiteit af te schermen. In mei 2026 is door een internationale opsporingsactie de criminele VPN-dienst First VPN offline gehaald.[22] Deze dienst adverteerde voornamelijk op bij politie bekende, cybercriminele fora en benaderde daarmee nadrukkelijk cybercriminelen als potentiële klanten. Bovendien werd expliciet vermeld dat elke medewerking met justitie geweigerd zou worden. Tijdens het strafrechtelijke onderzoek is uitgebreid onderzoek gedaan naar de dienst en zijn gebruikers. Tijdens de actie zijn 33 servers ontmanteld, die gelinkt zijn aan de criminele dienst. Daarnaast hebben alle gebruikers van deze aanbieder een bericht ontvangen waarin is medegedeeld dat de VPN-dienst offline is gehaald en zij als gebruiker van de dienst zijn opgemerkt.

Ook een proxydienst verbergt het echte IP-adres van de gebruiker. Door gebruik van een proxydienst lijkt het internetverkeer afkomstig van een ander apparaat, bijvoorbeeld van een router in een Nederlands huishouden. Cybercriminelen misbruiken dit soort routers, vaak verouderde apparaten zonder beveiligingsupdates (zogeheten "end-of-life"-apparatuur). Vervolgens bieden zij deze apparaten via online marktplaatsen te huur aan en maken zij gebruik van anonieme betaling in cryptovaluta. Hoewel niet iedere proxydienst illegaal is, worden ze ook door criminelen misbruikt om hun identiteit te verbergen. Dit maakt het opsporen en vervolgen van daders moeilijker en op die manier lijkt het alsof het strafbare feit door de eigenaar van het kwetsbare apparaat is gepleegd. In maart 2026 is in een grootschalig internationaal onderzoek door het cybercrime team van de politie in Limburg, onder leiding van het Openbaar Ministerie, in samenwerking met andere buitenlandse opsporingsdiensten de criminele proxydienst SocksEscort uit de lucht gehaald. SocksEscort bestond uit wereldwijd meer dan 369.000 gehackte en geïnfecteerde apparaten (zoals routers en camera’s) van thuisgebruikers. De dienst werd sinds 2010 tegen anonieme betaling in cryptovaluta aangeboden en werd gebruikt om strafbare feiten te plegen.[23]

Financieel onderzoek

Cybercriminaliteit genereert vaak aanzienlijke, grensoverschrijdende criminele opbrengsten. Cryptovaluta vormen de financiële ruggengraat van de cybercriminele economie. Zij maken het mogelijk opbrengsten van cybercriminaliteit wereldwijd te verplaatsen, wit te wassen en opnieuw te

[22] Criminele VPN-dienst First VPN offline gehaald | politie.nl
[23] Internationaal succes tegen georganiseerde cybercrime, criminele proxydienst uit de lucht | politie.nl

investeren in nieuwe aanvallen.[24] Het in kaart brengen van geldstromen, het afpakken van vermogen en/of verstoren van financiële infrastructuur van verdachte(n), raakt de kern van cybercriminaliteit, ondermijnt het criminele verdienmodel en past binnen de brede bestrijding. Financieel afpakken heeft daarnaast een belangrijke preventieve werking, doordat criminelen beseffen dat zij hun crimineel verkregen vermogen kunnen verliezen of daar niet langer over kunnen beschikken. Goede integratie van financieel onderzoek verhoogt de maatschappelijke impact van opsporing en vervolging door deze criminelen in hun portemonnee te raken. Het is noodzakelijk dat hier binnen onderzoeken en interventies van de politie en het OM nadrukkelijk aandacht voor is.

Recente EU-wetgeving ten aanzien van cryptovaluta moet het eenvoudiger maken om de identiteit van een cryptowallethouder te achterhalen. Veel cryptovalutadienstverleners zijn echter buiten de EU gevestigd. Ondanks dat ook in breder internationaal verband het belang van het kennen van de identiteit achter een cryptowallet is onderkend en het afgelopen jaar stappen zijn gezet, zijn aanbevelingen hierover nog niet wereldwijd geïmplementeerd.[25] Daarnaast maakt het gebruik van zogeheten cryptomixing diensten ook binnen de EU de attributie van transacties ingewikkeld.

