



MJenV

Directoraat-Generaal

Rechtspleging en

Rechtshandhaving

Directie Rechtshandhaving en

Criminaliteitsbestrijding

Cybercrime en zeden

Turfmarkt 147

2511 DP Den Haag

Postbus 20301

2500 EH Den Haag

www.rijksoverheid.nl/jenv

Datum

3 september 2026

nota

Voortgangsbrief integrale aanpak cybercrime

1. Aanleiding

Jaarlijks wordt de Kamer geïnformeerd over de integrale aanpak van cybercrime. Daarnaast is door de politie en het OM een nieuw Cybercrimebeeld Nederland (CCBN) opgesteld. Dit beeld is als bijlage bij de voortgangsbrief bijgesloten.

2. Geadviseerd besluit

U wordt geadviseerd akkoord te gaan met het verzenden van de voorgestelde Kamerbrief over de voortgang van de aanpak van cybercrime, inclusief de bijlage.

3. Kernpunten

Cybercriminaliteit wordt onvoorspelbaarder, geavanceerder en complexer. Gebruik van artificiële intelligentie (AI) door cybercriminelen vergroot het risico op slachtofferschap. 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. De Kamer wordt hierover jaarlijkse geïnformeerd. In de brief wordt tevens geïnformeerd over versterking van bevoegdheden in het digitale domein.

De volgende onderwerpen komen in de brief 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;

Bijlage 1 betreft het Cybercrimebeeld Nederland dat is opgesteld door het Openbaar Ministerie en de politie. 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.
- Achter vrijwel iedere cyberaanval schuilt een professionele internationale toeleveringsketen. Gespecialiseerde aanbieders van digitale infrastructuur, 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.

**Directoraat-Generaal
Rechtspleging en
Rechtshandhaving**
Directie Rechtshandhaving en
Criminaliteitsbestrijding
Cybercrime en zeden

4. Toelichting

4.1. Politieke context

In de Kamerbrief wordt ingegaan op punten uit het coalitieakkoord;

- Cybercrime heeft een groeiende impact op de veiligheid van Nederlanders. We verhogen daarom de strafmaat voor zware cyberdelicten.
- Cybercriminelen met duidelijke banden met het Russische regime worden op de Europese Sanctielijst geplaatst.

4.2. Financiële overwegingen

Dit is een overzicht van lopend beleid dat niet om nieuwe investeringen vraagt.

4.3. Krachtenveld

Afstemming over de inhoud van de brief heeft plaatsgevonden met de directie Veiligheid en Bestuur (DGRR), de portefeuille Politieel Beleid en Taakuitvoering (DGOPV), de directie Sanctie en Slachtofferbeleid (DGSenB), de politie, het Openbaar Ministerie, de Nationaal Coördinator Terrorismebestrijding en Veiligheid, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Economische Zaken.

Zowel het ministerie van Binnenlandse Zaken en Koninkrijksrelaties als het ministerie van Economische Zaken hebben (net als vorig jaar) aangegeven dat medeondertekenen niet noodzakelijk werd geacht omdat het overgrote deel van de inhoud van de brief betrekking heeft op het beleid van Justitie en Veiligheid.

4.4. Communicatie

Met DCOM/Woordvoering is contact gezocht om eventuele communicatie van de politie en het OM rondom de publicatie van het nieuwe Cybercrimebeeld vanuit JenV te versterken en voor eventuele communicatie rondom verzending van de brief.

5. Informatie die niet openbaar gemaakt kan worden

De persoonsgegevens van de ambtenaren zijn niet openbaar ter bescherming van de persoonlijke levenssfeer.

Datum
3 september 2026