

TOOL ACCESS ENABLED
LEARNING ACTIVE
STATUS RUNNING



CYBER CRIME BEELD NEDERLAND 2026

- > analysing environment
- > comparing possible actions
- > selecting optimal approach
- > executing action
- > observing response
- > evaluating outcome

RESULT // INCOMPLETE

Samenvatting

Previous approach discarded

- > generating alternative
- > adjusting parameters
- > selecting new action

0100 01
1101 01001001
0110011011
0010011100100
10101000101010
10010011100100
010011100100
11001 11001110110211
110010 0011100100
010101000 01000101010
1100100 10011100100
110010 00 1001001
1011001 100110110101
1110010 110010 11100100
001010 0010 1000101010
0111001001 010011100100
01110010011100100111001001
01110110011101100111011011
0100111001001110010011100100
0101010001010100010101000101
1100100111001001110010011100100
11001001110010011100100111
011 110011101100111011001110
011 001001110010011100100111
101010 01010100010101000101010001
10010011 010011100100111001001110
01110010 11 01001110010011100
01100111011 1101100111011
11 10011 111 0100111
0100010
0111
11
1110
00111
01000

01/02

Samenvatting

De inzichten uit het Cybercrimebeeld Nederland 2026 leiden tot drie belangrijke conclusies. Deze conclusies bieden aanknopingspunten om niet alleen individuen uit het cybercrime-ecosysteem op te sporen en te vervolgen, maar ook om onderliggende structuren en verdienmodellen duurzaam te verstoren.

1. De verschillende dadertypes zijn steeds meer met elkaar verweven, wat leidt tot hybride vormen van criminaliteit. Criminele groeperingen vermengen met statelijke actoren; jonge westerse cybercriminelen zijn betrokken bij nihilistisch gewelddadig extremisme.
2. Cybercrime moet niet langer worden gezien als een verzameling van afzonderlijke delicten, maar als een crimineel ecosysteem. Achter vrijwel iedere aanval schuilt een keten van onderling samenwerkende daders, middelen en criminele diensten die elkaar versterken: een criminele toeleveringsketen.
3. Kunstmatige intelligentie (AI) is een katalysator van cybercrime: deze vergroot het tempo en de schaal waarin aanvallen plaatsvinden. Crimineel AI-gebruik is niet meer hypothetisch en heeft een potentieel ontwrichtend karakter.

De capaciteit voor opsporing en vervolging is schaars. Het OM en de politie zullen dus keuzes moeten maken in welke zaken zij tijd, energie en expertise investeren. Dit daagt hen voortdurend uit om wendbaar en innovatief te zijn in hun aanpak. De brede bestrijding bestaat uit het vervolgen van verdachten, slachtoffer- en daderpreventie, verstoring van criminele activiteiten en het informeren van slachtoffers.

Het complexe dreigingslandschap van cybercrime vraagt naast een brede bestrijding ook om een integrale aanpak. Cybercrime- bestrijding is niet slechts voorbehouden aan de gespecialiseerde opsporingsteams bij het OM en de politie.

Het bedrijfsleven, publieke organisaties, wetenschap, de politiek én de individuele burger hebben allemaal een eigen rol in het beschermen van onze digitale veiligheid. De praktijk laat inmiddels zien dat die niet meer los te zien valt van onze fysieke veiligheid. Besef van urgentie is daarom niet langer toereikend; iedereen moet de eigen maatschappelijke rol oppakken en actief bijdragen aan een betere digitale weerbaarheid van onze samenleving. Wetenschappelijk onderzoek levert daarbij belangrijke handvatten.

Actiepunten OM en politie

Samenwerking intensiveren

Om effectief te blijven opsporen en vervolgen dienen het OM en de politie ten eerste de samenwerking te versterken met publieke en private partijen en internationale opsporingsdiensten. Alleen door grensoverschrijdend samen te werken, informatie uit wisselen en analysecapaciteit te delen kunnen zij effectief verdachten identificeren en vervolgen, criminele geldstromen volgen en de opsporings- en informatiepositie duurzaam versterken.

Meer innoveren

Ten tweede is het van belang om innovatieve en alternatieve opsporings- en interventiemethoden te ontwikkelen. Die zijn nodig om de verweven internationale daderstructuren effectief te kunnen doorbreken. Financieel rechercheren moet structureel een plek krijgen in cybercrime-onderzoeken. Als het OM en de politie vroegtijdig cryptovalutastromen in kaart brengen, inzetten op afpakken van crimineel vermogen en het verstoren van financiële infrastructuur, kunnen zij het criminele verdienmodel van cybercrime effectief aanpakken.