Slachtoffernotificatie

Binnen opsporingsonderzoeken wordt vaak data van slachtoffers gevonden. Zo worden bijvoorbeeld op inbeslaggenomen servers login- of andere privégegevens aangetroffen. Als het mogelijk is, maakt de politie die datasets doorzoekbaar. ‘Check je Hack’ is het online hulpmiddel dat de politie daarvoor ter beschikking heeft gesteld. Met deze tool kan gecontroleerd worden of privégegevens van burgers zijn buitgemaakt door cybercriminelen. De politie heeft ‘Check je Hack’ ook het afgelopen jaar in kunnen zetten bij grote datalekken.[26]

Om tot een internationaal systeem te komen van slachtoffernotificatie heeft de Nederlandse politie via het EU Internal Security Fund (ISF) een bijdrage ontvangen om Check je hack en No More Leaks ook in andere landen te introduceren, zodat steeds meer landen en hun burgers kunnen worden gewaarschuwd voor diefstal en handel van hun gegevens.

Het NCSC stuurt in het kader van doelwit- en slachtoffernotificatie vroege waarschuwingen uit naar organisaties wanneer er betrouwbare informatie is dat een organisatie mogelijk doelwit is van een cyberaanval of kwetsbaarheid.

Strafverzwaring

Mede naar aanleiding van de evaluatie van de Wet Computercriminaliteit III wordt bezien of de strafmaxima voor bepaalde cyberdelicten nog voldoende recht doen aan de ernst, schade en maatschappelijke impact van deze feiten.[27] Vooral bij

[24] CCBN 2026 https://fts.politie.nl/cybercrimebeeld/2026/
[25] Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs
[26] Check je hack | politie.nl
[27] Kamerstukken II, 2025/26, 34372 nr 33.

computervredebreuk, oplichting en heling van niet-openbare persoonsgegevens zijn de huidige stafmaxima onvoldoende afgestemd op de ernst, de grootschaligheid en de impact van deze delicten. Gegevens die door middel van computervredebreuk en heling in “criminele handen” komen, vormen de kern van veel vormen van online criminaliteit, zoals oplichting en afpersing. Recente jurisprudentie onderstreept dit en benadrukt dat er met de huidige strafmaxima op cybercrimedelicten onvoldoende rekening is gehouden met de vérstrekkende gevolgen ervan. Zo heeft het gerechtshof Arnhem-Leeuwarden in een uitspraak van 15 april 2025 uitgesproken dat de maximale straf voor heling van niet-openbare gegevens (artikel 139g Sr) volstrekt ontoereikend is.[28] De verhoging van de strafmaxima wordt – ook indachtig het coalitieakkoord – thans nader uitgewerkt.

iii. Preventie

De conclusie dat dreigingen onvoorspelbaarder en complexer worden, betekent niet per definitie dat het verdedigen daartegen dat ook altijd is. Veel digitale incidenten vinden hun oorzaak nog altijd in het niet op orde hebben van “digitale basishygiëne”.[29] Juist nu de complexiteit in het dreigingsbeeld toeneemt zijn basismaatregelen een eerste effectieve barrière. Voor een gemiddelde organisatie geldt dan ook: fixeer je niet op het complexe dreigingslandschap, maar weer je daar in eerste instantie tegen met de basisprincipes.[30]

Ook voor burgers geldt dat het nemen van basismaatregelen een goede eerste verdediging is. Niettemin kunnen burgers ook als zij hun apparaten goed beveiligen en alle beschikbare updates en beveiligingsmaatregelen nemen, slachtoffer worden van een hack bij een organisatie waarmee zij zakendoen.

