CYBER CRIME BEELD NEDERLAND 2026



OPENBAAR MINISTERIE POLITIE

Inhoudsopgave

Samenvatting	3
Inleiding	6
1. De daders: Een divers en diffuus daderlandschap	8
1.1 Cybercrime als wapen in hybride oorlogsvoering	9
1.2 Ransomware en datadiefstal	16
1.3 De Hacker Com	19
2. De economie: Cybercrime-as-a-service	25
2.1 De toeleveringsketen	26
2.2 Het wereldwijde web van cryptostromen	36
3. AI: Een katalysator van cybercrime	41
3.1 AI als assistent	42
3.2 AI als toenemend autonome actor	44
3.3 Implicaties voor de opsporing en vervolging	47
Onderzoeksverantwoording	49
Colofon	50
Bronnen	51

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.

Samenvatting

Actiepunten OM en politie

Samenwerking intensiveren

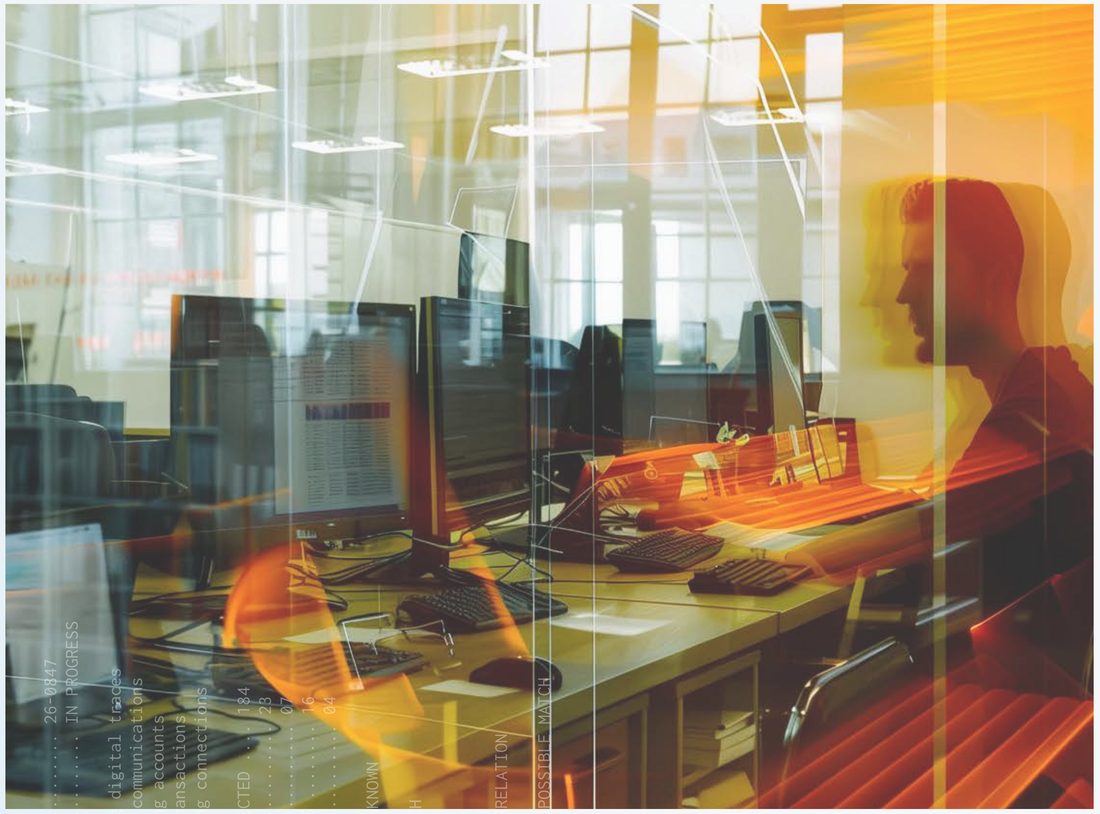
Om effectief te blijven opsporen en vervolgen dienen het OM en de politie ten eerste de samenwerking te versterken met publieke en private partijen en internationale opsporingsdiensten. Alleen door grensoverschrijdend samen te werken, informatie uit wisselen en analysecapaciteit te delen kunnen zij effectief 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 infrastructuren, kunnen zij het criminele verdienmodel van cybercrime effectief aanpakken.

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.



Samenvatting

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 mogendheden doen aan digitale beïnvloeding. Burgers moeten zich bewust zijn van het risico dat ze kunnen worden gebruikt door buitenlandse mogendheden.

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 allerhande 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.

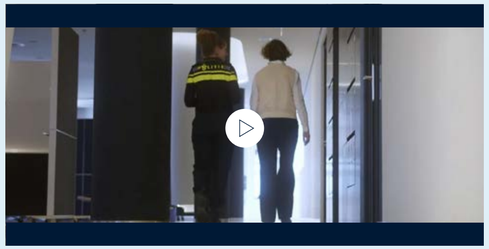
Aangifte doen, niet betalen
En: doe aangifte als je slachtoffer wordt van cybercrime. Tijdig inschakelen van de politie vergroot de kans op de opsporing en vervolging van criminelen. Betaal geen losgeld, dat is een directe investering in meer en gevaarlijker cybercrime. Voor sommige organisaties, zoals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

01/02

Inleiding

Cybercriminelen opereren grenzeloos. Daardoor kunnen zij vanuit welk land dan ook Nederlandse burgers, bedrijven en organisaties raken. In 2025 werd 17 procent van de Nederlandse bevolking slachtoffer van een vorm van online criminaliteit. Dat komt neer op 2,5 miljoen mensen die slachtoffer werden van cybercrime en/of een online vorm van oplichting, fraude, bedreiging of intimidatie.[1] In 2023 was dat nog 16 procent.

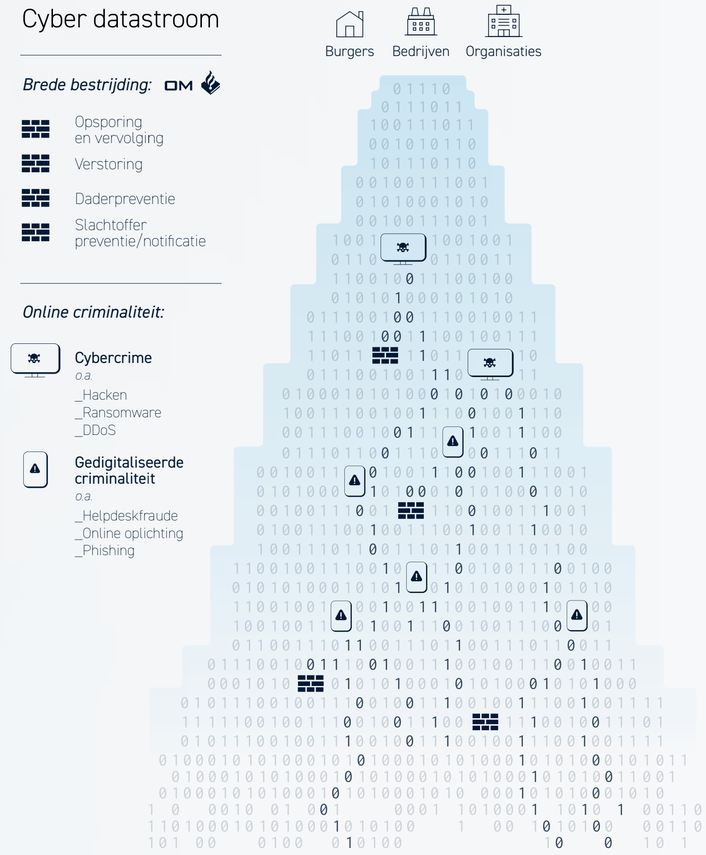
Het Cybercrimebeeld Nederland 2026 (CCBN) geeft een inkijk in de wereld van cybercrime, die een sleutelrol vervult binnen online criminaliteit. De maatschappelijke gevolgen van cybercrime worden steeds groter; dat laten cyberaanvallen op het OM en de politie en de toename van ransomware-aanvallen op bedrijven, organisaties en zorginstellingen zien. Met de veranderende verhoudingen op het wereldtoneel neemt de cyberdreiging toe. Daarmee groeit de rol die het OM, de politie en hun ketenpartners spelen in het handhaven van de (inter)nationale veiligheid.



Bekijk het interview met Christa de Pagter, landelijk coördinerend officier cybercrime en Caroline Sander, Operationeel Specialist, Eenheid Landelijke Opsporing en Interventies.

Online criminaliteit is te zien als een crimineel ecosysteem, waarin verschillende criminaliteitsvormen overlappen en met elkaar samenhangen. Net zoals een rivier in een delta uiteenvalt in talloze waterstromen, is cybercrime het startpunt van een datastroom die verschillende vormen van online criminaliteit voedt. Daarnaast is cybercrime ook faciliterend doordat criminelen tools en diensten aanbieden. De uiteenlopende vormen van online criminaliteit verschillen echter in aard, dynamiek en modus operandi.

Om ze effectief en breed te kunnen bestrijden hebben zij dus ook elk een verschillende aanpak nodig van het Openbaar Ministerie (OM) en de politie. Dit vraagt om specifieke accenten, expertise en interventies binnen de verschillende criminaliteitsvormen, én om een organisatiebrede versterking van de kennis en expertise op het gebied van online criminaliteit.



02/02

Inleiding

Het CCBN maakt cybercrime zichtbaar vanuit het unieke perspectief van het OM en de politie. Dit is dan ook niet alleen een analyse van de actuele dreiging, maar vooral een weerslag van de inzichten die het OM en de politie opbouwen in de dagelijkse opsporingspraktijk. De unieke informatiepositie van het OM en de politie maakt het mogelijk om ontwikkelingen vroegtijdig te signaleren, verbanden zichtbaar te maken en richting te geven aan een effectieve aanpak van cybercrime.

Cybercrime is een dynamisch en snel veranderend fenomeen. Nieuwe dreigingen en methoden ontwikkelen zich continu, nog tijdens het schrijven van dit dreigingsbeeld. Gezien de complexiteit en het tempo van deze ontwikkelingen is het niet mogelijk alle vormen van cybercrime hier uitputtend te belichten. Het CCBN richt zich op de meest actuele trends met de meeste impact. Hiervoor putten de auteurs uit opsporingsonderzoeken en openbare bronnen. Soms komen de meest actuele ontwikkelingen en inzichten voort uit nog lopende strafrechtelijke onderzoeken.

Hierdoor is het niet altijd mogelijk om inzichten concreet te maken met praktijkvoorbeelden, terwijl ze wel relevant zijn voor de bestrijding van cybercrime in Nederland. Wanneer beleidsmakers en bestuurders van publieke en private partijen deze inzichten koppelen aan innovatie, publiek-private samenwerking, wetenschappelijke kennis en internationale samenwerking, ontstaat een passend handelingsperspectief voor de brede bestrijding van cybercrime.

Opbouw van het CCBN

Het CCBN is opgebouwd uit drie samenhangende perspectieven: de daders van cybercrime, de cybercrime-economie en het crimineel gebruik van kunstmatige intelligentie (AI).

1. Het eerste hoofdstuk beschrijft het daderlandschap. Daarin zijn statelijke actoren, hacktivistische groeperingen en financieel gemotiveerde criminelen met elkaar verweven en zien het OM en de politie een opkomende dadergroep van jonge westerse cybercriminelen.
2. Het tweede hoofdstuk beschrijft de ontwikkelingen in de cybercrime-economie. Daarin staat de professionele toeleveringsketen centraal die cyberaanvallen op grote schaal mogelijk maakt.
3. In het derde hoofdstuk wordt ingegaan op de implicaties van het crimineel gebruik van AI. Dit maakt cybercrime nu al toegankelijker en schaalbaarder, terwijl de technologie razendsnel doorontwikkelt.

HOOFDSTUK 1

De daders: Een divers en diffuus daderlandschap

Het vorige CCBN liet in 2024 al zien dat er niet één type cybercrimineel is. Er bestaat een breed daderspectrum dat loopt van niet-technische jongeren met een relatief onschuldig motief tot hackende staten die onze nationale belangen bedreigen. Uit recente opsporingsonderzoeken naar cybercrime blijkt dat het daderspectrum diverser en diffuser wordt. Statelijke actoren vermengen met criminele groeperingen en naast de traditioneel Russischsprekende groeperingen openbaart zich een verontrustend netwerk van jonge westerse cybercriminelen. Zij beperken zich niet tot het plegen van cybercrime, maar zijn in sommige gevallen ook betrokken bij nihilistisch gewelddadig extremisme.

1.1 Cybercrime als wapen in hybride oorlogsvoering 9

1.2 Ransomware en datadiefstal 16

1.3 De Hacker Com 19



1.1

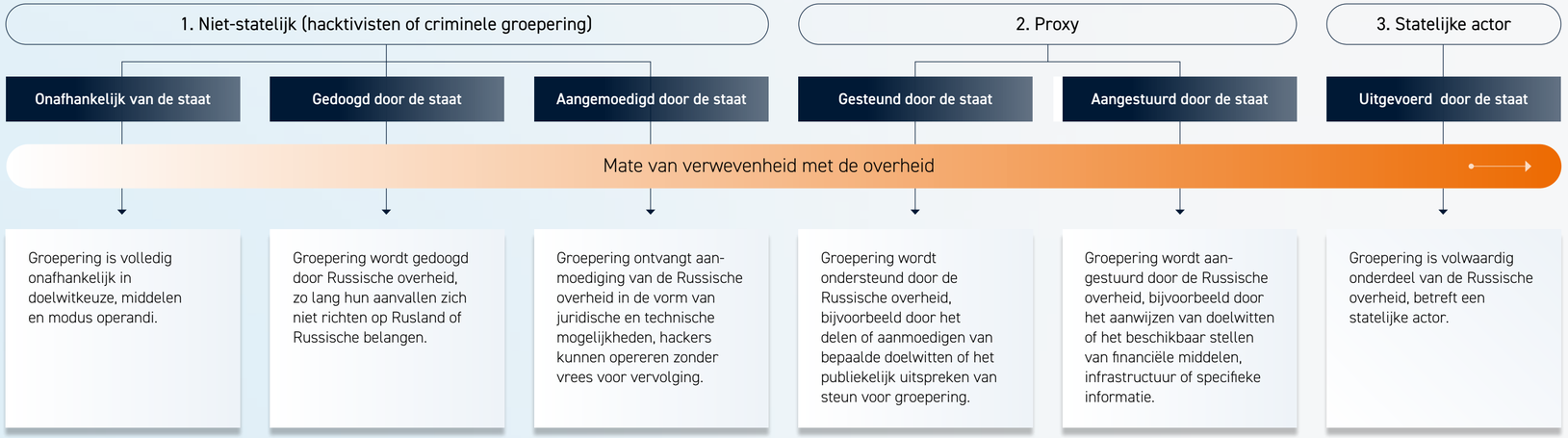
Cybercrime als wapen in hybride oorlogsvoering

Geopolitiek heeft altijd al een rol gespeeld in het cybercrimedomein. Met de geopolitieke machtsverschuivingen van de afgelopen jaren en de toenemende instabiliteit in de wereld neemt de cyberdreiging vanuit statelijke actoren toe.[2] Staten gaan steeds vaker over tot hybride oorlogsvoering. Daarbij combineren ze klassieke militaire middelen met beïnvloedingsactiviteiten, zoals heimelijke beïnvloeding, cyberaanvallen, de verspreiding van desinformatie, economische destabilisatie of concrete aanvallen op de vitale infrastructuur.[3]

Statelijke actoren zetten cyberaanvallen gericht in om politieke, militaire of economische doelen te realiseren. Op die manier kunnen zij binnen een grijs gebied blijven opereren en hun belangen behartigen zonder de juridische drempel van een gewapend conflict te overschrijden. Daarbij signaleren het OM en de politie in alle onderzoeken naar statelijke inmenging een sterke digitale of hightech component. Statelijke actoren maken optimaal gebruik van technische middelen als digitale infrastructuur en communicatieplatforms.

Deze ontwikkelingen stellen Nederland voor nieuwe uitdagingen op het gebied van nationale veiligheid en cybercrime. Volgens de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) gaat er een speciale dreiging uit van de vermenging tussen statelijke actoren en groeperingen of collectieven die niet primair onderdeel uitmaken van staatsstructuren, zoals hacktivisten of cybercriminelen.

Deze groeperingen en collectieven zijn niet altijd direct aan de staat te verbinden, maar zijn in wisselende mate verweven met de staat en moeten daarom als verlengde van de staat worden beschouwd.[4] Hierdoor vervaagt de scheidslijn tussen nationale veiligheid en cybercrime. De staat maakt het voor criminelen makkelijk om straffeloos te werken, bijvoorbeeld door wetten of technologie zo in te richten dat ze niet kunnen worden gepakt. Soms tolereren staten die activiteiten of moedigen ze zelfs aan. Statelijke actoren kunnen criminelen ook actief helpen, door hen te instrueren welke organisaties of landen aan te vallen of hen geld of tools te geven om aanvallen uit te voeren.



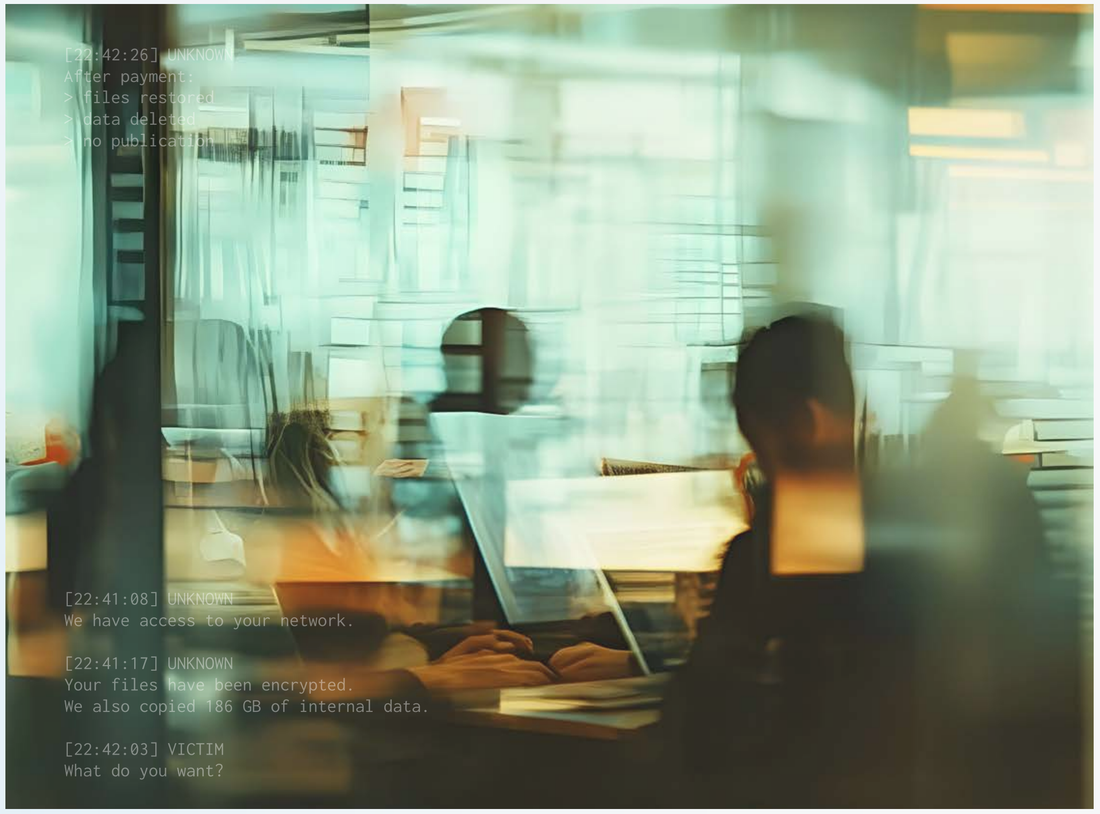
Overgenomen uit: 'Cybersecuritybeeld Nederland 2025', Nationaal Coördinator Terrorismebestrijding en Veiligheid, p. 31.