02/02

Samenvatting

Specialisme versterken en breed uitleren

Ten derde moeten het OM en de politie enerzijds blijven investeren in specialistische kennis – met name over cryptovaluta en AI anderzijds is deze kennis nu nog te vaak beperkt tot een kleine groep specialisten. Het is essentieel dat een breder fundament van kennis in de rest van de organisaties geborgd wordt, zodat zij niet afhankelijk zijn van een select groepje experts. Een sterke informatiepositie is een randvoorwaarde voor de bestrijding van cybercrime.

Actiepunten brede keten

Wendbare wetgeving

Voor een toekomstbestendige opsporing en vervolging is het belangrijk dat wet- en regelgeving meegroeit met een gedigitaliseerde wereld die continu en snel verandert. Criminele netwerken zijn online actief, maar wet- en regelgeving is vaak nog gebaseerd op de fysieke wereld. Om informatie van relevante publieke- en private partijen te kunnen gebruiken, hebben het OM en de politie passende juridische grondslagen nodig, zoals inmiddels is gecreëerd in de Cyberbeveiligingswet (Cbw). Voor het Nationaal Cyber Security Centrum is het nu makkelijker om informatie met de politie te delen zonder dat altijd een vordering nodig is.

Aanpak bad hosting

Maatregelen zijn nodig om *bad hosting* tegen te gaan. Verplicht daarom know your customer-beleid, verbied de eerste betaling in cryptovaluta en specificeer registratie van hostingbedrijven bij de Kamer van Koophandel. Ook dient het bestuursrecht effectief te worden benut om *bad hosting* tegen te gaan.

Meer preventie

Publieke en private partijen hebben een grote rol in preventie. Om cybercrime breed te bestrijden is het essentieel dat burgers goede voorlichting krijgen over de manier waarop buitenlandse mogelijkheden doen aan digitale beïnvloeding. Burgers moeten zich bewust zijn van het risico dat ze kunnen worden gebruikt door buitenlandse mogelijkheden.

Ook ouders en scholen hebben een belangrijke rol om te voorkomen dat jongeren, bewust of onbewust, online daders worden. Door te weten wat er online gebeurt en door jongeren digitaal weerbaar te maken tegen online beïnvloeding kunnen zij voorkomen dat jongeren belanden in cybercrime.

Ter voorkoming van slachtofferschap verdient ook het online consumptiegedrag van de individuele burger nadrukkelijke aandacht: het downloaden van allerlei apps en het aanschaffen van goedkope, veelal Chinese, apparatuur die zonder nadenken op het thuisnetwerk wordt aangesloten, vormt een significant risico. Het adagium 'als het gratis of goedkoop is, ben jij het product' gaat hier onverkort op: dergelijke apparaten en apps kunnen thuisnetwerken ongemerkt omvormen tot onderdeel van een proxynetwerk.

Basismaatregelen treffen

Bedrijven en organisaties kunnen hun weerbaarheid tegen digitale dreigingen relatief eenvoudig vergroten. Basismaatregelen op het gebied van cybersecurity maken vaak al een wereld van verschil. Geef dit prioriteit in beleid. Train personeel om weerbaarheid tegen *social engineering* te versterken en breng de eigen datahuishouding op orde. Ga ervan uit dat kwaadwillenden al in je netwerk zitten, óf op een dag binnenkomen en zorg dat zij dan beperkte datatoegang hebben door niet alle data op één plek op te slaan. Wanneer de potentiële fysieke consequenties hoog zijn, dient de beveiliging van systemen absolute prioriteit te hebben.

Aangifte doen, niet betalen

En: doe aangifte als je slachtoffer wordt van cybercrime. Tijdig inschakelen van de politie vergroot de kans op de opsporing en vervolging van criminelen. Betaal geen losgeld, dat is een directe investering in meer en gevaarlijker cybercrime. Voor sommige organisaties, zoals overheidsorganisaties, zou aangifte zelfs verplicht moeten zijn.

Het Cybercrimebeeld Nederland is een uitgave van het Openbaar Ministerie en Politie Nederland.

Neem voor inhoudelijke vragen contact op met ccbn@om.nl. Voor vragen vanuit de media kan contact worden opgenomen met [persvoorlichting van het Parket-Generaal](#).