Met de doelstellingen die geformuleerd zijn in de Nederlandse Cybersecuritystrategie (NCLS) 2022-2028, heeft het kabinet zich gecommitteerd aan het streven naar een digitaal veilig Nederland en werkt het naar een toekomst waarin de scheefgroei tussen digitale dreiging en digitale weerbaarheid zo klein mogelijk is.[31] Hiertoe zijn doelstellingen geformuleerd om burgers en organisaties beter te beschermen tegen digitale risico’s en burgers in staat te stellen om snel en adequaat te reageren op cyberincidenten.[32]

Preventie van cybercriminaliteit concentreert zich op drie type maatregelen:

1. Situationele of technische preventie: systemen en producten veiliger maken;
2. Slachtofferpreventie: (potentiële) slachtoffers weerbaarder maken door hun basisveiligheid te vergroten;
3. Daderpreventie: de daderpopulatie verkleinen door middel van gerichte interventies om daderschap te ontmoedigen en recidive te beperken;

---

[28] Gerechtshof Arnhem-Leeuwarden 15 april 2025, ECLI:NL:GHARL:2025:2408.
[29] CSBN 2025
[30] 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)
[31] Nederlandse Cybersecuritystrategie 2022-2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid
[32] Nederlandse Cybersecuritystrategie 2022-2028 | Nationaal Coördinator Terrorismebestrijding en Veiligheid

Situationele of technische preventie

Burgers zijn weliswaar in eerste instantie zelf verantwoordelijk voor hun veiligheid in de persoonlijke online omgeving, maar beschikken niet altijd over de nodige kennis of middelen om de digitale weerbaarheid te vergroten. Wanneer burgers hun gegevens delen met bedrijven of organisaties zijn zij afhankelijk van de cyberveiligheid van derden. Idealiter wordt cyberveiligheid in systemen ingebouwd: security by design. Het zou minder aan gebruikers van producten en diensten moeten worden overgelaten of zij zich veilig gedragen of niet. Deels wordt dit geregeld in de Cyber Resilience Act (CRA) die in december 2027 in werking treedt voor digitale producten die op de Europese markt worden gebracht.

Ook een Anti Phishing Shield (APS) is een technische maatregel die bescherming biedt zonder afhankelijk te zijn van gedrag. Een APS is een systeem dat internetgebruikers herleidt naar een waarschuwingspagina in het geval zij een malafide website dreigen te bezoeken. Tussen augustus 2025 en januari 2026 is met een pilot de inzet van een APS in Nederland onderzocht[33]. De pilot kwam tot stand dankzij samenwerking tussen het ministerie van Justitie en Veiligheid, het NCSC, KPN, de politie, de Nederlandse Vereniging van Banken en NLconnect. Gedurende de pilot hebben ook internetaanbieders SNLLR, TriNed en Kabelnoord zich bij het APS aangesloten.

De resultaten van de pilot waren veelbelovend; meer dan twee miljoen pogingen om kwaadaardige websites te bezoeken onder ruim 200.000 gebruikers zijn geblokkeerd. Het systeem werkt via een voortdurend bijgewerkte lijst van kwaadaardige domeinen, die doorlopend wordt geactualiseerd. Het gaat om domeinen die een bedreiging vormen voor netwerk- en informatiesystemen, zoals phishing en malware. Op het moment dat er geen malafide activiteiten meer aan de domeinen kunnen worden gelinkt, wordt een domein van de lijst gehaald. Voor de samenstelling van de lijst ontvangt het NCSC informatie van verschillende publieke en private partijen die als *trusted partner* zijn aangemerkt.

Tijdens de pilot is de werking van het proces van het APS getest, en is er een goed werkend (technisch) proces tot stand gebracht binnen de huidige wettelijke kaders. Op basis van de resultaten is besloten de pilot voort te zetten en het APS onder te brengen bij het NCSC.

Inmiddels is het aantal gebruikers dat extra beschermd wordt door het APS uitgebreid naar 300.000 gebruikers en zijn meer dan vier miljoen kliks naar kwaadaardige domeinen voorkomen. De komende tijd zal het APS verder worden ontwikkeld en onderzoekt het NCSC samen met de betrokken partijen op welke wijze het bereik van het APS verder kan worden vergroot. Het gaat hierbij zowel om het vergroten van het aantal betrokken partijen als om nader onderzoek naar overige mogelijkheden die het APS kan bieden om proactief de weerbaarheid van Nederland tegen online dreigingen te vergroten. Voorbeelden zijn het uitbreiden

[33] Actiepunt III. 2.2.3 van de Nederlandse Cybersecurity Strategie (NLCS).

van het APS naar het mobiele netwerk, het (tijdelijk) tegenhouden van betalingen aan online criminelen, en de implementatie van het APS door organisaties met een eigen netwerk. Een vereiste voor een internetaanbieder om aan te sluiten bij het APS is het kosteloos aanbieden van de dienst.