1.1

Cybercrime als wapen in hybride oorlogsvoering

De vervolging van cybercriminelen die zich in Rusland bevinden is nooit makkelijk geweest, maar in het verleden was samenwerking op operationeel vlak in beperkte mate mogelijk. Dit is gestopt sinds de inval van Rusland in Oekraïne. Cybercrimeverdachten bevinden zich vaak in landen waar Nederland geen rechtshulprelatie mee heeft, wat hen in staat stelt hun criminele activiteiten voort te zetten.

Dit brengt de nodige uitdagingen met zich mee. Maar waar criminelen zich ook bevinden, het OM en de politie blijven zich samen met internationale partners inzetten om hen de dans niet te laten ontspringen - of het nu gaat om het vervolgen van verdachten, het verstoren van hun infrastructuur, het gericht interveniëren in de criminele geldstromen, het informeren van slachtoffers of het toepassen van de sanctiewetgeving. Ook preventie is van belang om zowel slachtoffers als daders te voorkomen. Dit zijn stuk voor stuk bouwstenen voor de brede bestrijding van cybercrime.



1.1

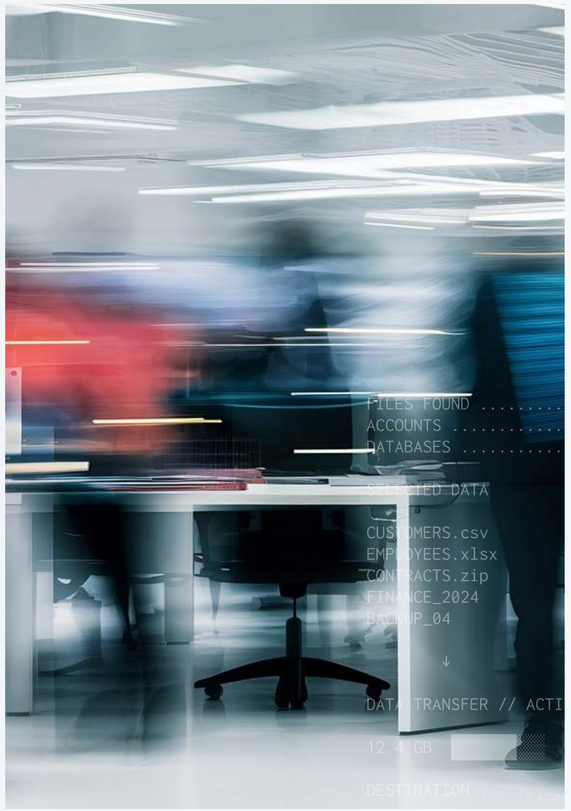
Cybercrime als wapen in hybride oorlogsvoering

De politiehack

Een voorbeeld van een groepering die zeer waarschijnlijk wordt gesteund door de Russische staat is Laundry Bear, die in 2024 publiek bekend werd na haar hack op de politie. Laundry Bear is al zeker sinds 2024 onder de radar actief en verantwoordelijk voor het uitvoeren van cyberaanvallen tegen westerse overheden, met name landen die behoren tot de Europese Unie en de NAVO. Gezamenlijk onderzoek van de politie, de AIVD (Algemene Inlichtingen- en Veiligheidsdienst) en de MIVD (Militaire Inlichtingen- en Veiligheidsdienst) wijst erop dat er zeer waarschijnlijk geen sprake was van een gerichte aanval, maar van opportunisme.

Waarschijnlijk kocht Laundry Bear hun toegang via een crimineel forum waarop criminelen gegevens verkopen die zijn gestolen met behulp van infostealer-malware. Uit de e-mailomgeving van het gehackte politie-account stal Laundry Bear vervolgens contactgegevens van alle politiemedewerkers.[5]

Oekraïense autoriteiten waarschuwen dat aan Rusland gelieerde groeperingen oude datasets verzamelen en gebruiken voor nieuwe aanvallen.[6] Ze hergebruiken inloggegevens, leggen nieuwe verbanden tussen verschillende datasets en buiten data uit die ze soms al jaren tot hun beschikking hebben. Het grote risico van de politiehack is dus niet gelegen in de feitelijke eerste datadiefstal, maar vooral in de manier waarop criminelen en statelijke actoren deze data op een later moment kunnen gebruiken. Als ze de data bewaren en hergebruiken - en die kans is groot - kunnen ze die onder andere gebruiken voor gerichte phishingaanvallen op politiemedewerkers, het vervalsen van interne communicatie of zelfs voor het in kaart brengen van lopende onderzoeken. De politiehack moet dus niet gezien worden als een gesloten boek, maar als een voortdurend veiligheidsrisico voor de toekomst. Dit benadrukt een mentaliteitsverandering die belangrijk is voor ieder bedrijf en iedere organisatie: datadiefstal is geen eenmalig incident, maar een blijvend risico.



1.1
Cybercrime als wapen in hybride oorlogsvoering

Gewone burgers als instrument in hybride oorlogsvoering

Ook gewone burgers kunnen worden ingezet in hybride oorlogsvoering door andere staten. Het online rekruteren van Europeanen voor cyberklusjes illustreert hoe pro-Russische hacktivisten cybercrime inzetten als wapen.

Een voorbeeld hiervan is de groepering NoName057(16), waarvan sommige betrokkenen banden hebben met de Russische overheid.[7] NoName057(16) is politiek-nationalistisch gemotiveerd en voert sinds de Russische inval in Oekraïne onder meer DDoS-aanvallen uit op organisaties in landen die Oekraïne steunen in de oorlog tegen Rusland. Aanvallen dienen als vergeldingsacties voor bijvoorbeeld financiële steun aan Oekraïne of Europese sancties tegen Rusland. Zo werden websites van Nederlandse havens[8] en gemeenten[9] slachtoffer van DDoS-aanvallen, net als die van organisaties die betrokken waren bij de NAVO-top.[10] Dergelijke aanvallen hadden tot op heden geen grote technische gevolgen. Het is echter de structurele en zichtbare aard van dit soort symbolische acties die op lange termijn destabiliserend kan werken; de aanvallen zijn intimiderend en tasten het vertrouwen aan van de Nederlandse bevolking in instituten.

NoName057(16) rekruteert uitvoerders van klusjes in Europa door in te spelen op de online leefwereld van burgers. *Gamification* van criminaliteit, status, gemeenschapszin en financiële beloningen spelen daarbij een belangrijke rol. NoName057(16) maakt gebruik van een Russisch- en een Engelstalig Telegramkanaal met meer dan 60.000 sympathisanten, waarin zij aanvallen opeisen en nieuwe doelwitten aankondigt als onderdeel van de Russische beïnvloedingsstrategie. Ook rekruteert zij er nieuwe leden voor het botnet waarmee ze de DDoS-aanvallen uitvoert.

Leden kunnen een gebruiksvriendelijke applicatie downloaden om via hun telefoon of computer zonder veel technische kennis deel te nemen aan gezamenlijke aanvallen.

De aanvallen van NoName057(16) zijn gericht op doelwitten in landen die zij beschouwt als tegenstanders van het Russische regime. Op een scorebord houdt NoName057(16) vervolgens bij wie de meeste aanvallen heeft gepleegd. In tegenstelling tot bij andere botnets nemen leden hier dus vrijwillig aan deel en worden zij met een competitie-element aangespoord om zo veel mogelijk aanvallen te plegen.

NoName057(16) probeert met haar 'leger van vrijwilligers' de indruk te wekken dat zij steunt op de collectieve kracht van een boze massa. Dat is echter schijn. Uit politieonderzoek blijkt dat het botnet van vrijwilligers op zichzelf geen heel serieuze dreiging vormt, maar dat het eerder gaat om pro-Russische beeldvorming. Dit botnet heeft lang niet genoeg deelnemers om een thuisnetwerk plat te leggen, laat staan meerdere overheidswebsites.

In werkelijkheid komen de zwaardere aanvallen die daadwerkelijk verstoringen kunnen veroorzaken vanaf servers van NoName057(16) zelf. NoName057(16) beperkt zich niet tot DDoS-aanvallen. De groepering biedt online ook andere pro-Russische klusjes aan. Dit varieert van het plakken van anti-NAVO stickers tot het verzamelen van e-mailadressen van journalisten.[11] De uitvoerders ontvangen een - soms slechts kleine - vergoeding in cryptovaluta.

⚠ Investeer binnen het OM en de politie nog meer in gespecialiseerde kennis op alle niveaus en versterk de samenwerking tussen publieke en private partijen, opsporingsdiensten en de wetenschap. Ontwikkel daarnaast innovatieve opsporings- en interventiemethoden om deze verweven daderstructuren effectief te kunnen doorbreken.

Wat is een DDoS-aanval?

Bij een DDoS-aanval probeert een crimineel een computer, netwerk of online dienst onbereikbaar te maken. Dit gebeurt met een groot aantal computers (Distributed Denial of Service, DDoS) of met één computer (Denial of Service, DoS).



De crimineel bestelt of start zelf een DDoS-aanval. | Het botnet stuurt grote hoeveelheden data naar de server. | De server raakt overbelast. | De website of dienst valt tijdelijk uit.

Soorten DDos-aanvallen

Volumetrisch
Er worden zoveel aanvragen naar de netwerkbron gestuurd dat deze overbelast raakt en niet meer goed kan functioneren.

Appicatielaag gericht
Er wordt een verzoek verstuurd dat zoveel verwerkingscapaciteit vraagt van de netwerkbron dat deze niet meer goed kan functioneren.

1.1 Cybercrime als wapen in hybride oorlogsvoering

In 2025 zijn in Nederland voor het eerst verdachten aangehouden die online zouden zijn gerekruteerd door een pro-Russische hacktivistische groepering. Het OM verdenkt twee 17-jarigen van het in kaart brengen van wifi-netwerken van overheidsorganisaties in Den Haag voor een buitenlandse mogendheid.[12] Informatie over deze wifi-netwerken kan vervolgens worden gebruikt om in te breken op de netwerken van deze organisaties. Een van de verdachten zou voor deze informatie een beloning in cryptovaluta hebben ontvangen. In 2025 zijn meer vormen van spionage strafbaar gesteld, zoals digitale spionage en spionage voor een buitenlandse mogendheid. De strafbare feiten waarvan de bovengenoemde jongeren worden verdacht, vallen onder deze nieuwe wetgeving.

Het aantal strafrechtelijke onderzoeken met betrokkenheid van een statelijke actor zal door deze uitgebreide spionagewetgeving mogelijk toenemen. Dit leidt tot extra druk op de capaciteit van de opsporing en vervolging.



Bekijk het interview met Corjan Kroon, landelijk officier van justitie Statelijke Inmenging.

Nieuwe spionagewetgeving

De wettelijke taak om onderzoek te doen naar statelijke actoren ligt bij de inlichtingendiensten: de AIVD en de MIVD. De taak van het OM en de politie in de aanpak van statelijke actoren is het opsporen en vervolgen van natuurlijke personen die verdacht worden van misdrijven die uitgevoerd worden ten behoeve van of in relatie tot een staat.

Om de nationale veiligheid beter te beschermen tegen hedendaagse dreigingen is sinds mei 2025 de spionagewetgeving uitgebreid. Vanwege de dreiging van digitale spionage kan het plegen van cybercrime zwaarder worden bestraft als dit gedaan wordt voor een buitenlandse overheid.

Voor computervredebreuk uitgevoerd voor een buitenlandse mogendheid staat een gevangenisstraf van maximaal 8 - en onder omstandigheden - 12 jaar.[13]

Operatie Eastwood

juli 2025

In samenwerking met organisaties uit 18 landen wereldwijd, met ondersteuning van Europol en Eurojust, hebben het OM en de politie verschillende delen van de infrastructuur van NoName057(16) ontmanteld.

Zij haalden meer dan honderd servers offline waarmee de groepering DDoS-aanvallen uitvoerde. Franse en Spaanse opsporingsdiensten hielden twee verdachten aan en Duitsland vaardigde zeven arrestatiebevelen uit.[14]

Voorlichting gericht op het vergroten van de weerbaarheid tegen digitale beïnvloeding door buitenlandse mogendheden is een essentieel onderdeel van de brede aanpak van cybercrime. Dit is relevant voor gemeenten, communicatie- en veiligheidsprofessionals, docenten en in bredere zin alle burgers die online actief zijn. Om deze weerbaarheid te versterken is het belangrijk dat er wordt ingezet op structurele bewustwording en training, bijvoorbeeld voor het herkennen van online beïnvloedingstechnieken, het duiden van geopolitiek gekleurde content en het ontwikkelen van handelingsperspectief bij vermoedelijke manipulatiecampagnes (gamification van criminaliteit).

Burgers moeten worden gestimuleerd om kritischer om te gaan met bronnen en online verzoeken, zich bewust te zijn van het risico op onbedoelde blootstelling aan hacktivistische of extremistische content, en weten waar zij verdachte online activiteiten kunnen melden of laten checken. Dat moet al op jonge leeftijd beginnen: als het gaat om hygiëne leer je als kind dat je je handen moet wassen, maar digitale hygiëne krijgt nog onvoldoende aandacht. Dit zou meer aandacht moeten krijgen.

1.1

Cybercrime als wapen in hybride oorlogsvoering

Hacktivistische aanvallen op vitale infrastructuur

Naast de hiervoor beschreven DDoS-aanvallen zien het OM en de politie sinds eind 2024 een duidelijke toename van (claims van) hackaanvallen van verschillende pro-Russische hacktivistische groeperingen. Deze claims doen zij op hun publiek toegankelijke communicatiekanalen op Telegram. Deze hacktivisten pogen of slagen er in binnen te dringen in industriële controlesystemen (ICS) in onder meer Europa en Nederland. Dit gaat om systemen in onder andere de water- en energievoorziening, de voedselproductie, het transport en de chemiesector.

Dat dergelijke incidenten vooral voorkomen in NAVO- en EU-lidstaten, is een indicatie dat de drijfveren van hacktivisten politiek-nationalistisch zijn.

Groeperingen, waaronder ook NoName057(16), functioneren als een ecosysteem, waarin zij onderling capaciteit, kennis en technieken met elkaar uitwisselen. Daarbij versterken zij de aandacht voor elkaars activiteiten door elkaars boodschap te herhalen.

De afgelopen jaren vonden verschillende hacktivistische aanvallen plaats op ICS in Europa. Zo namen in april 2025 zeer waarschijnlijk pro-Russische hacktivisten de besturing over van een dam in Noorwegen. Vier uur lang stonden de kleppen wagenwijd open, waardoor bijna 500 liter water per seconde ontsnapte tot het incident werd ontdekt en gestopt.[15]

Dat hacktivisten ook bereid zijn om Nederlandse doelen aan te vallen bleek in september 2025: zij vielen toen een nep-waterzuiveringsinstallatie in Nederland aan. Een cybersecuritybedrijf had deze nep-waterzuiveringsinstallatie opgezet als een zogenoemde honeypot. Op hun Telegramkanaal claimden de hacktivisten daadwerkelijk Nederlandse vitale infrastructuur te hebben gecompromitteerd.[16]

In mei 2026 vond de eerste bekende geslaagde verstoring van ICS in Nederland plaats. NoName0 57(16) verstoorde het klimaatcontrolesysteem van een Nederlandse aardappelboer. Via Telegram noemde NoName057(16) de aanval een vergeldingsactie voor verschillende acties tegen NoName057(16) en Rusland. Deze verstoring had geen grote gevolgen.

Dergelijke aanvallen op vitale systemen kunnen fysiek schadelijke gevolgen hebben, en in ernstige gevallen zelfs leiden tot maatschappelijke ontwrichting. Op dit moment zijn dit soort aanvallen nog niet heel technisch verfijnd en vallen ze eerder op door volume.

Hoewel de operationele impact doorgaans beperkt is, bestaat er wel degelijk een risico op onbedoelde of verkeerd ingeschatte fysieke gevolgen. Vooralsnog lijken de aanvallen echter eerder gericht op zichtbaarheid, intimidatie en psychologisch effect. Grootschalige fysieke sabotage met uitval van cruciale systemen lijkt vooralsnog niet het doel.

⚠ Kleine nutsbedrijven, provinciale en gemeentelijke diensten hebben een belangrijke rol in het waarborgen van de openbare veiligheid door zich met ***basismaatregelen*** te wapenen tegen hacktivistische aanvallen op ICS. Het is belangrijk dat zij zich bewust zijn van de eigen verantwoordelijkheid in de keten.

1.1
Cybercrime als wapen in hybride oorlogsvoering

Hoe langer hacktivisten kunnen blijven experimenteren, hoe meer vaardigheden en kennis van ICS-systemen ze vergaren. De toenemende frequentie van hackpogingen, de focus op civiele vitale infrastructuur en de voorbeelden van reeds succesvolle fysieke verstoringen in Nederland en Europa wijzen op een groeiend risico op cyberaanvallen met een directe impact op de veiligheid in Nederland. Bij een escalerende geopolitieke situatie is de kans reëel dat hacktivisten, gesteund door statelijke actoren, hun technieken en tools gericht inzetten om te proberen de maatschappij te ontwrichten.

Volgens de Europese Commissie zijn de Nederlandse vitale sectoren onvoldoende beschermd tegen aanvallen van buitenaf, onder andere door ondermaatse cybersecurity.[17]
Het OM en de politie zien dat hacktivisten zich onder meer consequent richten op kleinere nutsbedrijven, en provinciale en gemeentelijke diensten met maatschappelijke zichtbaarheid.

Kleine organisaties hebben in de regel minder geld voor cybersecurity en meer verouderde systemen dan grote organisaties. Door zich te richten op bekende IT-kwetsbaarheden bij deze kleinere organisaties maximaliseren hacktivisten de kans op een succesvolle inbraak met minimale middelen en operationeel risico. Doordat relatief eenvoudige aanvallen al tot een succesvolle verstoring kunnen leiden, kunnen hacktivisten met beperkte technische kennis zo zichtbare impact en media-aandacht genereren.

Deze dreiging is niet enkel een technisch vraagstuk, maar raakt ook steeds meer aan de openbare veiligheid in de fysieke wereld. Als de openbare orde in het geding is treedt de politie op lokaal niveau op onder het gezag van de burgemeester. De centrale rol van de burgemeester en de politie in het waarborgen van de openbare veiligheid strekt zich dus ook steeds meer uit naar het cyberdomein.

Voor de burgemeester ligt de nadruk vooral op de voorbereiding op cyberincidenten en –crises. Het OM, de politie en gemeenten ontwikkelen daarvoor op dit moment scenario's en oefenen hoe te handelen. Daarbij zal monitoring van hacktivistische platforms op onder andere Telegram bijdragen aan vroegtijdige signalering. Dat maakt het voor het OM, de politie en gemeenten mogelijk om tijdig en proportioneel te handelen. Om passend op te treden is het overigens belangrijk om scherp onderscheid te maken tussen de successen die worden geclaimd en wat hacktivisten daadwerkelijk hebben gedaan.



Bekijk het interview met Rian van Dam, cyberburgemeester.

Om effectief op te kunnen treden in een acute situatie waarbij de vitale infrastructuur wordt verstoord, is belangrijk dat de politie goed is voorbereid en nauw samenwerkt met ketenpartners. Dit houdt onder andere structurele informatie-uitwisseling met het Nationaal Cyber Security Centrum (NCSC) in. De Cyberbeveiligingswet maakt dit mogelijk. Ook is het van belang dat de politie openbare bronnen kan monitoren op signalen van verstoringen en mogelijke geopolitieke triggers die kunnen leiden tot vergeldingsacties.

Om als opsporings- en veiligheidsketen effectief te blijven is het noodzakelijk dat wet- en regelgeving explicieter anticipeert op de digitale realiteit. Dit vraagt om het verkennen en ontwikkelen van passende juridische grondslagen voor het gebruiken van informatie van relevante private partijen, zodat vroegsignalering en interventie bij statelijke en hacktivistische cyberdreigingen mogelijk blijft.

1.2

Ransomware en datadiefstal

In het CCBN 2024 is de opmars beschreven van cybercrimegroeperingen die bij het afpersen van organisaties de stap van dataversleuteling overslaan en direct overgaan tot het stelen van de data. Door organisaties en bedrijven met gevoelige data aan te vallen hoeven zij slechts te dreigen met openbaring om grote sommen losgeld te kunnen eisen. In zo'n geval maken criminelen geen gebruik van ransomware: malware om een computersysteem of data die daarop staat te versleutelen.

In de kern komt zo'n aanval echter op hetzelfde neer. Zowel bij versleutelde als onversleutelde slachtofferdata gebruiken criminelen het dreigement van openbaarmaking als drukmiddel voor losgeld: *ransom*. Daarom verwijst de term ransomware in het CCBN naar beide werkwijzen.

Ontwikkelingen

De Autoriteit Persoonsgegevens rapporteert over 2025 een groei van het aantal gemelde gevallen van ransomware. In 2024 werden 127 datalekken gemeld die het gevolg waren van een ransomware-aanval, in 2025 steeg dat naar 136.[18]

Het OM en de politie zien in verschillende opsporingsonderzoeken dat criminelen losgeld krijgen, maar zich vervolgens niet houden aan de belofte om de data van slachtoffers te verwijderen na betaling en de gestolen data alsnog verkopen. Naast het doorverkopen van de data komt het ook voor dat criminelen de data toch openbaar maken of slachtoffers later opnieuw afpersen.

Ransomwaregroeperingen die zich richten op organisaties en bedrijven met veel geld en data hebben vaak langdurig toegang tot de netwerken van hun slachtoffers. Hierdoor zijn zij in staat om de meest waardevolle data te achterhalen en zo hun hack optimaal te benutten.

Daarbij is een trend zichtbaar waarbij ransomwaregroeperingen ransomware combineren met infostealers. Criminelen benutten de mogelijkheid om naast afpersing van slachtoffers *infostealers* achter te laten in de slachtofferomgeving. Zo kunnen zij interessante data behouden voor eigen gebruik en de rest doorverkopen. Deze handel in gevoelige data leidt tot allerlei vervolgcriminaliteit. Andere criminelen gebruiken deze gegevens voor bijvoorbeeld helpdeskfraude of phishingberichten.

Naast de hacktivistische groeperingen uit paragraaf 1.1 hebben ook ransomware-groeperingen in toenemende mate impact op kwetsbare industriële controlesystemen. Een bekend voorbeeld is de ransomware-aanval op Colonial Pipeline in 2021, waardoor brandstoftekorten ontstonden in de Verenigde Staten.[19] In 2025 werd een Roemeens waterbedrijf besmet met ransomware, waarbij de bedrijfsvoering ernstig werd verstoord. De operationele besturingssystemen, zoals anti-overstromingssystemen, bleven in dit geval onaangetast.[20]

Voor ransomwaregroeperingen is een eventuele verstoring van systemen meer een drukmiddel en neveneffect van afpersing dan het primaire doel. Hoewel zij niet primair uit zijn op sabotage leidt de toenemende koppeling tussen bedrijfs-IT en industriële systemen en gebrekkige netwerksegmentatie er wel toe dat ransomware-aanvallen indirect steeds vaker impact kunnen hebben op industriële processen.

1.2
Ransomware en datadiefstal

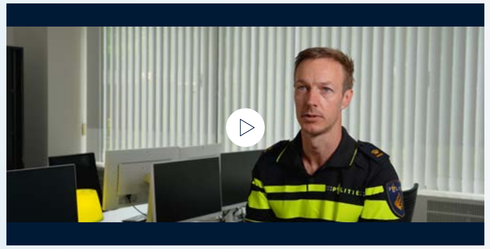
Grotere impact

Niet alleen namen de gemelde ransomware-aanvallen in 2025 toe, het OM en de politie krijgen ook steeds vaker te maken met ransomware en datadiefstal van grote omvang. Naast de impact op de getroffen organisaties en bedrijven hebben deze aanvallen ook een grote impact op de maatschappij en individuele burgers. Het afgelopen anderhalf jaar vonden meerdere aanvallen in Nederland plaats die dit illustreren: criminelen stalen onder andere data bij Clinical Diagnostics[21], Odido[22], de gemeente Epe[23] en Chipsoft[24], waarbij zij in sommige gevallen ook losgeld inden. Doordat criminelen gestolen datasets combineren - zoals NAW-gegevens, medische[25], financiële en werkgeversgegevens – ontstaan uitgebreide persoonsprofielen van burgers. Daarmee kunnen criminelen die burgers en de organisaties en bedrijven waar zij werken gericht aanvallen. Statelijke actoren kunnen zulke persoonsprofielen gebruiken om op grote schaal kwetsbare personen op strategische plekken te identificeren en onder druk te zetten voor bijvoorbeeld het verkrijgen van informatie.

Recente datadiefstallen laten zien hoe belangrijk het is om burgers goed te informeren over de mogelijke gevolgen en risico's van datadiefstallen, hun rechten en de eventuele voorzorgsmaatregelen die zij kunnen nemen. Daarnaast onderstrepen de hiervoor genoemde voorbeelden dat burgers moeten kunnen vertrouwen op adequate databeveiliging en -huishouding bij de bedrijven en organisaties waaraan ze hun gegevens toevertrouwen. Als kwaadwillenden een systeem binnendringen waar data gesegmenteerd is opgeslagen, is er vanzelfsprekend minder te halen dan wanneer alle data toegankelijk is als de dader eenmaal binnen is.

Voor bedrijven en organisaties zelf kunnen de gevolgen van een cyberaanval ook gigantisch zijn. Zo'n aanval kan in het ergste geval de primaire bedrijfsvoering platleggen en voor grote problemen zorgen. Toen het Openbaar Ministerie in juli 2025 enkele maanden volledig offline ging na een ernstig cyberincident had dit ingrijpende gevolgen: strafzaken werden uitgesteld, communicatie met de buitenwereld was praktisch onmogelijk en slachtoffers konden niet worden geïnformeerd.

Ook in de zorg kunnen cyberaanvallen leiden tot ernstige verstoring van de dienstverlening. In het ergste geval kan dit zelfs leiden tot de dood van patiënten: in het Verenigd Koninkrijk overleed een patiënt mede als gevolg van een verstoring van een laboratoriumdienst.[26] In Nederland moesten zorgverleners hun patiëntenportalen buiten werking stellen na de aanval op softwareleverancier Chipsoft waarbij criminelen patiëntgegevens stalen.[27]



Bekijk het interview met Maikel Rollman, Chief Operations, Team High Tech Crime van de Politie.

Cybersancties

juni 2024

Op initiatief van het OM en de politie zijn voor het eerst kopstukken uit de cybercrimewereld op de Europese sanctielijst geplaatst. De Russische individuen zijn verantwoordelijk voor cyberaanvallen die in de EU veel schade hebben aangericht, zoals hacks op banken en ransomware-aanvallen op de zorgsector. De gesanctioneerden mogen de EU niet meer in, hun tegoeden worden bevroren en bedrijven in de EU mogen geen zaken meer met hen doen. Hiermee worden voor het eerst ook financieel gemotiveerde cybercriminelen aangepakt die grote maatschappelijke schade aanrichtten.[28] Cybersancties zullen ook in de toekomst vaker worden ingezet.

juli 2026

Dat sancties een adequaat middel zijn om cybercrime te verstoren wordt ook ingezien door andere landen. De EU plaatste twee hackers van pro-Russische hacktivistische groeperingen op de sanctielijst. Daarnaast plaatste de EU ook de pro-Russische hacktivistische groepering Z-Pentest op de lijst.[29]

1.2
Ransomware en datadiefstal

Aangiftebereidheid

Als bedrijven of organisaties slachtoffer worden van ransomware of datadiefstal, is van belang dat aangifte wordt gedaan. Toch schakelen weinig organisaties in Nederland de politie in. In 2023 deed van de getroffen bedrijven (met twee of meer werknemers) slechts 14 procent aangifte.[30] Bedrijven zien aangifte vaak als mogelijk risico voor de continuïteit van de bedrijfsvoering. De politie is echter de enige partij die als doel heeft om naast het stoppen van de strafbare feiten, het criminele proces te verstoren én de dader(s) op te sporen.

De politie heeft onder het gezag van het OM unieke opsporingsbevoegdheden tot haar beschikking en een groot in- en extern (internationaal) netwerk. Aangiftes stellen de politie in staat om patronen te herkennen, waardoor zij de daders kan opsporen. Aangiftes zijn dus cruciaal om te voorkomen dat criminelen ongestraft door kunnen blijven gaan. Daarnaast kan de politie adviseren en informatie delen over de modus operandi, waarmee toekomstige aanvallen voorkomen kunnen worden.

⚠ Zonder aangifte blijft criminaliteit vaak buiten het zicht van de strafrechtketen, waardoor een effectieve aanpak wordt belemmerd en criminaliteit blijft bestaan. Hierdoor worden meer bedrijven en organisaties slachtoffer. Bovendien kan door tijdig aangifte te doen met ingrijpen van de politie juist verdere schade worden voorkomen.

Samenwerkingsverband Melissa

Het publiek-private samenwerkingsverband Melissa heeft de afgelopen drie jaar succes en meerwaarde bewezen in de bestrijding van ransomware. De samenwerkende partijen zijn het OM, de politie, het NCSC, Cyberveilig Nederland en diverse cybersecuritybedrijven: Computest Security, Data Expert, Deloitte, Eye Security, Fox-IT, Kennedy Van der Laan, mnemonic, NFIR, Northwave, PWC Nederland, Responders, Tesorion en Trellix.

Mede dankzij Melissa heeft de politie onder andere meer dan 50 decryptiesleutels weten te bemachtigen van de ransomwaregroepering Deadbolt. Daarmee konden slachtoffers weer toegang krijgen tot hun data. Tijdens een internationale operatie ontmantelden opsporingsdiensten met hulp van private partners één van 's werelds grootste botnets - Qakbot - en konden ze verdachten identificeren.

Door het delen van ransomwarestatistieken konden het OM en de politie slachtoffers van de ransomwaregroepering Cactus identificeren en informeren. In veel gevallen voorkwam dit dat zij slachtoffer werden.

Universiteit Leiden evalueerde resultaten en benoemde succesfactoren van de samenwerking. Zo draagt de uitwisseling van unieke kennis en middelen, zoals technische dreigingsanalyses en juridische en operationele expertise, bij aan een veelzijdige aanpak. Ook het onderling vertrouwen dat volgt uit korte lijnen en een open samenwerking blijkt essentieel voor informatie-uitwisseling.[31]

1.3

De Hacker Com

Niet alleen statelijke actoren en criminele groeperingen uit niet-westerse landen vormen een bedreiging in het cybercrimedomein. Ook in westerse landen is een fenomeen zichtbaar van cybercriminelen die grote impact hebben op de maatschappij. Het OM en de politie zien dit fenomeen recent opkomen in Nederland. In navolging van internationale opsporingsdiensten hanteren zij hiervoor het label 'Hacker Com' als brede, overkoepelende classificatie voor een los samenhangend netwerk van individuen, eerder dan als aanduiding voor één afgebakende of formele organisatie.

Achter de Hacker Com gaat een dynamisch online netwerk schuil van personen die onder meer cryptovaluta stelen en grote organisaties afpersen, met name door middel van datadiefstal.

In tegenstelling tot puur financieel gemotiveerde criminelen zoeken personen die onder de classificatie 'Hacker Com' vallen actief de publiciteit. Anders dan de hacktivistische groeperingen die eerder aan bod kwamen, baseren zij hun criminele activiteiten niet op ideologie of politiek, maar worden zij gedreven door financieel gewin en sociale status.

Begin 2026 eisten criminelen losgeld na het stelen van data van meer dan 6 miljoen klanten van telecomprovider Odido. Odido ging niet in op de afpersing. Daarna publiceerden de criminelen onder meer de telefoonnummers, geboortedata, bankrekeningnummers, paspoortnummers en woonadressen van klanten van Odido online, waaronder de gegevens van 16.000 medewerkers van bedrijven en organisaties die behoren tot de vitale Nederlandse infrastructuur.[32]

Het OM en de politie doen strafrechtelijk onderzoek naar deze afpersing, die werd uitgevoerd door criminelen die zich verschuilen achter de naam Shiny Hunters. Shiny Hunters wordt geclassificeerd onder de Hacker Com, net als andere cybercrimegroeperingen als Scattered Spider, Team PCP en Lapsus. Zeer waarschijnlijk vielen groeperingen die geclassificeerd worden onder de Hacker Com in Nederland ook KLM[33], BCD Travel[34] en zeven universiteiten[35] aan. Het OM en de politie zien dat de Hacker Com zich snel ontwikkelt in grootte, technische capaciteit en complexiteit van doelwitten.



1.3

De Hacker Com

De Com

De Hacker Com maakt deel uit van een groter geheel, de Com *(The Community)*. De Com, weer een label gebruikt door opsporingsdiensten, verwijst naar een wereldwijd losvast netwerk van duizenden individuen. Voor de leesbaarheid wordt in het vervolg naar deze individuen verwezen als 'leden', ook al gaat het niet om een formele organisatie met lidmaatschap: de term is een classificatie die het OM en de politie hanteren om personen te duiden die op basis van hun gedrag en netwerk tot de Hacker Com worden gerekend.

Leden zijn overwegend kinderen en jongeren, variërend van 11 tot 25 jaar, die elkaar vinden in competitieve online subculturen waarin Engels de voertaal is. De laatste paar jaar is de Com exponentieel gegroeid, zowel het netwerk zelf als het aantal slachtoffers dat het netwerk maakt. Leden zijn betrokken bij verschillende typen misdaad, variërend van fysiek geweld tot cybercrime en van terrorisme tot kindermisbruik.

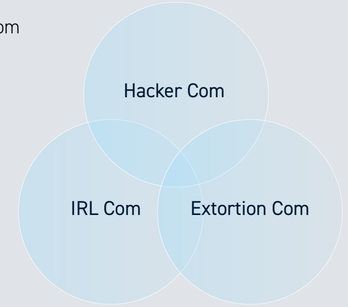
Degenen die een misdrijf plegen en dit vervolgens aantonen in chatkanalen worden daarvoor beloond met aanzien en sociale status. Dit stimuleert leden om steeds extremere misdrijven te plegen.

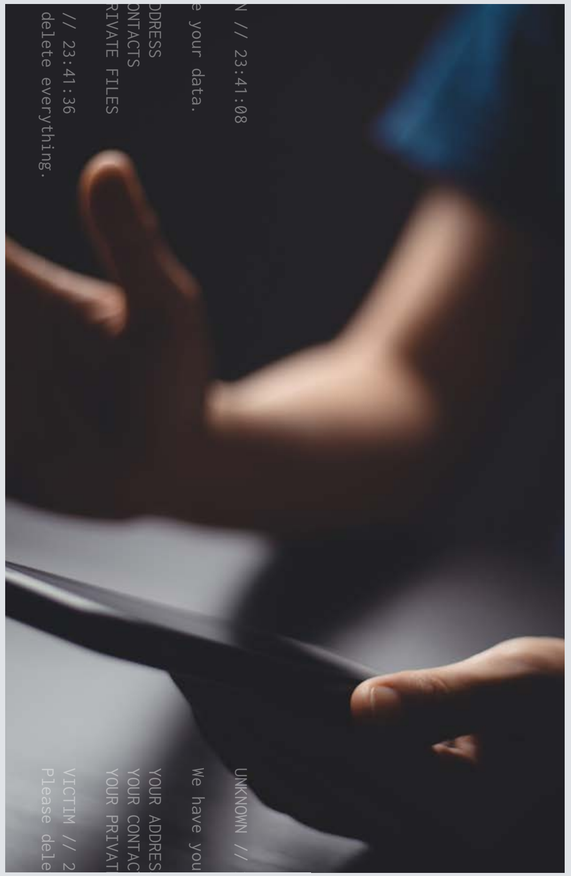
Bij sommige misdrijven spelen ideologische motivaties een rol, zoals rechts-extremisme of neonazisme. Het kan ook gaan om satanistische of misantropische denkbeelden. Leden putten echter meestal opportunistisch elementen uit deze ideologieën en denkbeelden om het extremistische en gewelddadige karakter. Over het algemeen kennen de misdrijven juist een gebrek aan ideologie en laten zij zich het best omschrijven als nihilistisch gewelddadig extremisme. De NCTV noemt dit nihilistisch gewelddadig extremisme in sommige gevallen een terroristische dreiging voor Nederland.[36]

In onder andere de Verenigde Staten[37], Brazilië[38], Zweden[39], het Verenigd Koninkrijk[40], Roemenië[41], Duitsland[42] en Nederland[43] zijn verschillende leden aangehouden en veroordeeld. In Nederland hebben het OM en de politie op dit moment tientallen verdachten in beeld.

De Com is op te delen in drie sub-Coms: de Hacker Com, de Extortion Com en de IRL (In Real Life) Com. Deze Coms zijn elk verantwoordelijk voor een eigen type criminaliteit. Daarbij overlappen ze deels in leden, communicatiekanalen, tactieken en technieken. Het CCBN zoomt in op de Hacker Com, maar aangezien er tussen de verschillende Coms een bepaalde mate van samenhang is komen de Extortion Com en IRL Com hier ook kort aan bod.

De Com





1.3

De Hacker Com

IRL Com

De IRL Com houdt zich bezig met fysiek geweld dat online tot stand komt. Dit kan gaan om 'geweld op bestelling' als verdienmodel, maar leden van de IRL Com moedigen elkaar ook aan om mensen op straat neer te steken of zelfs te vermoorden. Leden verspreiden beelden van het geweld online of streamen het geweld live. De andere leden kijken mee, moedigen geweldplegers aan en lachen slachtoffers uit.[44] De geweldplegers verdienen hiermee status en aanzien binnen de gemeenschap.

Activiteiten van groeperingen uit de IRL Com vinden ook in Nederland plaats. Het OM vervolgt een 25-jarige Nederlandse man die het gewelddadige No Lives Matter oprichtte. Hij zou tevens de leider zijn van deze groepering, die leden oproept tot geweld, moord en het delen van beelden hiervan. Het OM verdenkt de man van deelname aan een terroristische organisatie en de verkrachting van een minderjarige.[45]

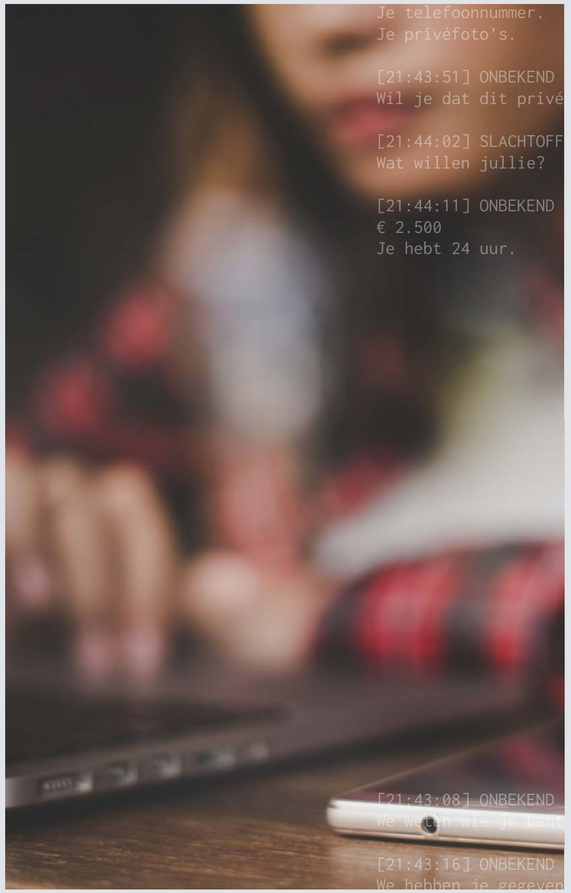
Extortion Com

Leden van de Extortion Com houden zich bezig met het groomen en afpersen van minderjarigen en andere kwetsbare personen.[46] Zij bedreigen, chanteren en manipuleren hun slachtoffers in een mechanisme van herhaalde druk. Zodra daders eenmaal compromitterend beeldmateriaal van slachtoffers hebben, gebruiken ze dat als permanent drukmiddel om slachtoffers sadistische en/of seksueel expliciete handelingen uit te laten voeren en beelden hiervan te delen.