Slachtofferpreventie

Iedereen kan slachtoffer worden van cybercrime. Veel mensen schamen zich, maar dat is niet nodig. Criminelen gaan geraffineerd te werk en schaven hun werkwijze continu bij om zoveel mogelijk geld te kunnen verdienen. Een oordeelvrije en begripvolle benadering van slachtoffers is essentieel, zodat wordt voorkomen dat de schuld bewust of onbewust bij slachtoffers wordt gelegd.[34]

Om te voorkomen dat burgers slachtoffer worden van cybercrime en daaruit volgende criminaliteit is het van belang hun digitale basisweerbaarheid te verhogen door hen te informeren over te nemen veiligheidsmaatregelen. Deze maatregelen vergen weinig tot geen technische kennis. Vaak blijkt aansporing echter nodig om deze maatregelen daadwerkelijk te treffen[35]. Onderzoek laat bovendien zien dat er onder burgers een brede informatiebehoefte over cybercrime bestaat.[36] Deze bevindingen vormen aanleiding om op publiekscommunicatie in te zetten.[37] Enerzijds om burgers bewust te maken van risico's en anderzijds door hen concrete handelingsperspectieven te bieden. Hiermee wordt ingezet op bewustwording en uiteindelijk ook gedragsverandering zodat (herhaald) slachtofferschap en schade voorkomen kan worden.

De campagne Laat Je Niet Interneppen is van start gegaan in 2023. Dit is een samenwerking tussen de ministeries van Justitie en Veiligheid, vanuit een veiligheidsperspectief, en van Binnenlandse Zaken en Koninkrijksrelaties, vanuit digitaal burgerschap, om burgers te waarschuwen voor *social engineering*.[38] *Social engineering* omvat de technieken die criminelen inzetten om door middel van psychologische manipulatie burgers en bedrijven te verleiden om toegang tot systemen te verkrijgen, malware te installeren of in het bezit te raken van persoonlijke gegevens van slachtoffers. Met die persoonlijke gegevens worden vervolgens criminele activiteiten uitgevoerd. Hoewel de uitingsvormen van *social engineering* continu in ontwikkeling zijn, blijven de onderliggende technieken en daarmee de te treffen beveiligingsmaatregelen hetzelfde.

Om slachtofferschap te voorkomen ligt het zwaartepunt van de campagne op het stimuleren van mensen om hun reactie te pauzeren en het bericht te controleren, *social engineering* te herkennen en een vervolgactie te nemen. Op laatjenietinterneppen.nl, de landingspagina van de campagne, kunnen burgers terecht voor meer informatie en tips. Naast het vergroten van de bewustwording voorziet de campagne in handelingsperspectieven voor minder digitaal vaardige burgers.

---

[34] Jildau Borwell, 'Unravelling the impact of cybercrime – Understanding victim experiences and implications for police practice'.
[35] Flitspeiling – Multi-Factor Authenticatie – Ipsos I&O (Augustus 2022).
[36] Veilig Online: Onderzoek naar kennis, houding en gedrag onder Nederlanders (Ipsos I&O, 2026).
[37] Actiepunt IV.1.1.1. van de Nederlandse Cybersecurity Strategie (NLCS).
[38] Laat je niet interneppen (veiliginternetten.nl)

Uit het campagne-effectonderzoek blijkt dat de campagne goed wordt gewaardeerd en de campagneboodschap duidelijk overkomt.[39] De campagne Laat Je Niet Interneppen zal ook in 2026 worden voortgezet rekening houdend met de inzichten die in 2025 zijn opgedaan.