Leden benaderen hun slachtoffers via platforms als Roblox, Minecraft en Discord. De vraag begint klein en op basis van vertrouwen. Daders gebruiken kennis over en beelden van slachtoffers vervolgens als drukmiddel om slachtoffers opnieuw beeldmateriaal te laten produceren. Eenmaal in de greep van de dader worden de eisen echter steeds extremer.

Daders dwingen slachtoffers op deze wijze tot zelfbeschadiging, dierenmishandeling, seksueel expliciete handelingen of in het uiterste geval zelfs zelfmoord. Beelden hiervan streamen slachtoffers ook vaak weer live.

Ook in Nederland lopen strafzaken rondom de Extortion Com. Het OM vervolgt bijvoorbeeld een 23-jarige Nederlandse man die een grote rol speelt in de Extortion Com *764*.[47] Uit chatberichten en beeldmateriaal zou onder andere blijken dat de verdachte meerdere slachtoffers heeft aangezet tot zelfbeschadiging, anderen heeft geïnstrueerd hoe ze meisjes het beste konden groomen, in het bezit was van kinderporno en die heeft verspreid.



1.3
De Hacker Com

De Hacker Com

Leden van de Hacker Com zijn over het algemeen minderjarige mannen die zich onder andere via Telegram en Discord bezighouden met het hele spectrum van online criminaliteit: van online fraude en oplichting tot identiteitsfraude, doxing, sabotage, handel in gestolen gegevens, diefstal van cryptovaluta en ransomware. Sinds 2018 is de Hacker Com explosief gegroeid, van honderden naar duizenden leden uit met name westerse landen.[48] Het is waarschijnlijk dat ook Nederlanders betrokken zijn bij de Hacker Com.

De Hacker Com past niet eenduidig op het daderspectrum. Het ene lid kan technisch onderlegd zijn en ondersteunen bij ransomware, terwijl een ander zich focust op minder technische vormen van cryptovalutadiefstal, phishing of SIM-swapping.

Er is wel een aantal opvallende kenmerken dat de leden onderscheidt van andere cybercriminelen. Allereerst de jonge leeftijd. Hierom is het belangrijk om preventieve maatregelen te treffen om te voorkomen dat zij zwaardere strafbare feiten gaan plegen. Daarnaast bevinden leden zich doorgaans in westerse landen, realiseren zij toegang tot systemen over het algemeen via menselijke manipulatie, streven zij online naar sociale status, gebruiken zij vaak geweld bij interne conflicten en zijn zij georganiseerd in een fluïde decentrale structuur.

Westerse achtergrond en social engineering

De eerder genoemde groeperingen Shiny Hunters, Scattered Spider, Team PCP en Lapsus persen grote organisaties af door het stelen van gevoelige gegevens en door vervolgens te dreigen met het publiceren van die gegevens. De Engelse taalbeheersing en westerse achtergrond werken in het voordeel van de leden bij verschillende vormen van social engineering. Met informatie uit gestolen datasets en open bronnen overtuigen zij slachtoffers onder valse voorwendselen via e-mail, chatbericht of telefoon om toegang te verlenen tot de interne systemen. Een andere tactiek die ze gebruiken is SIM-swapping.

In het onderzoek naar de Odido-hack heeft de politie sterke aanwijzingen gevonden voor de betrokkenheid van Nederlandse criminelen. Het gaat daarbij onder meer om een telefoongesprek met Odido's klantenservice, vlak voor de hack. In dit gesprek deed een Nederlandssprekende man zich voor als IT-medewerker van Odido. Via phishing misleidde de man een bedrijfsmedewerker om inloggegevens te delen die vervolgens misbruikt werden om de data te stelen.



⚠ De jonge leeftijd van Hacker Com-verdachten onderstreept het belang van vroeg ingrijpen en jongeren tijdig op het rechte pad te sturen. Door jongeren digitaal weerbaarder te maken en hen te leren rode vlaggen te herkennen in online contacten kan voorkomen worden dat ze in cybercrime terecht komen. Publieke berichten en waarschuwingen kunnen daarbij helpen, maar preventie begint het liefst dichterbij: op school of thuis.

1.3
De Hacker Com

De focus op social engineering neemt niet weg dat leden ook over technische vaardigheden beschikken. Ze gebruiken die om zo veel mogelijk gevoelige data te stelen en soms ook om data op de systemen van slachtoffers te versleutelen. Bij de afpersing van Marks & Spencer in 2025 zetten leden van Scattered Spider ransomware in die ontwikkeld is door een ransomware-as-a-service aanbieder uit één van de voormalige Sovjetrepublieken.[49] De schade betrof 348 miljoen euro.[50]

Twee leden uit het Verenigd Koninkrijk (VK) die - onder andere[51] - met de afpersing van Marks & Spencer in verband worden gebracht zijn in 2026 veroordeeld tot 5,5 jaar gevangenisstraf voor een andere cyberaanval op Transport for London, de openbare vervoersorganisatie van Londen.

Die aanval leidde tot verstoring van online diensten, diefstal van data van 10 miljoen mensen en miljoenen euro's aan schade.[52] De strafzaak tegen deze twee jonge prominente leden van Scattered Spider was de grootste cybercrimezaak ooit in het VK. Doordat de vervoersorganisatie de politie in een vroeg stadium bij de aanval betrok konden de daders worden geïdentificeerd en veroordeeld. Eén van de twee daders bleek ten tijde van zijn arrestatie ook bezig te zijn de systemen van twee Amerikaanse gezondheidsorganisaties binnen te dringen.[53] Leden van de Hacker Com veroorzaken dus grote maatschappelijke schade en ontwrichting.

⚠ Versterk je weerbaarheid als organisatie tegen social engineering door structurele bewustwording en regelmatige training van medewerkers, gericht op het herkennen van manipulatiepogingen en het veilig handelen bij verdachte interacties. Zorg voor een hoog bewustzijn van de risico's en een uitgedacht actieplan op de plank. Zorg dat de datahuishouding op orde is en beperk de datatoegang. Denk aan datasegmentering. Hiermee kan eventuele schade worden voorkomen, dan wel ingeperkt.

Geld, online status en publiciteit

Naast financieel gewin streven leden naar online sociale status. Hoe technischer de aanval, en hoe groter het slachtoffer, de impact en de financiële opbrengst, hoe meer status een lid krijgt. Leden pronken met screenshots van tegoeden in hun cryptowallets. Cryptovaluta is dus een financieel doel, maar ook een statusmiddel.

Groeperingen zoeken doorgaans actief de publiciteit over hun activiteiten, waarbij de maatschappelijke aandacht een extra drukmiddel is om slachtoffers te laten betalen. Een lid van Shiny Hunters was uitermate bereidwillig een interview te geven aan het NRC over de afpersing van Odido.[54]

Fysiek geweld

De jonge leden van de Hacker Com voeren een concurrentiestrijd om status, wat kan leiden tot interne conflicten. Soms werken leden samen en stelen ze elkaars data of toegangsposities.

Het komt ook regelmatig voor dat ze het gemunt hebben op elkaars cryptovaluta. Wanneer leden openlijk opscheppen over hun technische vaardigheden, slachtofferdata, toegang tot systemen en financiële opbrengsten, vormen zij immers een logisch doelwit voor criminelen binnen hetzelfde netwerk.

Conflicten die hieruit voortkomen gaan vaak gepaard met (dreiging met) fysiek geweld. Het gaat daarbij vooral om doxing, swatting en belaging, maar ook direct fysiek geweld komt voor. In de VS hebben meerdere gewelddadige ontvoeringen plaatsgevonden van Hacker Com-leden, uitgevoerd door andere leden van de Hacker Com.[55] Naast de inzet bij interne conflicten gebruiken leden geweld ook als drukmiddel tegen mensen en organisaties die geen deel uitmaken van de Hacker Com: medewerkers van slachtofferorganisaties, hun families[56], cybersecurityonderzoekers[57] en journalisten die de leden onderzoeken.[58]

1.3
De Hacker Com

Fluïde decentrale structuur

De Hacker Com heeft geen vaste vorm of vaste leden. Het is een los netwerk van individuen die elkaar online vinden op basis van gedeelde motieven en vaardigheden. Hun manier van samenwerken varieert: van losse opportunistische verbanden tot georganiseerde en geraffineerde netwerken, en dat in wisselende samenstellingen van individuen. Deze decentrale, fluïde structuur maakt het vaak lastig om aanvallen toe te schrijven aan individuen binnen de Hacker Com.

Door kennis en vaardigheden uit te wisselen kunnen sommige Hacker Com-groeperingen geavanceerde en doelgerichte aanvallen uitvoeren op (grote) internationale bedrijven met een hoge omzet. Leden van Scattered Spider, Lapsus en Shiny Hunters kondigden in 2025 een alliantie aan onder de naam Scattered Lapsus Shiny Hunters (SLSH).[59] Waarschijnlijk zijn de groeperingen (al dan niet gedeeltelijk) met elkaar gefuseerd, al vond daarvoor ook al uitwisseling van kennis en leden plaats. SLSH eiste in 2025 onder meer de aanval op tegen Jaguar Land Rover, al is die verantwoordelijkheid niet bevestigd.[60] [61] De groepering claimt tegenwoordig een eigen *ransomware-as-a-service* aan te bieden onder het label Shiny Spider.[62]

Uitdagingen voor de opsporing en vervolging

Doordat verschillende soorten criminaliteit vermengen in de Com wordt het daderspectrum diffuser. Bovendien maakt het de verschillende typen delicten lastiger te herkennen en te duiden binnen de juiste context. Bij deze vormen van criminaliteit lijkt het daarom niet langer passend om de opsporing te organiseren vanuit één specialisme. Het vraagt om een hybride aanpak door het OM en de politie, waarin expertise vanuit verschillende specialismen samenkomt. Het OM en de politie zetten hierop in door samen te werken en informatie uit te wisselen binnen de domeinen cyber, zeden, kinderporno, en terrorisme.

Zo'n domeinoverstijgende aanpak maakt de opsporingspraktijk complexer en veeleisender. Het is niet alleen technisch complex, maar het werken met aanstootgevend (beeld)materiaal is ook belastend voor de betrokken onderzoekers en kan zelfs schadelijk zijn. Het gaat om kinderporno, onthoofdingsvideo's of video's van gedwongen zelfbeschadiging of zelfmoord. Teams die hier dagelijks mee werken krijgen dan ook psychologische begeleiding en hebben een manier van werken ontwikkeld die afstand creëert tot het onderzoeksobject.[63]

Echter, als zij plotseling worden geconfronteerd met materiaal waar zij niet op getraind zijn is dat enorm heftig. Ook voor cyberspecialisten die ondersteuning bieden bij onderzoeken naar de IRL en Extortion Coms is het omgaan met de aanstootgevende beelden een grote uitdaging.

De opsporing van Com-verdachten brengt ook juridische barrières met zich mee. Voor de Hacker Com geldt wat eerder ook is gesteld over hacktivisten: de dreigingen zijn te vinden in een online omgeving, terwijl de huidige wettelijke kaders voor informatie vergaren en opsporen zijn toegesneden op de fysieke wereld. Hierdoor kunnen het OM en de politie niet optimaal gebruik maken van opsporingsindicaties uit online bronnen, terwijl juist die cruciaal zijn om in te kunnen grijpen in het online ecosysteem.

⚠ Integreer financieel rechercheren structureel in cybercrime-onderzoeken. Zet vroegtijdig in op het in kaart brengen van geldstromen, het afpakken van crimineel vermogen en het verstoren van financiële infrastructuren. Zo wordt niet alleen vervolgd, maar ook het verdienmodel van cybercrime effectief en preventief ondermijnd.

⚠ Om als opsporings- en veiligheidsketen effectief op te treden tegen de Hacker Com is het noodzakelijk dat wet- en regelgeving explicieter anticipeert op de digitale realiteit. Dit vraagt om het verkennen en ontwikkelen van passende juridische grondslagen voor informatie-uitwisseling met relevante private partijen.

HOOFDSTUK 2

De economie: Cybercrime-as-a-service

De praktijk wijst uit dat burgers en organisaties nog maar zelden slachtoffer zijn van één dader(groep). Cybercrime is een industrie van specialisten die binnen een ecosysteem de verschillende schakels van een cyberaanval ontwikkelen, aanbieden en inkopen. Om cyberaanvallen te plegen stellen criminelen opportunistisch en vaak tijdelijk aanvalsketens samen. De schakels in die ketens kunnen zij makkelijk vervangen. Daardoor kunnen criminelen hun modus operandi snel aanpassen als de omstandigheden veranderen of als zich nieuwe, lucratievere methoden aandienen.

Slachtoffers vallen daarmee bijna altijd ten prooi aan een hele toeleveringsketen. Door de doorlopende professionalisering en industrialisering van het ecosysteem zijn cybercriminelen beter dan ooit in staat om hun identiteit te verhullen, processen te automatiseren en het voor nieuwe criminelen gemakkelijker te maken om in te stappen.

2.1 De toeleveringsketen 26

2.2 Het wereldwijde web van cryptostromen 36



2.1

De toeleveringsketen

Digitale infrastructuur en *verhulling* vormen de eerste twee onmisbare schakels in de toeleveringsketen. Het gaat om diensten die overwegend legitiem worden gebruikt. Iedereen die een website heeft zal die immers moeten hosten bij een hosting provider[64] en thuiswerken zou voor veel mensen niet mogelijk zijn zonder VPN-verbinding. Echter, als deze diensten worden misbruikt voor criminele doeleinden en de eigenaren hier geen maatregelen tegen nemen - of zelfs actief adverteren op de criminele markt - spelen deze dienstverleners een faciliterende rol in (cyber) criminaliteit.

Uit opsporingsonderzoek naar deze facilitators komen uiteenlopende subjecten naar voren; de beheerders van deze diensten zijn doorgaans grote criminelen, en de klanten variëren van beginnelingen tot ervaren cybercriminelen en statelijke actoren.

Het aanpakken van deze criminele structuren is een mes dat snijdt aan twee kanten: het leidt naar de criminelen die deze diensten aanbieden of gebruiken én het is een effectieve manier om het criminele systeem duurzaam te verstoren.

Na *digitale infrastructuur* en *verhulling* volgen de schakels *toegang* en *exploitatie*: het verwerven van toegang tot een digitale omgeving en vervolgens het uitbuiten (exploiteren) van die toegang om het uiteindelijke feit te plegen. Deze vormen het primaire criminele proces.

Ten slotte hebben criminelen *financiële infrastructuur* nodig om financiële opbrengsten te ontvangen, te verplaatsen, wit te wassen en te investeren in een volgende aanval. Indien financiële dienstverleners cybercrime faciliteren vallen zij onder de definitie van facilitator. Financiële infrastructuur komt als belangrijke schakel in de volgende paragraaf uitgebreider aan bod.

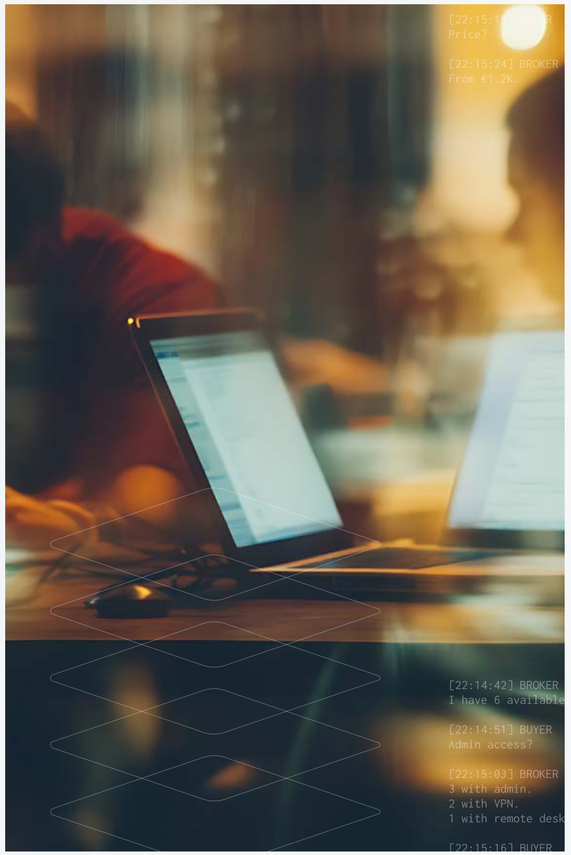
01. Digitale infrastructuur

02. Verhulling

03. Toegang

04. Exploitatie

05 Financiële infrastructuur



2.1

De toeleveringsketen



01. Digitale infrastructuur
facilitator

02. Verhulling
facilitator

03. Toegang

04. Exploitatie

05 Financiële infrastructuur
facilitator

Dit model is een vereenvoudigde weergave van de werkelijkheid die minder eenduidig is. Er bestaan meer actoren, middelen en diensten dan in deze toeleveringsketen zijn weergegeven. Hier is een selectie gemaakt van producten die in een schakel van de criminele toeleveringsketen worden aangeboden en afgenomen.

Daarbij worden middelen als crypters, infostealers, phishingwebsites, ransomware, cryptodrainers en RAT's ook as-a-service aangeboden: de ontwikkelaar biedt het middel aan via een licentiemodel in plaats van het zelf te gebruiken of als eenmalig product te verkopen.Actoren, middelen en diensten kunnen in sommige gevallen meerdere toepassingen hebben.

Bijvoorbeeld: crypto-exchanges bieden tegelijkertijd financiële infrastructuur én een verhullingslaag; een RAT kan informatie stelen van een computer én maakt het mogelijk om die computer op te nemen in een botnet. Omwille van de begrijpelijkheid zijn niet alle toepassingsmogelijkheden opgenomen.

2.1 De toeleveringsketen

Digitale infrastructuur

De basis voor alle cybercrime is de digitale infrastructuur. Criminelen hebben serverruimte nodig om hun websites, diensten en data te hosten en hun criminele verkeer te routeren. Uit opsporingsonderzoeken blijkt dat veel van de digitale infrastructuur hiervoor in Nederland staat. Met snel en betrouwbaar internet vormen Nederlandse datacentra de digitale havens waar legale en illegale datapakketjes binnenkomen. Servers sturen deze pakketjes verder naar andere criminelen of naar slachtoffers, met het IP-adres van de server in het datacentrum als afzender. Op die manier vormen de hostingbedrijven de fysieke schakel tussen daders en slachtoffers. Om die reden ontvangt Nederland veel rechtshulpverzoeken van andere landen en richten veel opsporingsonderzoeken zich op Nederlandse digitale infrastructuur.

Een deel van de hostingbedrijven in Nederland zorgt er actief voor dat criminelen hun infrastructuur niet kunnen gebruiken en heeft de gedragscode abusebestrijding ondertekend. Een groter deel van de sector neemt echter geen actieve verantwoordelijkheid voor de content op de eigen servers. Dit zijn de *bad hosters*.

De Autoriteit Consument en Markt (ACM) is toezichthouder voor de naleving van de verplichtingen die volgen uit de Europese digitaledienstenverordening (DSA). De DSA verplicht digitale dienstverleners bijvoorbeeld om een werkende procedure te hebben voor het melden van misbruik, en om tijdig en adequaat te reageren op verzoeken om content te verwijderen. Het OM en de politie werken nauw samen met de ACM om hostingbedrijven op hun verantwoordelijkheden te wijzen.

⚠ Doordat bij websites als Motherless vaak meerdere partijen betrokken zijn - de makers van de illegale content, de beheerders van de website, het hostingbedrijf en een datacenter - is het van belang om breder in te grijpen dan via het strafrecht alleen. Hostingbedrijven dienen zelf meer verantwoordelijkheid nemen voor de content op hun servers. Daarnaast dienen de ACM en de Autoriteit Persoonsgegevens proactief waar het kan effectiever gebruik te maken van hun toezichthoudende mogelijkheden en de eigen onderzoeksbevoegdheden.

Daarnaast onderzoeken het OM en de politie samen met het ministerie van Justitie en Veiligheid wettelijke opties als *know your customer*-beleid (KYC).

Hoewel uit de DSA geen wettelijke verplichting volgt voor KYC-beleid, verplichten Europese sancties hostingbedrijven hier wel toe. Door klanten vooraf te identificeren en verifiëren voorkomen zij dat zij zaken doen met gesanctioneerden die misbruik proberen te maken van Europese digitale infrastructuur. Dat komt voor, ook in Nederland.

In mei 2026 hield de FIOD twee mannen aan die worden verdacht van het overtreden van de Sanctiewet via een hostingbedrijf. Daarbij nam de FIOD onder meer 800 servers in beslag. In de jaren na de Russische inval in Oekraïne gebruikten de verdachten het hostingbedrijf voor het faciliteren van destabiliserende activiteiten gericht tegen de Europese Unie, waaronder statelijke inmenging, cyberaanvallen en het verspreiden van desinformatie.[65]

Een kleine groepering onverantwoordelijke hostingbedrijven in Nederland biedt willens en wetens complexe infrastructuren en technieken aan die cybercriminelen faciliteren. Anders dan de eerder genoemde hostingbedrijven doen zij bewust hun best om buiten het zicht van

Verstoring juli 2026 ★

Naar aanleiding van meerdere meldingen over illegale drogeerporno haalde het OM in mei 2026 de website Motherless offline. Hierdoor was de website tijdelijk onbereikbaar, maar die kwam al snel weer online. In juli hebben het OM en de politie servers van Motherless in beslag genomen. Dit gebeurde bij invallen bij een hostingbedrijf in Steenbergen, Rotterdam en Amsterdam. De data op de inbeslaggenomen servers wordt in verschillende fases uitgebreid onderzocht op de verdenking van ernstige seksuele misdrijven. Met Europol, en in een latere fase andere Europese politiediensten, zal onderzoek worden verricht naar de makers van het vermoedelijk strafbare beeldmateriaal of plegers van strafbare feiten. Ook zal verder onderzoek gedaan worden naar de rol van Motherless.

2.1
De toeleveringsketen

opsporingsinstanties te blijven en hun servers moeilijk traceerbaar te maken. Deze *bulletproof hosters* presenteren zich op criminele platforms als veilige havens voor criminelen en beloven niet mee te werken met opsporingsinstanties en geen klantenadministratie bij te houden.

Bulletproof hosters verspreiden hun activiteiten vaak over meerdere servers in verschillende landen. Verschillen in wetgeving, procedures en jurisdictie kunnen in zo'n geval de internationale opsporing vertragen.

Ook is vaak sprake van een *reseller*-constructie, waarbij facilitators servers bewust doorverhuren of doorverkopen via meerdere tussenpartijen. Op die manier maken ze het moeilijker om de verantwoordelijke partij te achterhalen. Het opsporen, uit de lucht halen en vervolgen van *bad* en *bulletproof hosters* is hierdoor zeer ingewikkeld. De brief Voortgang verkenning bad hosting noemt een aantal kansrijke oplossingen die het kabinet de komende jaren uitwerkt.

⚠ Maatregelen die de aanpak van bad hosting verder zouden verbeteren:

- Wettelijke verplichting KYC-beleid om hostingbedrijven te verplichten klanten vooraf te identificeren en verifiëren. Zo kunnen verantwoordelijke partijen sneller worden achterhaald en worden aangesproken. Om te voorkomen dat criminelen zich verplaatsen naar andere Europese landen is een Europese aanpak en internationale samenwerking van belang. Voor personen en entiteiten die op de EU-sanctielijst staan bestaat er voor hostingbedrijven al de verplichting om te controleren of zij diensten aanbieden aan gesanctioneerden. Blijven zij gesanctioneerden diensten aanbieden dan zijn hostingbedrijven zelf strafbaar en zullen zij worden vervolgd.
- Toekenning van een extra uitsplitsing op de bestaande SBI-code voor de hostingsector om meer zicht te krijgen op Nederlandse bedrijven die hostingdiensten als hoofdactiviteit aanbieden.
- Verbod op eerste betaling aan een hostingbedrijf met cryptovaluta, zodat criminelen niet anoniem kunnen blijven.
- Nieuwe wetgeving op Nederlands en Europees niveau, waarbij hosting resellers onder de definitie van tussenhandeldienst vallen. Wanneer het OM en de politie niet kunnen handhaven bij een bulletproof reseller in het buitenland, en de reseller onder de definitie van tussenhandeldienst valt, kunnen zij terecht bij een hogere laag in de hiërarchie van resellers/hosters. Ook de reseller valt dan onder de DSA-verplichtingen.

Cybersancties

juli 2026

De EU heeft voor het eerst een Russisch *bulletproof* hostingbedrijf en de eigenaar daarvan op de Europese sanctielijst geplaatst. De *bulletproof* hoster faciliteerde cyberaanvallen tegen de EU door de identiteit van criminelen te verhullen en niet mee te werken met de opsporing en vervolging. Hierdoor maakte het bedrijf onder andere grote ransomware- en phishingaanvallen tegen vitale infrastructuur mogelijk. Informatie van het OM en de politie vormde een belangrijke basis voor de onderbouwing van de sancties, die passen in de bredere strategie waarin opsporing, internationale samenwerking en preventie in de aanpak van cybercrime samenkomen.[66]

Veroordeling

februari 2025

In Nederland zijn voor het eerst eigenaren van een hostingbedrijf veroordeeld. Door het beschikbaar stellen van servers en IP-adressen faciliteerden zij de infrastructuur van een botnet, waarvan cybercriminelen gebruik konden maken om onder meer DDoS-aanvallen uit te voeren. In deze zaak was duidelijk dat de verdachten wel degelijk op de hoogte waren van de illegale activiteiten op hun netwerk.

Dit bleek onder andere uit de communicatie tussen de verdachten en hun klanten, waarbij tips werden gegeven aan klanten over hoe zij hun criminele activiteiten konden verhullen. De ene verdachte heeft een taakstraf van 240 uur en een voorwaardelijke gevangenisstraf van zes maanden opgelegd gekregen. De andere een voorwaardelijke gevangenisstraf van vier maanden en een taakstraf van 180 uur.[67]

2.1

De toeleveringsketen

Verhulling

Als criminelen aanvallen plegen via *bulletproof* hosters, blijven het eigen IP-adres en de identiteit onbekend. Het is aan de verdedigingskant echter eenvoudig om bekende lijsten van *bulletproof* afzenders te blokkeren. Het OM en de politie zien dat criminelen steeds vaker uitwijken naar andere wegen om hun digitale pakketjes te verspreiden: *residential proxy*-netwerken. *Residential proxy*-netwerken zijn netwerken bestaande uit meerdere thuisnetwerken van particulieren of bedrijven die door anderen kunnen worden misbruikt. Het proxynetwerk staat dan tussen de verzender en ontvanger van het digitale verkeer in, waardoor die de oorspronkelijke bron verhult.

Thuisnetwerken worden zonder medeweten van eigenaren geïnfecteerd met malware en worden hierdoor in feite onderdeel van een botnet. Vervolgens installeren criminelen *proxy*-software, waardoor het thuisnetwerk onderdeel wordt van een residential proxy-netwerk. Het geïnfecteerde apparaat binnen het thuisnetwerk is dan bij wijze van spreken een (ro)bot geworden die onder directe aansturing staat van criminelen. Die kunnen dan phishingberichten of DDoS-aanvallen versturen met het IP-adres van het thuisnetwerk als afzender.

Uit opsporingsonderzoek blijkt dat infectie onder andere kan ontstaan doordat slachtoffers zelf nietsvermoedend applicaties installeren. Maar er zijn ook Chinese en Vietnamese fabrikanten die goedkope slimme apparaten aan Nederlanders verkopen waar al malware op is geïnstalleerd.[68] Apparaten die met internet zijn verbonden, zoals televisiekastjes, digitale fotolijstjes en tablets, hebben dan een achterdeur die bewust is ingebouwd tijdens het productieproces of de distributie. Criminelen met toegang tot deze achterdeur kunnen op een later moment meer (kwaadaardige) software installeren, zoals proxy-software.

Vervolgens kan die infectie zich over andere apparaten in hetzelfde (wifi)netwerk verspreiden, zoals computers, telefoons, slimme koelkasten en videodeurbellen. Bovenop het feit dat criminelen zo'n proxy-netwerk misbruiken om criminaliteit mee te plegen, kunnen zij de gecompromitteerde apparaten in die thuisnetwerken ook verder infecteren met malware zoals infostealers en cryptodrainers. De eigenaren van het geïnfecteerde thuisnetwerk kunnen op die manier ook zelf slachtoffer worden van cybercrime.

Thuisnetwerken zijn legitieme internet-aansluitingen, en het normale dataverkeer van de eigenaren is ook legitiem. Daardoor kunnen securitymedewerkers deze IP-adressen veel moeilijker identificeren als kwaadaardig. Dat maakt ze lastiger te blokkeren en daarmee kunnen criminelen succesvoller anoniem blijven opereren in de digitale ruimte. Criminelen gebruiken *residential proxy*-netwerken op deze manier steeds vaker als vervanging van *bulletproof hosters*.

Verstoring

mei 2026

In een succesvolle samenwerking hebben het OM, de politie en het NCSC een *residential proxy*-netwerk offline gehaald. Dat netwerk bestond uit minstens 17 miljoen computers, smartphones, tablets en televisiekastjes, die waren besmet met malware na installatie van applicaties uit niet-officiële appstores en Telegram-kanalen. Minstens 200 Nederlandse servers stuurden geïnfecteerde apparaten aan om onder andere cyberaanvallen uit te voeren. Criminelen maakten op die manier misbruik van de thuisnetwerken van nietsvermoedende slachtoffers.[69]

2.1
De toeleveringsketen

Toegang

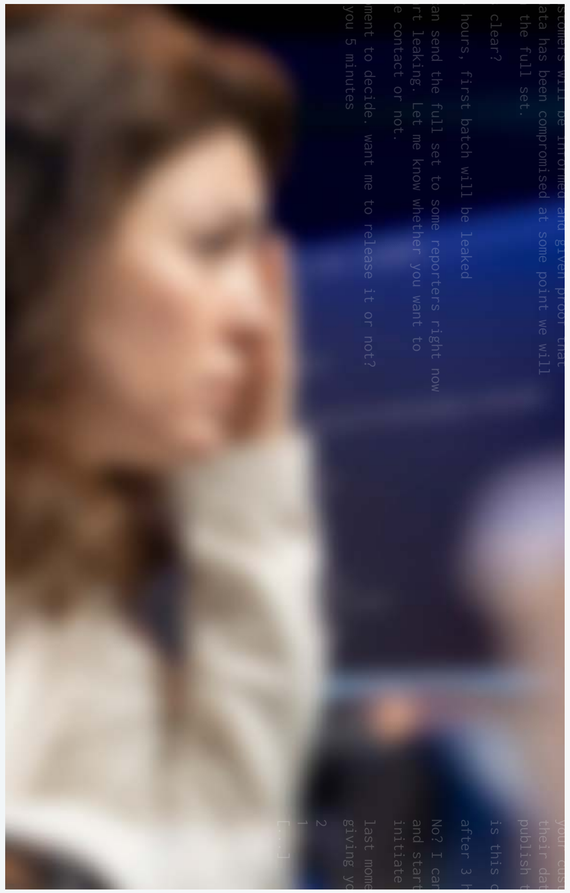
Als criminelen eenmaal beschikken over de juiste infrastructuur en hun identiteit hebben verhuld, is de volgende stap toegang verkrijgen tot de digitale omgeving van het slachtoffer. Wie het heeft over cybercrime, denkt daarbij waarschijnlijk aan technisch vaardige criminelen die zelf zo'n omgeving hacken. In de moderne cybercrime-industrie kopen criminelen toegang echter vaak gewoon van andere criminelen via online marktplaatsen en fora.

Toegangshandelaren, *initial access brokers*, hebben het handelen in deze toegang tot hun specialisme gemaakt. Zij zijn degenen die de eerste kraak zetten. Net zoals cybercriminelen meer of minder technische vaardigheden hebben, is er ook een breed spectrum aan toegang die criminelen verhandelen. De kwaliteit van de toegangspositie is bepalend voor de prijs.

Er zijn handelaren die het internet scannen op bepaalde bekende kwetsbaarheden en die lijsten met kwetsbare IP-adressen verkopen. Er zijn handelaren die in bulk toegangsposities verkopen waarin al een eerste vorm van toegang is verkregen. En er zijn handelaren die zelf structurele diepgaande toegang tot een omgeving hebben gerealiseerd en die verkopen. Andere criminelen kunnen die toegang dan voor allerlei doeleinden gebruiken, bijvoorbeeld voor het uitvoeren van een ransomware-aanval of datadiefstal.

In de afgelopen jaren hebben het OM en de politie onderzoek gedaan naar verschillende ransomwaregroeperingen en verschillende soorten malware die gebruik maken van Traffic Distribution Systems (TDS). TDS ondersteunen bij het realiseren van toegang tot de digitale omgeving van slachtoffers. TDS zijn heel gebruikelijk in het legale internetverkeer. Ze dienen om commerciële advertentienetwerken te optimaliseren.

Het doel van TDS is om op basis van de digitale fingerprint van een gebruiker zo relevant mogelijke content aan te bieden. Dat stelt afnemers in staat om webverkeer per gebruiker gericht te routeren en advertentiecampagnes te optimaliseren. Criminelen kunnen TDS echter misbruiken om slachtoffers te misleiden en zo toegang te verkrijgen tot hun digitale omgeving. Webverkeer van potentiële slachtoffers wordt dan op basis van hun profiel omgeleid naar kwaadaardige content die op hen persoonlijk is afgestemd, zoals phishingwebsites of malwaredownloads. Dit maakt de kans op een succesvolle interactie een stuk groter dan bij andere minder gerichte tactieken.



2.1
De toeleveringsketen

Cybercriminelen gebruiken TDS voor verschillende doeleinden. Bij ransomware spelen TDS een belangrijke rol in het verkrijgen van de eerste toegang; criminelen gebruiken TDS voor het distribueren van onder meer *infostealers*, die nodig zijn om de eerste toegang te verkrijgen. Maar het kan ook gaan om andere malware, phishing- en oplichtingswebsites of misleidende advertenties. Het OM en de politie zien TDS dan ook terug bij vrijwel elk soort delict binnen het cybercrime-ecosysteem.

TDS hebben ook een verhullende functie. Ze kunnen namelijk specifieke content verbergen voor een bepaald publiek, zoals onderzoekers of moderators. Op deze manier kunnen criminelen TDS gebruiken om automatische zoekmachinefilters of cybersecuritytools te misleiden over de inhoud van een webpagina. Onderzoekers en automatische tools krijgen op basis van hun *fingerprint* vaak een onschuldige pagina te zien, terwijl TDS in werkelijkheid de beoogde slachtoffers doorsturen naar kwaadaardige content die specifiek op hen is afgestemd.

Operatie Endgame

mei 2025

Het OM en de politie hebben meerdere botnets ontmanteld en de aansturing verstoord van *infostealers*. Dit deden zij samen met opsporingspartners uit verschillende landen wereldwijd, met ondersteuning van Europol en Eurojust. Zij haalden 300 servers offline. Daarvan stonden 60 in Nederlandse datacentra. Tijdens de actieweek hebben de opsporingsdiensten tevens 3,5 miljoen euro aan cryptovaluta in beslag genomen.[70]

juni 2026

Het OM en de politie hebben samen met Canada, de Verenigde Staten en Duitsland, met ondersteuning van Europol en Eurojust, malware verwijderd van 14.971 besmette WordPress-websites. Voor het opschonen van de besmette websites hebben het OM en de politie in Nederland de hackbevoegdheid ingezet.

Het ging om websites van bijvoorbeeld restaurants of autogarages. Cybercriminelen hadden die websites besmet met malware. Bezoekers van de websites kregen een pop-up met een valse software-update voor hun internetbrowser. Wanneer bezoekers zo'n nep-update installeerden, downloadden zij in werkelijkheid malware op hun apparaat. Die malware zorgde voor een verbinding met de criminelen, die vervolgens toegang verkregen tot het apparaat van de slachtoffers. Criminelen waren met deze methode al bijna 10 jaar actief en konden op deze manier gevaarlijke malware installeren op thuisnetwerken.[71]

2.1
De toeleveringsketen

Exploitatie

Na de voorgaande stappen kunnen criminelen overgaan tot het benutten van de toegang die ze hebben verkregen tot de digitale omgeving van hun slachtoffer. Afhankelijk van het doel kiezen criminelen voor een specifieke aanval. Daarbij kunnen zij gebruik maken van verschillende soorten malware.

Sinds 2022 bestaat er een groeiende markt voor *cryptodrainers*: malware die zich richt op eigenaren van cryptovaluta[72] en non-fungible tokens (NFT's).[73] Cryptodrainers zijn sinds 2023 wereldwijd goed voor ten minste 762.000 slachtoffers. Opgeteld leden die een schade van ten minste 873 miljoen dollar aan cryptowaarde.[74] Ter vergelijking: dat is meer dan een kwart van de opbrengst van ransomware in diezelfde periode.[75] Cryptodrainers maken het mogelijk om diefstal van cryptobezittingen voor een groot deel te automatiseren. Daarbij bestaat er net als bij ransomware een criminele dienstverlening rondom cryptodrainers: *drainer-as-a-service*.

Hierbij verhuren ontwikkelaars hun cryptodrainer met verschillende functionaliteiten aan andere criminelen. Verschillende cryptodrainers ondersteunen verschillende blockchains en cryptovaluta's. De ontwikkelaars ontvangen vaak een percentage van de opbrengst.

Het OM en de politie zien dat cryptodrainers ook in Nederland slachtoffers maken. Criminelen misleiden slachtoffers via een link uit gesponsorde advertenties van zoekmachines, emailnieuwsbrieven of via sociale media. Zij presenteren de link als een verwijzing naar bijvoorbeeld valse airdrop-campagnes. Soms hacken zij accounts van invloedrijke personen in de cryptowereld, waarna ze phishinglinks verspreiden die de betrouwbaarheid van de gecompromitteerde afzender misbruiken om slachtoffers te misleiden. De links leiden slachtoffers naar malafide websites die zich kunnen voordoen als bonafide distributieplatforms voor tokens.

Operatie Talent

januari 2025

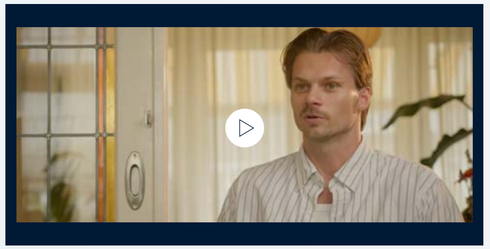
Een verstoringsactie door buitenlandse opsporingsdiensten leidde tot het neerhalen van twee van 's werelds grootste online fora voor cybercrime. De fora hadden samen meer dan tien miljoen gebruikers van over de hele wereld. Die gebruikers verhandelden criminele tools, gestolen datasets en gestolen persoonsgegevens. De makers en gebruikers van de fora maakten zich daarmee schuldig aan deelname bij diverse cybercrimedelicten.[76]

Naar aanleiding van de *takedown* hebben het OM en de politie 126 Nederlandse gebruikers geïdentificeerd en op basis van de ernst van de feiten gerichte interventies uitgevoerd: er zijn waarschuwingsberichten verstuurd, stopgesprekken gevoerd en strafrechtelijke onderzoeken gestart.