In 2024 is de campagne Dubbel Beveiligd is Dubbel zo Veilig van start gegaan, gericht op het stimuleren van het instellen van tweestapsverificatie (2FA). Hoewel veel burgers bekend zijn met het principe van 2FA, dankzij het gebruik van 2FA bij onder andere het doen van bankzaken, inloggen op een werkomgeving, of het gebruik van DigiD, beperkt het instellen van 2FA zich veelal tot eerdergenoemde voorbeelden.[40] Voor het gebruik van andere apps of websites, zoals bijvoorbeeld de emailomgeving of een WhatsApp-account, is voor veel mensen nog onbekend dat er 2FA-mogelijkheden zijn en wat in deze gevallen de toegevoegde waarde is. Daarnaast maken mensen een afweging tussen het risico (gebrek aan digitale veiligheid) en de gebruiksvriendelijkheid (extra handeling), met als gevolg dat in veel gevallen 2FA niet geïnstalleerd wordt. Tot slot ontbreekt het in veel gevallen aan kennis om bovenstaande afweging zorgvuldig te kunnen maken, en wordt de term 2FA als technisch en ingewikkeld ervaren.[41]

De campagne Dubbel Beveiligd is Dubbel zo Veilig richt zich naast informatieverstrekking op praktische ondersteuning bij het instellen van 2FA, bijvoorbeeld door middel van een (digitaal) stappenplan en oefenomgeving op oefenen.dubbelzoveilig.nl.[42] De kwalitatieve concepttest onder de doelgroep heeft uitgewezen dat deze interventie werkt, waarna is besloten om het stappenplan en de oefenomgeving onder te brengen bij partners (bibliotheken, ouderenorganisaties en veiliginternetten.nl). De campagne heeft daarnaast bijgedragen aan bewustwording. In de nieuwe campagneflight zullen de gebleken effectieve hulpmiddelen worden ingezet om de bewustwording verder te vergroten.

Naast campagnes vindt publiek-private samenwerking plaats. Onder de vlag van het Actieprogramma Veilig Ondernemen heeft de City Deal Lokale Weerbaarheid Cybercrime[43] ertoe bijgedragen dat interventies voor het verhogen van cyberweerbaarheid van verschillende doelgroepen tot stand zijn gekomen.[44] Eind 2025 is de City Deal Lokale Weerbaarheid Cybercrime beëindigd. Dit jaar is door het ministerie van Justitie en Veiligheid en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een landelijke implementatieondersteuning voor gemeenten en regio’s ingericht in samenwerking met het Centrum voor

---

[39] https://open.overheid.nl/details/518d7ac4-52e1-40d2-81d7-2df52ca52945
[40] Kennis, houding en gedrag ten aanzien van Multi Factor Authenticatie (Klein & Winninghoff, 2023)
[41] Kennis, houding en gedrag ten aanzien van Multi Factor Authenticatie (Klein & Winninghoff, 2023)
[42] Uit onderzoek (Dubbel beveiligd is dubbel zo veilig: Onderzoeksrapport naar potentiële effectiviteit van interventies gericht op instellen van 2FA bij e-mailaccounts van 65-plussers (Van der Lelij et al., 2025) blijkt dat de interventie om droog te oefenen effectief is in het ondersteunen van mensen bij het instellen van tweestapsverificatie.
[43] City Deal Lokale Weerbaarheid Cybercrime - Het CCV
[44] Actiepunt IV.1.1.2 van de Nederlandse Cybersecurity Strategie (NLCS)

Criminaliteitspreventie en Veiligheid (CCV). Het doel is om gemeenten en regio's te helpen bij de borging en verdere uitrol van de opbrengsten van de City Deal Lokale Weerbaarheid Cybercrime via netwerksamenwerking en actieve kennisdeling voor de doelgroepen mkb, senioren en jeugd. Streven is deze ondersteuningsaanpak de komende jaren voort te zetten. De laatste projecten vanuit de City Deal worden dit jaar afgerond en geëvalueerd. De evaluatie van City Deal-projecten geven organisaties inzicht in de effectiviteit, de werkzame elementen en handvatten om de interventie door te ontwikkelen. Recent is een module van Hackshield op effect geëvalueerd door CyberweerbaarNL. De module "Online Grenzen" is zowel inhoudelijk kwalitatief als kwantitatief onderzocht. Het volledige rapport is hier te lezen.[45]

Net als voorgaande jaren draagt het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ook dit jaar bij aan de Nationale cursus Digitale Weerbaarheid.[46] Het betreft een gratis interactieve onlinecursus waarvan iedereen in Nederland gebruik kan maken. Inmiddels bestaat de cursus uit zeventien modules waarin onderwerpen aan bod komen, zoals cybercrime, online veiligheid, online fraude, desinformatie, digitaal flirten, verantwoord smartphonegebruik, AI en online privacy. Maandelijks bereikt de cursus tienduizenden Nederlanders, waaronder kwetsbare groepen.

Andere interventies die zijn gerealiseerd zijn het lespakket Digiveiliger, specifiek gericht op het vergroten van de digitale weerbaarheid van senioren, en het initiatief Appinspector,[47] bedoeld om Nederlanders te helpen inzicht te krijgen in de risico's van het gebruik van apps.

Daderpreventie

In samenwerking met team Cyber Offender Prevention Squad (COPS) van de politie wordt aandacht besteed aan het verkleinen van daderschap op het gebied van cybercrime. Wetenschappelijk onderzoek toont aan dat jonge cybercriminelen via verschillende wegen in die wereld terechtkomen.[48] Het identificeren en het op het juiste pad brengen van deze doelgroep is gecompliceerd maar niet onmogelijk. Het COPS team van de politie heeft daarvoor verschillende interventies ontwikkeld, zoals Hack Right en Re BOOTCAMP.

Hack_Right is een interventie die is ontwikkeld als alternatief of aanvullend straftraject voor daders tot 30 jaar. De interventie heeft tot doel recidive te voorkomen en kaders te bieden waarbinnen deelnemers hun ICT-talent op legale wijze kunnen ontwikkelen. Tot op heden hebben 44 jongeren deze interventie gevolgd. Dit is minder dan vooraf verwacht. Momenteel wordt een procesevaluatie uitgevoerd. Hack_Right wordt tot en met eind 2026 gesubsidieerd door het Ministerie van Justitie en Veiligheid. Aan het eind van de

[45] Effectevaluatie-Hackshield-eindrapport.pdf
[46] https://www.digitale-weerbaarheid.nl/
[47] https://www.appinspector.nl/
[48] https://cybercrime-pathways.com/research-outputs

subsidieperiode wordt gekeken of en op welke wijze Hack_Right kan worden ingebed in het interventiepalet van de uitvoerders.

re_B00TCMP is een evenement voor jongeren van 12 tot en met 25 jaar die interesse en vaardigheden hebben op het gebied van ICT en risico lopen online de grens op te zoeken. Er hebben inmiddels 18 edities van het evenement plaatsgevonden door het hele land en bijna 600 jongeren hebben deelgenomen. re_B00TCMP heeft inmiddels een evaluatie uit laten voeren. De adviezen uit de evaluatie zijn verwerkt in de nieuwe edities van het evenement.

Tot slot is dit jaar in Almere de pilot “Van Daderpreventie naar Talentontwikkeling” gestart. Het doel van deze pilot is het door(ontwikkelen) van een effectieve methodiek om jongeren met digitale vaardigheden die dreigen af te glijden naar cybercrime, om te vormen tot gekwalificeerde IT-professionals waarbij de basis wordt gelegd voor een schaalbare aanpak. De aanpak bouwt voort op de in de bovengenoemde City Deal Lokale Weerbaarheid Cybercrime ontwikkelde trainingen en ondersteunende initiatieven. Binnen de pilot wordt samengewerkt met meerdere partijen om cybertalenten te signaleren, op te leiden en richting de arbeidsmarkt te begeleiden. De pilot wordt vanuit de ministeries van Justitie van Veiligheid en ministerie van Economische Zaken ondersteund en loopt tot eind 2026.