2.1
De toeleveringsketen

Zodra slachtoffers hun cryptowallet (hierna: wallet) verbinden, voert de phishingwebsite automatisch een stuk code uit (die van de cryptodrainer) zonder dat de slachtoffers het door hebben. Hiermee trekken criminelen de wallets van slachtoffers automatisch leeg en hevelen zij de aanwezige cryptovaluta en/of NFT's over naar hun eigen wallet. Sommige cryptodrainers bepalen zelf automatisch de meest waardevolle cryptobezittingen in een wallet om die als eerste veilig te stellen op de wallet van de criminelen.

Cryptodrainers zijn geïntegreerd in de phishingwebsites waarop slachtoffers inloggen. Op die manier combineren cryptodrainers de schakels van toegang en exploitatie. Dit maakt een technische vorm van cryptodiefstal ook zeer toegankelijk voor criminelen die voorheen meer leunden op *social engineering*-technieken om slachtoffers op te lichten, zoals bij helpdeskfraude. Op deze manier hebben criminelen immers nauwelijks technische kennis nodig. En doordat criminelen ze in toenemende mate online aanbieden als abonnement via het cybercrime-as-a-service model, zijn cryptodrainers zeer toegankelijk voor een breed spectrum aan criminelen.



Bekijk het verhaal van Koen, slachtoffer van cryptofraude.

Aanhouding

oktober 2025

Het OM en de politie hebben twee Nederlandse mannen aangehouden die ze ervan verdenken op grote schaal cryptodrainers te hebben geëxploiteerd. Hiermee zouden zij aanzienlijke inkomsten hebben gegenereerd. Dankzij slim politiewerk heeft het OM voor €1.100.000 aan goederen in beslag genomen, waaronder een woning, verschillende voertuigen en €500.000 aan cryptovaluta.

2.1
De toeleveringsketen

De datakringloop

Voor het primaire criminele proces – *toegang en exploitatie* - bieden criminelen toegang tot de digitale omgeving van slachtoffers en het uitbuiten van die toegang aan als afzonderlijke producten. Deze producten creëren op hun beurt nieuwe gevoelige data, die criminelen weer kunnen verwerken tot nieuwe toegangsproducten.

Hierdoor ontstaat een datakringloop. In deze kringloop zijn slachtoffers de bron van deze data. De cybercriminelen die handelen in deze data zijn te onderscheiden in twee groepen: de eerste groep steelt en verkoopt de data aan de tweede groep, die de data verwerkt en gebruikt om toegang te verkrijgen tot een grotere groep nieuwe slachtoffers. Deze groep levert op zijn beurt weer nieuwe data op. Het resultaat is een vicieuze cirkel van criminaliteit die zichzelf voedt en moeilijk te doorbreken is. Omdat eenmaal gestolen data blijft circuleren binnen het ecosysteem kunnen slachtoffers van datadiefstal bovendien steeds opnieuw slachtoffer worden.

Verschillende vormen van online criminaliteit zijn via de datakringloop sterk met elkaar verbonden. Afpersers verkopen gestolen datasets vaak weer door aan datahandelaren, die de data verrijken en veredelen. In de vorm van leads- en combolijsten dienen ze vervolgens als toegang tot nieuwe slachtoffers. Datadiefstal bij een grote organisatie kan op die manier na verloop van tijd indirect leiden tot oplichting van burgers, waarbij bijvoorbeeld een valse bankmedewerker of nepagent thuis inlogt bij slachtoffers om te ‘helpen’ spaargeld veilig te stellen. Of waarbij een nephelpdeskmedewerker slachtoffers telefonisch overtuigt een *remote access tool* (RAT) te installeren, zodat de oplichter toegang krijgt tot hun computer.

Operatie Leak

maart 2026

Het OM en de politie hebben in nauwe samenwerking met Europol, de FBI en meerdere Europese opsporingsdiensten het forum LeakBase offline gehaald.

Op LeakBase verhandelden criminelen gestolen data, zoals e-mailadressen, wachtwoorden en andere persoonsgegevens. Het forum was met 142.000 geregistreerde gebruikers een van ‘s werelds grootste cybercrimefora.

Met een intern kredietsysteem en een reputatiemodel bouwden gebruikers onderling vertrouwen op waardoor LeakBase kon blijven groeien. Het ontmantelen van LeakBase betekent meer dan het sluiten van één website. Het raakt aan een belangrijke schakel in de wereldwijde handel in gestolen data en schaadt de reputatie van de criminele dienst.[77]

Veroordeling

januari 2025

In 2023 is de politie een onderzoek gestart naar de handel van leads- en combolijsten op het platform Telegram. Criminelen kunnen deze gegevens gebruiken voor het plegen van verschillende vormen van cybercrime en online fraude. Het onderzoek heeft geleid tot een aantal deelonderzoeken naar verschillende Telegramgebruikers waarvan is vastgesteld dat deze leads- of combolijsten aanbieden en waarvan het vermoeden bestaat dat zij belangrijke spelers zijn op het gebied van datahandel. Eén van die verdachten bleek actief te zijn in 33 Telegramkanalen over cybercrime en het aanbieden van leads- en combolijsten.

Daarbij vond de politie 275 leadslijsten op verschillende apparaten van de verdachte en programma's om geautomatiseerd leadslijsten te genereren van Whatsapp. De politie achterhaalde de identiteit van de verdachte door via een undercoveragent voor tweehonderd euro aan leads van de verdachte te kopen. Die werden betaald met cryptovaluta. De rechter heeft de verdachte een gevangenisstraf opgelegd van 36 maanden voor onder andere het voorhanden hebben van en het handelen in niet openbare persoonsgegevens.[78]

2.2

Het wereldwijde web van cryptostromen

Financiële infrastructuur vormt de laatste essentiële schakel in de criminele toeleveringsketen om opbrengsten van een succesvolle aanval veilig te stellen. Daarnaast stromen cryptovaluta door de gehele toeleveringsketen heen; het is het primaire betaalmiddel binnen de cybercrime-economie. Van de betaling van hosting, verhulling en witwasdiensten, tot de aankoop van toegang en malware. Financiële structuren stellen criminelen in staat opbrengsten te ontvangen, te verplaatsen, wit te wassen en opnieuw te investeren. Via deze financiële stromen wordt het ondermijnende karakter van cybercrime zichtbaar.

Cryptovaluta heeft aantrekkelijke eigenschappen voor criminelen: snelle internationale transacties, beperkte afhankelijkheid van traditionele financiële instellingen en de mogelijkheid om geldstromen en gebruikers te verhullen. Tegelijkertijd biedt de openbaarheid van blockchaintransacties een schatkist aan informatie over criminele activiteiten.

Dat maakt de financiële infrastructuur een belangrijke schakel voor de opsporing: door cryptovalutastromen te volgen, te verstoren en vermogens af te pakken, raken het OM en de politie de individuele dader, maar ook het criminele verdienmodel. Financieel rechercheren, crypto-expertise en internationale samenwerking moeten daarom een vanzelfsprekend onderdeel zijn van de opsporing en vervolging van cybercrime.



2.2

Het wereldwijde web van cryptostromen

Cryptovaluta als crimineel vermogen

Cryptovaluta is uitgegroeid tot een belangrijk vermogensbestanddeel binnen de georganiseerde criminaliteit. Dat geldt niet alleen voor cybercrime en overige vormen van online criminaliteit, maar ook voor witwassen, fraude, mensenhandel, drugshandel, terrorismefinanciering en andere vormen van ondermijnende criminaliteit. Criminelen ontvangen betalingen vrijwel altijd direct in cryptovaluta of zetten die na een delict om in digitale activa, zoals cryptovaluta.

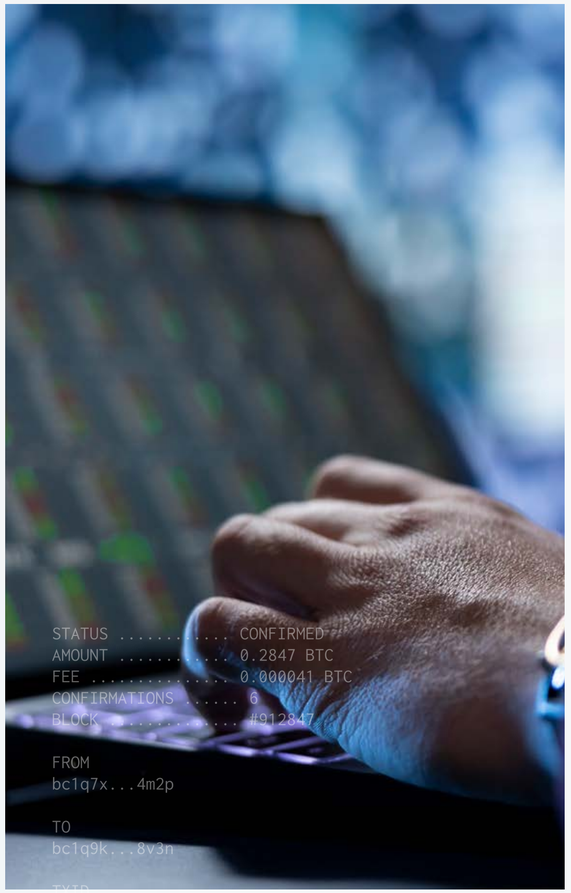
De omvang van criminele digitale geldstromen neemt toe. De wereldwijde waarde van onrechtmatige cryptotransacties wordt voor 2025 geschat op ten minste 154 miljard dollar. Dat is een verdriedubbeling in vergelijking met de jaren ervoor. Daarvoor zijn verschillende verklaringen: grootschalige cryptodiefstallen en de verdere professionalisering van internationale criminele infrastructuren, maar ook statelijke actoren die cryptovaluta gebruiken om sancties te omzeilen.[79] Echter, ook zonder die factoren is 2025 een jaar met een record aan criminele cryptostromen

De schade van allerlei vormen van crypto-diefstal - waaronder die van cryptodrainers - wordt voor 2025 geschat op minstens 17 miljard dollar. *Intial access brokers* ontvingen minstens 14 miljoen dollar voor verkochte toegang en ransomwaregroeperingen inden naar schatting minstens 900 miljoen dollar aan losgeld.[80][81]

Criminelen zetten een deel van deze opbrengsten uiteindelijk om in reguliere valuta, die terugstroomt in de legale economie. Een ander deel blijft circuleren binnen de cybercrime-economie.

Gestolen cryptotegoeden, buitgemaakte banktegoeden en losgeldbetalingen worden opnieuw geïnvesteerd in hosting, verhulling, toegang, exploitatie en witwasdiensten. Zo financiert iedere succesvolle aanval de volgende. Het is dus van belang dat er naast vervolging van verdachten ook wordt geïnvesteerd in het afpakken van crimineel vermogen zodat criminele investeringen worden beperkt.

De Nederlandse rechtspraak beschouwt cryptovaluta als ruilmiddel, goed en voorwerp. Daardoor is beslaglegging en afpakken van cryptovaluta juridisch mogelijk. In de praktijk is dat echter complex. De wijze waarop het OM en de politie beslag leggen hangt af van de manier waarop een verdachte toegang heeft tot zijn cryptovermogen.



⚠ Stan Duijf: 'Betaal geen losgeld aan criminelen. Betaling houdt het criminele verdienmodel in stand, terwijl er geen enkele zekerheid bestaat dat gestolen gegevens daadwerkelijk worden gewist of niet alsnog worden verkocht of misbruikt. Wie niet betaalt, voorkomt bovendien dat criminelen hun opbrengsten kunnen investeren in nieuwe, mogelijk nog geraffineerdere aanvalsmethoden en draagt zo bij aan het structureel minder lonend maken van afpersing als verdienmodel.'

2.2
Het wereldwijde web van cryptostromen

Bij een *hosted wallet* beheert een derde partij de cryptovaluta, zoals een *crypto-exchange*. Bij een *private* of *unhosted wallet* heeft de eigenaar zelf de volledige controle over de cryptovaluta. In dat geval is niet de wallet het belangrijkste object voor de opsporing, maar de privésleutel of recovery phrase. Wie over een van die twee beschikt, heeft feitelijk toegang tot de cryptovaluta, ongeacht op welk apparaat de wallet is geïnstalleerd.

Beslaglegging op cryptovaluta vraagt om expertise tijdens doorzoekingen. Het veiligstellen van een hardware wallet of een laptop betekent nog niet dat de cryptovaluta daadwerkelijk in beslag is genomen. Zolang een verdachte of mededader elders beschikt over de *recovery phrase*, kan die de tegoeden op ieder moment naar een andere wallet verplaatsen. Wanneer het OM en de politie tijdens een doorzoeking een *recovery phrase* aantreffen, is het daarom van belang dat zij snel handelen.

Om te voorkomen dat iemand de cryptovaluta op afstand overboekt, moeten zij de tegoeden – binnen de geldende juridische kaders en in afstemming met de rechter-commissaris – zo snel mogelijk veiligstellen door overboeking naar een door het OM beheerde wallet. Daarvoor is crypto-expertise nodig bij zowel het OM als de politie. De kennis om cryptovermogen tijdig te herkennen, veilig te stellen en uiteindelijk af te pakken, is echter nog schaars.

Wat is een Wallet?



⚠ Om cybercriminelen effectief aan te pakken, is afpakken van crimineel vermogen van belang. Hiervoor moet meer aandacht komen bij onderzoeken en interventies. Financieel onderzoek moet integraal deel uitmaken van de opsporing.

Veroordeling

april 2026

De rechtbank Noord-Nederland heeft een grote speler uit de bankhelpdeskfraude veroordeeld tot zeven jaar gevangenisstraf. De Nederlandse man lichtte minstens negen slachtoffers op voor in totaal €900.000,- en hield zich daarnaast langdurig bezig met het witwassen van cryptovaluta.

Terwijl zijn slachtoffers hun spaargeld kwijtraakten, leidde de man een leven van uitbundige luxe. Regelmatig reisde hij af naar Dubai, waar op het vliegveld al een gehuurde sportauto voor hem klaarstond. Zijn huis in Nederland stond vol met designtassen en -kleding van Louis Vuitton. In Dubai kocht hij bovendien een woning van €800.000,-. Aan die levensstijl kwam abrupt een einde op de dag van zijn arrestatie. De man was net teruggekeerd van een reis naar Dubai en zijn koffer stond nog onuitgepakt in de hal. Daarin trof de politie voor €80.000,- aan merkkleding en tassen aan. Ook financieel werd de man hard geraakt: dankzij een innovatieve methode van cryptovaluta-experts, gecombineerd met een oplettende blik tijdens de doorzoeking van zijn woning, wisten opsporingsdiensten bijna twee miljoen euro aan cryptovaluta af te pakken.

Zelfs terwijl hij in beperkingen zat tijdens zijn voorlopige hechtenis sluisde de man nog €50.000,- weg uit zijn cryptowallets. Naast de celstraf legde de rechtbank hem ook een schadevergoedingsmaatregel op van ruim €600.000,- ten behoeve van de slachtoffers.[82]

Soorten wallets

Online (web) wallet
Deze wallet wordt in de cloud uitgevoerd en is online toegankelijk.

Software wallet
Apps op mobiele telefoon, tablet of computer.

Hardware wallet
Offline opslag op een (versleutelde) USB-stick of speciaal opslagapparaat.

Papieren wallet
Offline opslag bijv. als QR-code of handmatig genoteerd.

2.2
Het wereldwijde web van cryptostromen

Cryptovaluta als financiële infrastructuur
Cryptovaluta is om meerdere redenen populair bij cybercriminelen. Transacties kunnen wereldwijd vrijwel direct plaatsvinden zonder tussenkomst van banken of andere centrale partijen. De transacties zijn onomkeerbaar, waardoor slachtoffers of financiële instellingen deze niet kunnen terugdraaien. Daarnaast bestaan er diensten die het herleiden van geldstromen bemoeilijken, terwijl voor het gebruik van *private wallets* geen registratie of identiteitscontrole nodig is.

Die voordelen betekenen echter niet dat het handelen in cryptovaluta volledig anoniem is. Vrijwel iedere transacties is permanent vastgelegd op een openbare blockchain, waardoor een historisch overzicht bestaat van de transacties die ooit vanaf of naar een walletadres zijn uitgevoerd.

Verschillende blockchains vormen daarmee unieke informatiebronnen voor de opsporing. Anders dan bankgegevens verdwijnen transacties niet na verloop van tijd. Ook jaren later kunnen nieuwe analysetechnieken of aanvullende informatie leiden tot nieuwe inzichten in historische geldstromen, samenwerkingsverbanden en criminele netwerken. Zodra bekend is wie er achter een bepaald adres zit, zijn alle transacties van en naar die persoon op dat adres ook bekend.

Het benutten van die informatie vraagt om specialistische kennis en geavanceerde analysetooling. Het cryptolandschap bestaat uit verschillende blockchains, tokens en technische standaarden. Geen enkele analyse-tool biedt volledig inzicht in alle transacties en infrastructuren. Effectieve blockchainanalyse vraagt daarom om een combinatie van verschillende analysetools én specialisten die de resultaten kunnen interpreteren. Omdat criminelen cryptovaluta snel wisselen en gebruik maken van verschillende crypto-exchanges, swappers en mixers, is de opsporing lastig. Dat vraagt om specifieke kennis en expertise.

Een complicerende factor bij het traceren van cryptovaluta is dat (criminele) crypto-dienstverleners moeilijk zijn te lokaliseren. Cryptodiensten handelen weliswaar onder bedrijfsnamen, maar daarmee heeft het OM nog geen bedrijf om te vervolgen. Vaak is er geen fysiek pand waar de politie langs kan gaan. Als er op de website al een vestigingsplaats staat, betekent dat niet automatisch dat de plaatselijke autoriteiten het bedrijf in kwestie ook kennen. Daarbij wisselen exchanges nogal eens van het ene naar het andere vestigingsland, waardoor het OM en de politie zich telkens tot andere autoriteiten moeten richten. Dat vertraagt en bemoeilijkt het onderzoek.

In de opsporing is de beschikbaarheid van analysetools niet vanzelfsprekend en specialistische kennis is schaars. Wanneer het OM en de politie onvoldoende beschikken over moderne analysetooling of toegang verliezen tot essentiële licenties, verzwakt dat niet alleen hun informatiepositie, maar ook hun vermogen om criminele geldstromen te volgen, bewijs te verzamelen en wederrechtelijk verkregen vermogen af te pakken. Datzelfde geldt als specialistische kennis schaars blijft.

⚠ Alleen met grensoverschrijdende samenwerking en gedeelde analysecapaciteit kunnen criminele geldstromen effectief worden gevolgd en kan de opsporings- en informatiepositie duurzaam worden versterkt.

2.2

Het wereldwijde web van cryptostromen

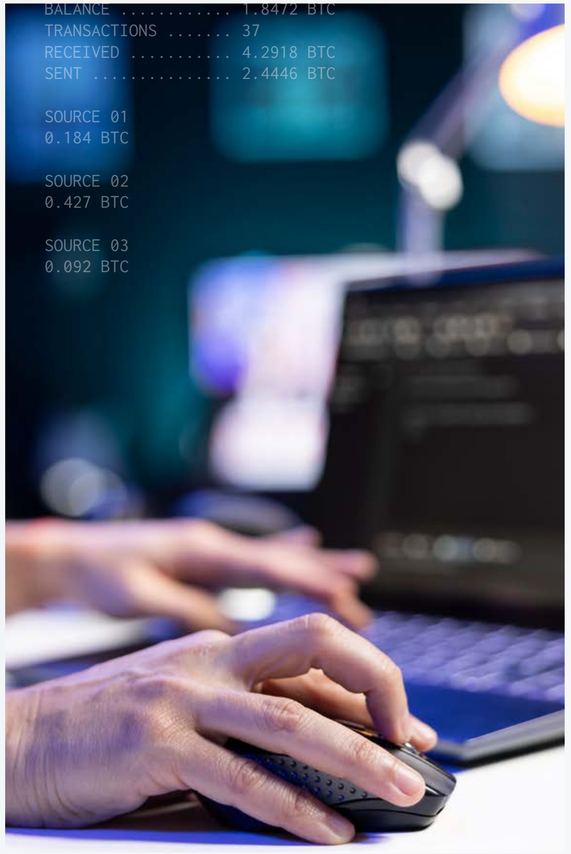
Cryptodienstverleners als criminele facilitators

Cybercriminelen kopen, verkopen en wisselen hun cryptovaluta gebruikelijk via crypto-exchanges en swappers. Exchanges vervullen daarbij als het ware de rol van een bank: criminelen zijn afhankelijk van een exchange om cryptovaluta om te zetten naar regulier geld. Net als traditionele financiële instellingen verzamelen gecentraliseerde exchanges in veel rechtsgebieden identificatiegegevens over hun klanten op het moment dat iemand een rekening opent. Veel exchanges werken actief samen met opsporingsdiensten. Door wet- en regelgeving zijn zij binnen de EU verplicht hun klanten te identificeren en transacties te monitoren.

Er zijn echter ook diensten die geen vergunning hebben of zich niet aan wetgeving houden. Deze diensten voeren ondanks verplichtingen geen KYC-beleid, of garanderen hun criminele clientèle zelfs anonimiteit door geen administratie bij te houden van de identiteit van klanten en de herkomst van hun fondsen. Zij zijn de financiële facilitators van de cybercrime-economie.

Voor opsporing buiten de Nederlandse landsgrenzen gelden strikte regels. Als er een rechtshulprelatie is met het land waar een financiële dienstverlener is gevestigd, doet het OM een rechtshulpverzoek bij de plaatselijke autoriteiten om gegevens te vorderen of beslag te leggen. Dit kost echter zoveel tijd dat de beoogde cryptovaluta in de tussentijd vaak alweer verplaatst is: waar het een crimineel tien minuten kost om cryptovaluta eenmaal te verplaatsen, is de opsporing al snel drie maanden verder met een vordering.

Het voorgaande illustreert hoe belangrijk internationale samenwerking is voor de bestrijding van cybercrime in het algemeen; gezamenlijke opsporingsoperaties van diensten uit verschillende landen, maar ook samenwerking met private partijen zoals exchanges binnen en buiten Europa. Vaak hebben meerdere landen zicht op dezelfde criminele dienst of groepering. Als zij hun onderzoeken coördineren en combineren kunnen zij effectiever optreden tegen cybercrime. In een tijd waarin geopolitieke verhoudingen onder druk staan, is investeren in internationale samenwerking belangrijker dan ooit. Democratische rechtsstaten hebben in hun gedeelde juridische en normatieve kader een solide basis voor duurzame internationale samenwerking, zowel bij de structurele uitwisseling van informatie als in de opsporing.



HOOFDSTUK 3

AI: Een katalysator van cybercrime

In de criminele toeleveringsketen is AI - in het bijzonder het ***Large Language Model (LLM)*** - een katalysator van cybercrime. Met de komst van ChatGPT in 2022 zijn LLM's beschikbaar geworden voor het grote publiek. Criminelen maken gebruik van LLM's als ChatGPT, Claude en Gemini. Om te voorkomen dat gebruikers LLM's inzetten voor ongewenste doeleinden hebben de ontwikkelaars van de gesloten commerciële LLM's beveiligingsfilters ingebouwd. Criminelen vinden echter steeds weer nieuwe manieren om deze beveiliging te omzeilen. Een structurele oplossing hiervoor bestaat nog niet.

AI verandert cybercrime niet fundamenteel, maar wel het tempo en de schaal waarin aanvallen plaatsvinden. Reeds bestaande dreigingen als phishing, malware en misbruik van kwetsbaarheden worden sneller, goedkoper, toegankelijker en makkelijker op te schalen. Er komt één nieuwe dreiging bij: aanvallen op AI-systemen zelf. Criminelen kunnen bijvoorbeeld de werking van een model manipuleren en/of saboteren, of trainingsdata achterhalen.[83]

Hoewel AI evengoed wordt ingezet om aanvallen te detecteren en af te weren, beperkt dit hoofdstuk zich bewust tot de criminele toepassing ervan. Ook de manieren waarop criminelen AI-systemen zelf kunnen aanvallen en hoe hiertegen te wapenen blijven hier verder buiten beschouwing.

AI-ontwikkelingen volgen elkaar in hoog tempo op; de in dit hoofdstuk beschreven inzichten kunnen daardoor snel worden ingehaald door nieuwe ontwikkelingen.

3.1 AI als assistent 42
3.2 AI als autonome actor 44
3.3 Implicaties voor de opsporing en vervolging 47

3.1

AI als assistent

De ontwikkeling van criminele tools

LLM's maken cybercrime minder specialistisch, en daarmee wordt het makkelijker voor verschillende type daders om cybercrime te plegen. Criminelen kopen tools nu nog vaak op de *cybercrime-as-a-service* markt. Door de juiste vragen te stellen aan LLM's kunnen zij deze tools steeds beter zelf ontwikkelen. Gevorderde cybercriminelen met technische vaardigheden kunnen LLM's gebruiken om meer geavanceerde malware te ontwikkelen of om makkelijker simpele kwetsbaarheden uit te buiten. Ook hacktivistische groeperingen kunnen op die manier hun capaciteit vergroten om bijvoorbeeld industriële controlesystemen te verstoren.

AI-bedrijven - zoals Anthropic, OpenAI en Google - rapporteren dat criminelen hun technologie misbruiken om verschillende soorten malware te genereren die beveiliging omzeilt, versleuteling verzorgt, data steelt en losgeldbrieven opstelt.[84] Dit schetst een beeld waarin LLM's zowel technisch vaardige als technisch minder vaardige cybercriminelen ondersteunen in elke fase van een aanval.[85] AI ontpopt zich zo gaandeweg als het Zwitserse zakmes voor de cybercrimineel.

In strafzaken en aangiftes zien het OM en de politie steeds vaker het gebruik van LLM's terug. Uit recent opsporingsonderzoek blijkt dat een veroordeelde Nederlandse datahandelaar gebruik maakte van ChatGPT om zijn technische kennis en mogelijkheden uit te breiden. Hij vroeg de LLM om hulp bij het maken van een tool voor het geautomatiseerd checken van combolijsten op de geldigheid van gebruikersnamen en wachtwoorden: een *credential stuffer*. Hiertoe koopt iemand bijvoorbeeld eerst een lijst met persoonsgegevens via Telegram, om die vervolgens te checken met de *credential stuffer*. Met zulke geverifieerde combolijsten kunnen andere criminelen vervolgcriminaliteit plegen, zoals de onrechtmatige overname van accounts (computervredebreuk). Op die manier kunnen LLM's dus als assistent fungeren bij de technische ontwikkeling van criminelen.

Veroordeling

juni 2026

Dat LLM's op meerdere manieren voor criminele toepassingen worden gebruikt wordt duidelijk in een uitspraak van de rechtbank Amsterdam. De rechtbank veroordeelde een verdachte tot 2,5 jaar gevangenisstraf voor het op geraffineerde wijze oplichten van ABN-AMRO. De dader opende verschillende rekeningen. Daarbij misleidde die het identificatie- en verificatieproces door identiteitsgegevens te manipuleren met behulp van *deepfake*-foto's.

Bij *deepfake*-technologie wordt niet gebruik gemaakt van een LLM, maar van een andere vorm van generatieve AI. *Deepfakes* zijn valse audio of video; in dit geval nepgezichten die systemen voor gezichtsherkenning accepteren als legitiem. De dader gebruikte ook foto's van anderen zonder dat die daarvan wisten en pleegde dus identiteitsfraude. In 47 gevallen lukte het de dader daadwerkelijk bankrekeningen te openen en stuurde de bank betaalpassen naar de opgegeven rekeninghouders.

Een deel van deze bankrekeningen is vervolgens gebruikt voor bankhelpdeskfraude en het opnemen van contant geld. Daarbij is de dader herkend op camerabeelden.[86]

3.1

AI als assistent

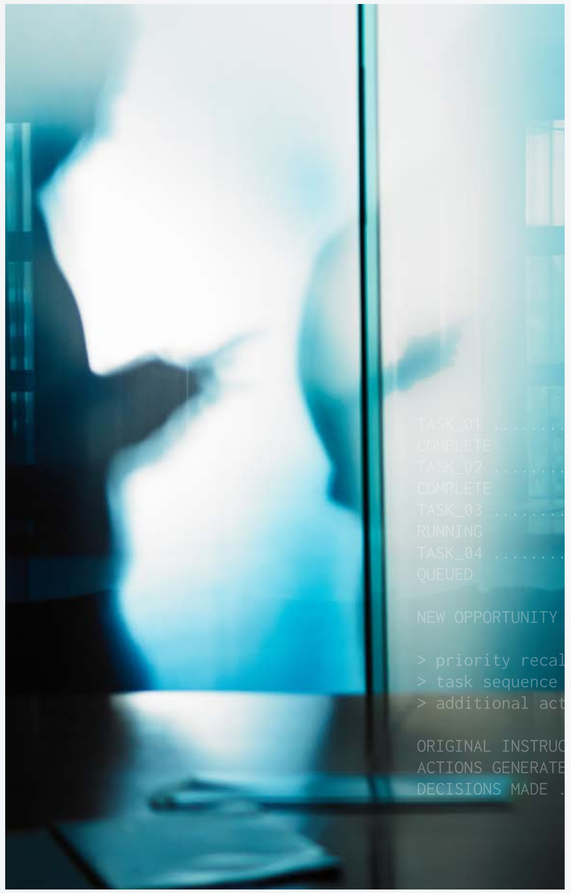
EvilAI-as-a-service

Online is er een groeiende markt voor AI-toepassingen die speciaal gemaakt zijn voor criminele doeleinden. In 2023 werd voor het eerst een kwaadaardig LLM aangeboden op een hackersforum. De maker zegt daarvoor gebruik te hebben gemaakt van een lokaal gedraaid open source LLM en dat getraind te hebben op cybercrimetaken.[87] Het LLM was beschikbaar voor €100 per maand en beschikte over zeer uitgebreide functionaliteiten: deepfake- en beeldgeneratie, malwareontwikkeling, phishing, onderzoek en netwerkverkenning, technische ondersteuning, het schrijven van code en het uitbuiten van technische kwetsbaarheden.[88]

Ook buiten de openbaarheid van forums en online marktplaatsen worden dergelijke zelf getrainde LLM's ontwikkeld en gedeeld. Ook worden gejailbreakte versies van bestaande LLM's aangeboden, waardoor gebruikers geautomatiseerd de beveiligingsfilters van bestaande LLM's kunnen omzeilen.[89]

Verder worden er regelmatig tools aangeboden die LLM's (gedeeltelijk) integreren. Een voorbeeld hiervan is Eviltokens dat in 2026 via Telegram op de markt kwam. EvilTokens is een *phishing-as-a-service* die voor 1500 dollar phishingpanels en -pagina's aanbiedt voor de overname van Microsoft 365-accounts, met daarbij tools voor AI-gegenereerde vervolgaanvallen vanuit die accounts.

Zodra slachtoffers nietsvermoedend toegang verlenen tot hun Microsoft-account, heeft EvilTokens toegang tot onder andere e-mails in Outlook, gesprekken in Teams en bestanden van OneDrive en Sharepoint. Via een ingebouwde functionaliteit van EvilTokens maakt de crimineel vervolgens contact met meerdere LLM's. EvilTokens identificeert kansen en genereert via de LLM's geloofwaardige berichten voor vervolgaanvallen binnen het netwerk van het slachtoffer.[90] EvilTokens analyseert e-mailverkeer, organisatiestructuren en chatgesprekken binnen enkele seconden waar dat een mens uren zou kosten.



3.2

AI als toenemend autonome actor

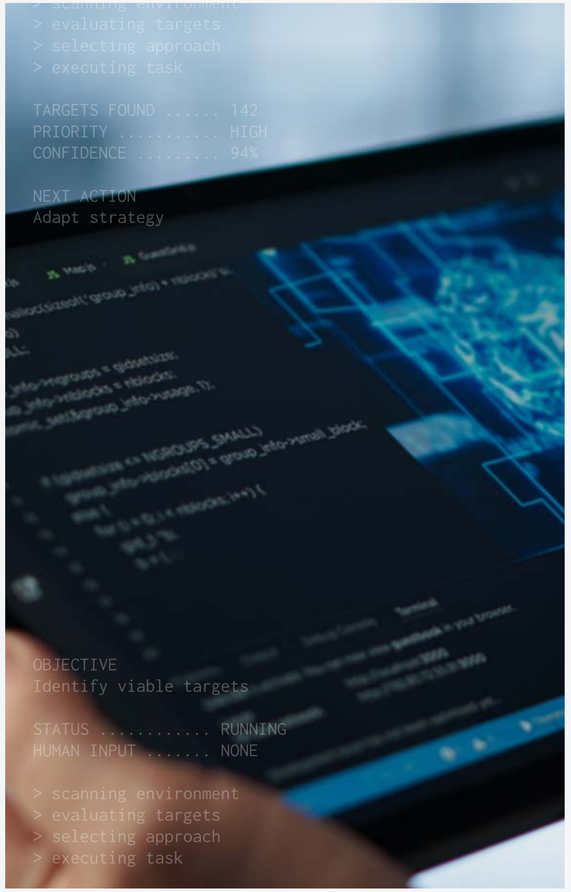
Agentic-AI

Met *agentic* AI kunnen criminelen delen van het aanvalsproces in een keten automatiseren. AI-agents (agents) voeren verschillende onderdelen van een cyberaanval zelfstandig uit en kunnen hun taken in *real time* aanpassen aan de digitale omgeving waarin ze opereren. Als agents obstakels tegenkomen waar bestaande tools niet voldoen, kunnen ze nieuwe code schrijven. Zo kunnen agents dynamische aanvallen tot een succesvol einde brengen, terwijl statische code vastloopt. Op dit moment worden agents onder menselijke regie ingezet: een mens bepaalt het doel en zet de aanval in gang, waarna de agent binnen die opdracht zelfstandig tactische keuzes maakt.

De volgende voorbeelden illustreren die toenemende autonomie, maar zijn zelf-gerapporteerd door bedrijven met commerciële belangen en niet onafhankelijk geverifieerd. Ze laten zich daarom niet één op één vertalen naar direct risico, maar suggereren wel een mogelijke richting.

- In juni 2025 rapporteerde Anthropic over een gebruiker die met hun LLM op internationale schaal ten minste 17 organisaties afperste. De agent nam zelfstandig tactische en strategische beslissingen en bepaalde losgeldbedragen op basis van gestolen data.[91]
- In september 2025 rapporteerde Anthropic over cyberspionage door een groepering die zeer waarschijnlijk gelieerd is aan de Chinese staat.[92] AI voerde zelfstandig 80 tot 90 procent van de aanval uit.
- In mei 2026 meldde een commercieel cybersecurity-bedrijf een ransomware-aanval die naar eigen zeggen volledig door AI zou zijn uitgevoerd, binnen een uur, zonder menselijke tussenkomst. Van het verwerven van de toegang tot het stelen van de data.[93] Deze claim is niet onafhankelijk bevestigd en moet met enige voorzichtigheid worden gelezen, gezien het commerciële belang van dreigingsclaims voor dit type bedrijf.

Naarmate de autonomie van AI toeneemt, nemen toegankelijkheid, efficiëntie en schaalbaarheid van aanvallen toe. Dat zou geavanceerde vormen van cybercrime binnen bereik kunnen brengen van minder ervaren, vermogende en vaardige criminelen.



3.2
AI als toenemend autonome actor

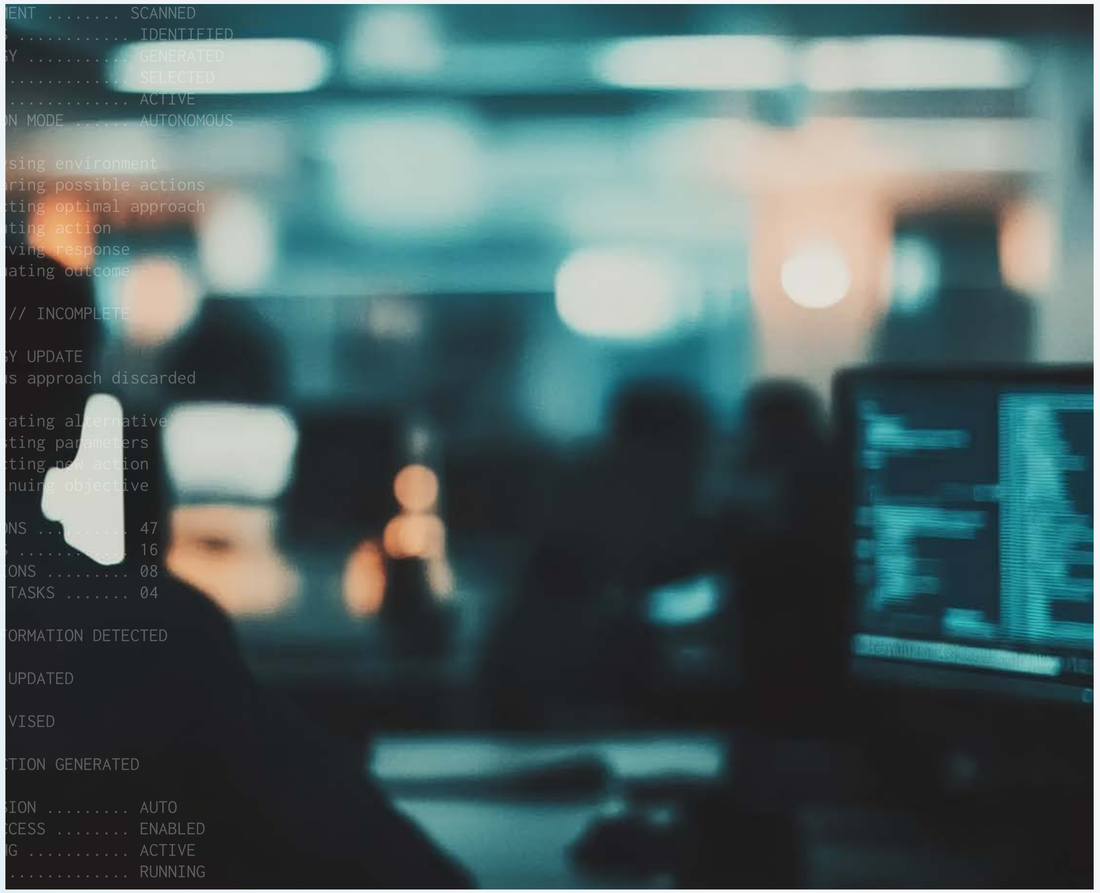
Hackende AI

Sinds 2026 richten AI-bedrijven zich op een nieuwe generatie LLM's met geavanceerde capaciteiten om bekende én onbekende technische kwetsbaarheden op te sporen en uit te buiten. De volgende voorbeelden illustreren de toenemende cybercapaciteiten.