iv. Versterking bevoegdheden digitale domein

Wet Computercriminaliteit III

De wet Computercriminaliteit III (CCIII) is in de afgelopen jaren twee keer geëvalueerd. De eerste evaluatie richtte zich enkel op de bevoegdheid ten aanzien van het op afstand binnendringen van een geautomatiseerd werk (de “hackbevoegdheid”). Uw Kamer heeft de beleidsreactie daarop ontvangen in de brief van 7 december 2023.[49]

Als uitvloeisel van de evaluatie is op enkele punten het beleid aangepast, zoals het beleid ten aanzien van de inkoop van commerciële binnendringsoftware. Daarnaast wordt op enkele onderdelen de wet- en regelgeving aangepast om knelpunten bij de inzet van de hackbevoegdheid in de praktijk op te lossen. Dit gaat onder meer om de regeling ten aanzien van de samenloop van verschillende bevoegdheden te verduidelijken en de inzet van de hackbevoegdheid als steunbevoegdheid voor de inzet van andere bevoegdheden mogelijk te maken. Deze vloeien voor het grootste deel voort uit de genoemde evaluatie en worden opgenomen in de Tweede Aanvullingswet voor de vernieuwing van het Wetboek van Strafvordering. Inwerkingtreding is voorzien in 2029.

Wijzigingen op het niveau van Algemene Maatregel van Bestuur worden opgenomen in het Besluit Heimelijke Bevoegdheden, behorend bij het gemoderniseerde Wetboek van Strafvordering. De inwerkingtreding daarvan wordt daarom ook in 2029 voorzien. Voor de praktijk van de opsporing is die

[49] Kamerstukken II, 2023–2024, 34372, nr. 31.

termijn erg lang. Om die reden wordt het nu nog geldende Besluit Onderzoek in een Geautomatiseerd Werk aangepast, conform de aanpassingen die in 2029 in werking zullen treden in het Besluit Heimelijke Bevoegdheden. Een voorstel daartoe is in juli 2026 in consultatie gebracht.[50] Daarmee kan de opsporingspraktijk enkele jaren eerder gebruik maken van de betreffende wijzigingen. Dit gaat primair om de nieuwe wijze van keuren van technische hulpmiddelen, eveneens een uitvloeisel van de eerdergenoemde evaluatie.

Eind 2025 is de WODC-evaluatie van de gehele wet CCIII verschenen. Deze evaluatie had als focus de vraag in hoeverre de doelstellingen van de Wet CCIII in de praktijk zijn gerealiseerd. Uw Kamer heeft de beleidsreactie daarop ontvangen bij brief van 11 mei 2026.[51] Gelet op de focus van dat onderzoek zijn er geen aanbevelingen die aanleiding geven tot substantiële, zelfstandige wijziging van beleid of wet- en regelgeving. Enkele aanbevelingen waar dat wel het geval zou kunnen zijn, passen in reeds aangekondigd beleid van het kabinet. Een voorbeeld is het stelen en helen van gegevens. Het kabinet onderschrijft de conclusie in het rapport dat de huidige strafmaxima voor deze delicten niet in verhouding staan tot de ernst, schaal en maatschappelijke impact. Zoals hierboven reeds vermeld wordt de verhoging van de strafmaxima zoals aangekondigd in het coalitieakkoord nader uitgewerkt.

Implementatie e-Evidence

Het ministerie van Justitie en Veiligheid, het OM en de politie hebben veel inspanning geleverd om de implementatie van het nieuwe EU-rechtsinstrument e-Evidence tijdig te realiseren. Dit instrument zal de opsporing van strafbare feiten waarbij digitaal bewijs aanwezig is aanmerkelijk effectiever kunnen maken. Het instrument dat staat in de traditie van de wederzijdse erkenning van strafrechtelijke bevoegdheden in de EU, gaat verder dan al bestaande instrumenten zoals het Europees Onderzoek Bevel. In het bijzonder waar het betreft het uitgangspunt dat – onder voorwaarden – een justitiële autoriteit uit een EU-lidstaat rechtstreeks en grensoverschrijdend bij een bedrijf dat in de EU elektronische diensten aanbiedt waardoor digitale sporen van menselijk handelen zijn vastgelegd, kan bevelen zulk bewijsmateriaal te verstrekken of in afwachting van verstrekking te bewaren. Bedrijven moeten binnen 10 dagen aan een bevel voldoen. Dit vergt een behoorlijke aanpassing van de werkprocessen bij het OM en de politie, en ook bij de bedrijven die een bevel ontvangen. Daarbij komt dat – in feite vooruitlopend op implementatie van de zogenoemde digitaliseringverordening (e-Justice) – in de Verordening e-Evidence verplicht is opgenomen dat justitiële autoriteiten en bedrijven het e-Evidence instrument met behulp van een specifiek opgericht EU IT-systeem moeten afhandelen. Dit heeft eveneens veel impact op de genoemde werkprocessen en allerhande werk rond vormgeving, inrichting en het operationeel krijgen van IT-hulpmiddelen.

Helaas is het, net als in veel andere EU lidstaten, niet gelukt de implementatievoorbereidingen af te ronden voor de in de verordening voor

[50] Overheid.nl | Consultatie Besluit houdende wijziging van het Besluit onderzoek in een geautomatiseerd werk
[51] Kamerstukken II, 2025–2026, 34372, nr. 33.

inwerkingtreding vastgelegde datum van 18 augustus 2026. Naast de realisatie van de benodigde IT-systemen en de diverse (samenhangende) werkprocessen en opleidingen die nog niet zijn afgerond, is het nationale wetgevingsproces ten behoeve van de implementatie van de verordening en richtlijn nog niet afgerond. Het wetsvoorstel Uitvoeringswet elektronisch bewijsmateriaal is in behandeling bij de Tweede Kamer. Het huidige streven en de verwachting is dat Nederland in het eerste trimester van 2027 operationeel van start kan gaan met het e-Evidence pakket. Tot dat moment zal Nederland binnenkomende en uitgaande verzoeken om elektronisch bewijsmateriaal blijven afhandelen langs de huidige bestaande werkwijze van rechtshulp.

VN cybercrime verdrag

Op 25 oktober 2025 is het VN Cybercrimeverdrag door enkele landen en door de Europese Unie ondertekend. Het verdrag kan gezien worden als een belangrijke stap voor versterkte samenwerking bij de bestrijding van cybercriminaliteit en het verkrijgen van elektronisch bewijs via rechtshulp. Het verdrag biedt de mogelijkheid voor samenwerking met landen die niet zijn aangesloten bij het Cybercrimeverdrag van de Raad van Europa (Verdrag van Budapest). Bij de ondertekening is door de Europese Unie benadrukt dat effectieve criminaliteitsbestrijding hand in hand moet gaan met robuuste waarborgen voor mensenrechten, fundamentele vrijheden, privacy en gegevensbescherming. Ook is expliciet gemaakt dat internationale samenwerking kan worden geweigerd wanneer verzoeken politiek gemotiveerd zijn of kunnen leiden tot mensenrechtenschendingen.

Op 20 mei 2026 stemde het Europees Parlement met een overweldigende meerderheid in met het VN Cybercrimeverdrag. Vervolgens heeft de Raad op 4 juni 2026 het verdrag namens de Unie goedgekeurd.

De Rijksministerraad ging op 26 juni 2026 akkoord met ondertekening van het VN Cybercrimeverdrag door Nederland. Na ondertekening zullen in Nederland de voorbereidingen worden getroffen voor ratificatie, via de uitdrukkelijke goedkeuringsprocedure.

Tot slot

De ontwikkelingen op het gebied van cybercrime laten zien dat blijvende inzet noodzakelijk is. De dreiging verandert snel en nieuwe technologieën waaronder AI brengen nieuwe risico’s met zich mee. Dit vraagt om blijvende inzet op preventie, verstoring, opsporing en vervolging, in nauwe samenwerking met private én internationale partners. Innovatie en het verder ontwikkelen van kennis en expertise om effectief op te treden tegen cybercriminelen en de digitale infrastructuur die zij gebruiken is essentieel.

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