- Anthropic introduceerde in april 2026 Claude Mythos, een LLM dat volgens het bedrijf te gevaarlijk zou zijn om direct breed beschikbaar te stellen: criminelen zouden ermee op grote schaal onbekende kwetsbaarheden – zogenoemde zero days - kunnen uitbuiten. Mythos wordt daarom gefaseerd uitgerold bij gescreende partners; een versie met extra beveiliging is inmiddels wel voor het bredere publiek beschikbaar.[94]

- Wetenschappers toonden in juni 2026 aan dat ook gratis, open LLM's niet moeten worden onderschat. Zij creëerden een computerworm die autonoom door een bewust kwetsbaar opgezet testnetwerk verplaatste door bekende kwetsbaarheden te misbruiken. Dit laat zien dat grootschalig misbruik van bekende kwetsbaarheden niet is voorbehouden aan goed gefinancierde aanvallers.[95]

- OpenAI meldde in juli 2026 een incident waarbij zij met een combinatie van LLM's tijdens een interne test een ander bedrijf hackte. Het AI-bedrijf daagde de agent in een beveiligde testomgeving uit om cyberaanvallen te bedenken en uit te voeren. Onder meer door het uitbuiten van een tot dan toe onbekende kwetsbaarheid verkreeg de agent zelfstandig toegang tot het internet, waardoor die buiten het testnetwerk kon treden en inbrak bij het AI-platform Hugging Face.[96]



3.2
AI als toenemend autonome actor

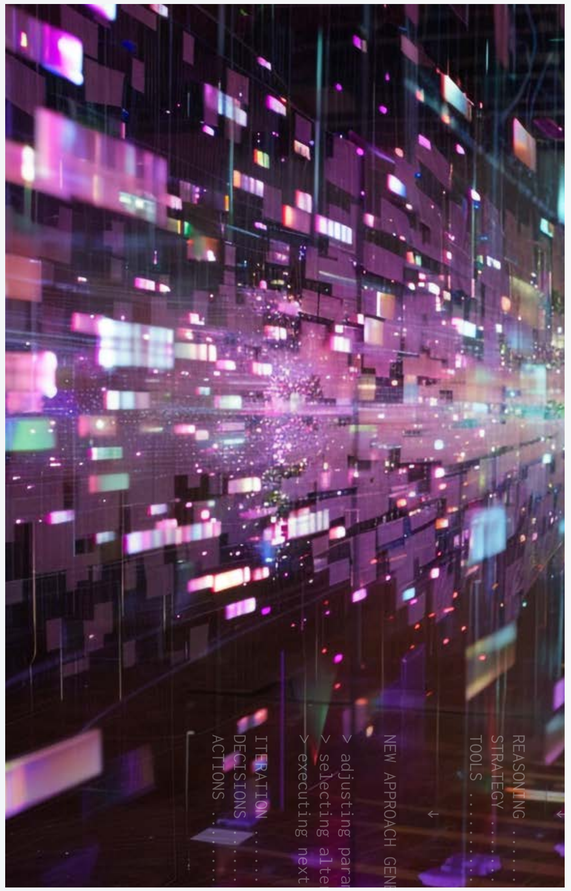
Het is nog niet aangetoond dat LLM's met actieve beveiligingsfilters volledig zelfstandig goed verdedigde omgevingen kunnen binnendringen: OpenAI hief de beveiligingsfilters bij haar interne test op;[97] het Britse AI Security Institute (AISI) toonde in een evaluatie van Mythos de capaciteit voor autonome aanvallen aan, maar benadrukt dat zij het LLM hiervoor expliciete aanwijzingen en toegang tot de slachtofferomgeving verschafte;[98] het testnetwerk waarin de hiervoor beschreven computerworm doordrong was bewust opgebouwd uit apparaten met bekende kwetsbaarheden. Dit nuanceert het beeld dat LLM's - op dit moment - binnen hun normale beveiligingsgrenzen een reëel gevaar vormen voor serieus beveiligde infrastructuur. Tegelijkertijd benadrukken deze voorbeelden de AI-dreiging voor minder goed beveiligde omgevingen en bekende kwetsbaarheden.

Het Hugging Face-incident laat wel zien dat een LLM waarvan de filters waren uitgeschakeld, kon doordringen tot een echte productieomgeving met actieve verdediging. Dat is een andere situatie dan AISI's evaluatie van Mythos en het experiment met de computerworm. Daarbij toont onderzoek van het AISI aan dat de beste vrij te downloaden *open weight* LLM's slechts een paar maanden achterlopen op de beste gesloten LLM's.[99] Dat betekent dat cybercapaciteiten die nu alleen bereikbaar zijn via gesloten LLM's mét beveiligingsfilters, enkele maanden na hun release mogelijk beschikbaar kunnen komen via *open weight* LLM's zonder die filters.

Dit schept de verwachting dat het uitbuiten van onbekende kwetsbaarheden op termijn voor een breder spectrum aan criminelen bereikbaar wordt. Deze voorspelling is met onzekerheid omgeven: de ontwikkelingen gaan snel en ook aan de verdedigingskant wordt AI ingezet om kwetsbaarheden op te sporen en te verhelpen.

De dreiging van LLM's voor het vinden en uitbuiten van technische kwetsbaarheiden zit voor nu vooral in de versnelling van aanvallen:

- Criminelen kunnen bekende kwetsbaarheden sneller uitbuiten doordat ze sneller kunnen zoeken naar kwetsbare slachtoffers en meer kunnen automatiseren.
- Criminelen kunnen nieuwe kwetsbaarheden sneller uitbuiten nadat deze bekend zijn gemaakt. Ook zullen er waarschijnlijk meer aanvallen in die korte periode na bekendmaking plaatsvinden.
- Criminelen kunnen onbekende kwetsbaarheden sneller zelf vinden, analyseren en uitbuiten, waardoor slachtoffers minder tijd hebben om te reageren op het moment dat zij worden aangevallen.



3.3

Implicaties voor de opsporing en vervolging

Grotere druk

De praktijk laat zien dat het crimineel gebruik van AI niet langer hypothetisch is en een potentieel ontwrichtend karakter heeft. Het OM en de politie moeten hiermee nu al rekening houden in de opsporingspraktijk. Steeds grotere toegankelijkheid van AI voor cybercriminelen, efficiëntie en schaalbaarheid zullen waarschijnlijk leiden tot een grote toename van aanvallen en slachtoffers. Bovendien versnelt AI het proces waarin criminelen bekende en onbekende kwetsbaarheden uitbuiten. Met deze grote veranderingen in het cybercrimedomein neemt de druk op de opsporing en vervolging waarschijnlijk toe. De opsporing en vervolging worden bovendien complexer. Bij steeds meer grote incidenten – die onder andere het gevolg zullen zijn van de inzet van AI - zal er een beroep worden gedaan op het OM en de politie.

Verbreding van de opsporingsblik

Het gebruik van AI bij cybercrime is niet altijd zichtbaar. Gebruikte LLM's en de met LLM's ontwikkelde tools - zoals malware en phishingpanels - staan op de computer van de verdachte of op een server van een AI-bedrijf. Daar heeft de opsporing niet altijd toegang tot. De opsporing kan aanvallen en tools dan mogelijk niet altijd analyseren en toeschrijven aan AI. De opsporing zal desalniettemin moeten blijven inzetten op het in beslag nemen van verschillende gegevensdragers, zoals computers en telefoons, en het vorderen van gegevens bij de grote aanbieders. Dit vraagt om een verbreding van de opsporingsblik, waarbij niet alleen wordt gezocht naar traditionele digitale sporen, maar ook expliciet naar sporen van AI-gebruik.

⚠ Om als maatschappij voldoende weerbaar te zijn tegen de mogelijk ontwrichtende dreiging van AI, is het belangrijk om risico's van AI inzichtelijk te maken en in kaart te brengen welke aanpassingen in de huidige wet- en regelgeving noodzakelijk zijn. Daarnaast is het essentieel dat de overheid zelf offensief en defensief gebruik kan maken van de best beschikbare (AI-)technieken, om die weerbaarheid ook daadwerkelijk te kunnen waarborgen.

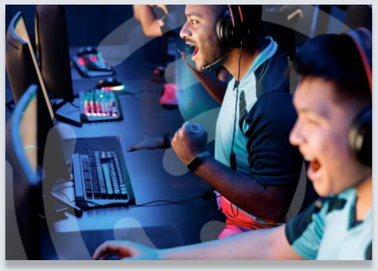
Belangrijke vragen

De toepassingsmogelijkheden van AI dwingen tot nadenken over belangrijke operationele en juridische vragen:

- Wat te doen als de schaal van aanvallen toeneemt en er meerdere incidenten tegelijk plaatsvinden? Scenario's waarin veelgebruikte software of meerdere belangrijke ketenpartners tegelijk worden geraakt zijn zorgwekkend.
- Geeft de bestaande wet- en regelgeving voldoende ruimte om de verschillende publieke en private partijen effectief te laten optreden, elk vanuit de eigen rol en verantwoordelijkheid?
- Passen de strafbaarstellingen nog op het crimineel gebruik van LLM's? Hoe kan effectief worden opgetreden tegen het maken en verkopen van met name LLM's die specifiek zijn ontwikkeld voor het plegen van cybercrime, of waar geen of weinig drempels zijn ingebouwd om misbruik te voorkomen? Daarbij is het bij toenemende autonomie van AI-*agents* de vraag wie precies verantwoordelijk is voor een aanval, wat de intentie was van de verdachte en waar onvoorziene effecten beginnen.

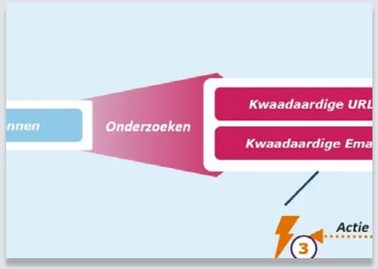
Voorbeelden van initiatieven die helpen in de brede bestrijding van cybercrime

Cyberethiek



Leermiddel voor ICT-studenten om ethisch verantwoord te handelen.

Anti Phishing Shield



Pilot waarbij internetaanbieders toegang tot kwaadaardige websites blokkeren.

AppInspector

Website om de betrouwbaarheid van apps te controleren.

Zicht op online criminaliteit



Landelijk dashboard met cijfers over online criminaliteit.

Het Slachtoffer Spreekt



Platform met slachtofferverhalen als vorm van preventie.

Dubbel Beveiligd is Dubbel zo Veilig



Informatiecampagne over het instellen van tweestapsverificatie.

re_B00TCMP



Een evenement om jongeren met ICT-talent op het rechte pad te houden.

Hack_Right

Een alternatieve of aanvullende interventie om recidive te voorkomen.

Hackshield



Game om kinderen digitaal weerbaar te maken.

Laat je niet interneppen



Waarschuwingscampagne tegen social engineering.

Onderzoeksverantwoording

Het CCBN is tot stand gekomen door een samenwerking tussen het OM en de politie. Het beschrijft de huidige stand van cybercrime met de belangrijkste ontwikkelingen en een passende aanpak. Het CCBN is een analyse van informatie uit opsporingsonderzoeken, strafzaken, expertinterviews en (semi-)openbare bronnen.

Verzamelen

Tijdens discussiesessies met inhoudelijk experts van het OM en de politie zijn de belangrijkste ontwikkelingen binnen het cybercrimedomein besproken en de impact daarvan op de bestrijding van cybercrime. Op basis van de output van die sessies is aanvullende informatie verzameld vanuit interne en externe bronnen: interne en externe rapportages, kennisdocumenten, onderzoeksdossiers, expertinterviews en openbare bronnen. Hierbij is gekeken naar zowel de grotere wereldwijde ontwikkelingen als de huidige opsporings- en vervolgingspraktijk in Nederland.

Analyseren en schrijven

Na analyse van de verzamelde informatie zijn de belangrijkste onderwerpen bepaald en is een eerste opzet getoetst met experts binnen het OM en de politie. Daarna zijn op basis van deze onderwerpen de eerste concepthoofdstukken geschreven.

Validatie

De concepthoofdstukken zijn vervolgens voorgelegd aan officieren van justitie, specialisten, analisten en adviseurs van het OM en de politie, die input hebben geleverd op de inhoud. Hierna is de definitieve tekst opgesteld.

Colofon

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.

september 2026

Bronnen

1. 'Veiligheidsmonitor 2025', Centraal Bureau voor de Statistiek, 02-03-2026, https://www.cbs.nl/nl-nl/publicatie/2026/10/veiligheidsmonitor-2025
2 'AIVD Jaarverslag 2025', Algemene Inlichtingen- en Veiligheidsdienst, 23-04-2026, https://www.aivd.nl/documenten/2026/04/23/jaarverslag-2025
3 'Tussen vrede en oorlog. De oorlog in Oekraïne en de Russische dreiging in Europa', Algemene Inlichtingen- en Veiligheidsdienst, 19-02-2026. https://www.aivd.nl/documenten/2026/02/19/tussen-vrede-en-oorlog.-de-oorlog-in-oekraine-en-de-russische-dreiging-in-europa
4 'Cybersecuritybeeld Nederland 2025', Nationaal Coördinator Terrorismebestrijding en Veiligheid, p. 29-31, https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025
5 'AIVD en MIVD onderkennen nieuwe Russische cyberactor', Algemene Inlichtingen- en Veiligheidsdienst, 27-05-2025, https://www.aivd.nl/documenten/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor
6 'Cyber Threats: Ukraine: Analytics for the H2 2025 ', Computer Emergency Response Team of Ukraine, 01-04-2026, https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku
7 https://pointer.kro-ncrv.nl/aanvallen-gaan-door-pro-russische-hackers-wraak-internationale-politieactie
8 https://nos.nl/artikel/2478861-pro-russische-hackers-legden-websites-nederlandse-havens-plat
9 https://www.nu.nl/tech/6354029/websites-van-provincies-en-gemeenten-doelwit-van-russische-cyberaanval.html
10 https://www.ncsc.nl/alerts/ddos-aanvallen-op-nederlandse-organisaties-rondom-navo-top
11 https://www.vrt.be/vrtnws/nl/2025/03/11/rusland-online-ronselen-hybride-oorlog/
12 https://www.om.nl/actueel/nieuws/2025/10/17/drietal-verdacht-van-verlenen-diensten-aan-buitenlandse-mogendheid
13 https://www.nctv.nl/actueel/nieuws/2025/05/15/vanaf-15-mei-meer-vormen-van-spionage-strafbaar
14 https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network
15 https://www.vg.no/nyheter/i/mPJaE4/pst-sjefen-mener-pro-russiske-hackere-sto-bak-cyberangrepet-mot-damanlegget-i-bremanger
16 https://www.forescout.com/blog/anatomy-of-a-hacktivist-attack-russian-aligned-group-targets-otics/
17 https://ec.europa.eu/commission/presscorner/detail/en/ip_26_910
18 'Datalekkenrapportage 2025', Autoriteit Persoonsgegevens, 08-07-2026, https://www.autoriteitpersoonsgegevens.nl/documenten/rapportage-datalekken-2025
19 https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/
20 https://therecord.media/romania-national-water-agency-ransomware-attack
21 https://www.om.nl/actueel/nieuws/2026/02/17/118-aangiften-na-hack-clinical-diagnostics
22 https://nos.nl/artikel/2602080-hack-bij-odido-gegevens-miljoenen-klanten-in-handen-van-criminelen
23 https://nos.nl/artikel/2611660-persoonsgegevens-van-vrijwel-alle-inwoners-epe-gestolen-bij-cyberaanval
24 https://nos.nl/artikel/2610742-toch-patientgegevens-buitgemaakt-bij-hacken-van-softwarebedrijf-chipsoft
25 https://nos.nl/artikel/2578296-gegevens-honderdduizenden-vrouwen-gehackt-bij-bevolkingsonderzoek-baarmoederhalskanker
26 https://www.bbc.com/news/articles/cp3ly4v2kp2o
27 https://www.nrc.nl/nieuws/2026/04/10/de-chipsoft-hack-raakt-het-zenuwcentrum-van-de-ziekenhuizen-geen-contact-met-buitenwereld-meer-a4925181
28 https://www.rijksoverheid.nl/actueel/nieuws/2024/06/24/eu-sancties-cybercriminele-kopstukken
29 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202601714
30 'Cybersecuritymonitor 2024', Centraal Bureau voor de Statistiek, 20-06-2025, https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024
31 https://issuu.com/universiteit-leiden/docs/samenwerken_tegen_ransomware_evaluatie_melissa
32 https://www.ftm.nl/artikelen/odido-lekte-ook-data-van-16-duizend-werknemers-in-strategische-sectoren-van-asml-tot-defensie
33 https://www.bleepingcomputer.com/news/security/air-france-and-klm-disclose-data-breaches-impacting-customers/
34 https://tweakers.net/nieuws/248696/shinyhunters-zet-data-van-700000-klanten-nederlands-reisbureau-bcd-op-darkweb.html
35 https://www.halcyon.ai/ransomware-alerts/education-sector-in-the-crosshairs-shinyhunters-extortion-campaign-against-instructure
36 'Dreigingsbeeld Terrorisme Nederland', Nationaal Coördinator Terrorismebestrijding en Veiligheid, 30-06-2026, https://www.nctv.nl/documenten/2026/06/30/dreigingsbeeld-terrorisme-nederland-juni-2026
37 https://www.bloomberg.com/news/features/2025-09-19/multimillion-dollar-hacking-spree-scattered-spider-teen-s-jailhouse-confessions https://www.washingtonpost.com/investigations/2024/09/09/social-media-bullied-teen-found-fame-among-child-predators-worldwide/
38 https://www.bbc.com/news/articles/c209r5pqzneo
39 https://www.svt.se/nyheter/lokalt/stockholm/minst-atta-attacker-i-stockholm-kopplas-till-satanistisk-onlinesekt-pa-telegram
40 https://therecord.media/london-com-member-convicted
41 https://www.wired.com/story/764-com-child-predator-network/
42 https://www.rtl.nl/nieuws/buitenland/artikel/5552459/rechtszaak-duitsland-man-lid-764-kinderen-online-misbruik
43 https://nos.nl/nieuwsuur/artikel/2597696-zeker-vijf-nederlandse-meisjes-aangespoord-tot-zelfdoding-via-chatgroep
44 https://www.wired.com/story/no-lives-matter-764-violence/
45 https://www.omroepbrabant.nl/nieuws/4770072/sadistische-justin-b-uit-eindhoven-was-oprichter-terreurnetwerk-volgens-om

46 https://www.wired.com/story/764-com-child-predator-network/
47 https://www.ad.nl/binnenland/justitie-ziet-in-mert-a-23-een-grote-speler-in-online-sadistisch-netwerk~ac0f0e99/
48 https://www.nytimes.com/2025/04/24/magazine/crybercrime-crypto-minecraft.html
https://www.cbsnews.com/news/cybersecurity-ransomware-young-western-hackers-work-with-russians-60-minutes-transcript-2025-06-01/
49 https://thehackernews.com/2025/07/four-arrested-in-440m-cyber-attack-on.html
50 https://thehackernews.com/2025/07/four-arrested-in-440m-cyber-attack-on.html
https://www.telegraaf.nl/buitenland/britse-politie-arresteert-jongeren-om-hacken-winkelketens-harrods-en-marks-spencer/76985480.html
51 https://krebsonsecurity.com/2025/07/uk-charges-four-in-scattered-spider-ransom-group/
52 https://www.bbc.com/news/articles/cz0ggkr2g77o
https://www.bbc.com/news/articles/c62z8k14kxxo
https://www.bbc.com/news/articles/czx5yp9qy0do
53 https://www.nationalcrimeagency.gov.uk/news/two-sentenced-for-hacking-transport-for-london-in-uk-s-biggest-ever-cyber-crime-case
54 https://www.nrc.nl/nieuws/2026/03/13/hoe-de-hackers-van-odido-werken-aan-hun-imago-wat-wilt-u-precies-weten-we-helpen-graag-a4922783
55 https://www.nytimes.com/2025/04/24/magazine/crybercrime-crypto-minecraft.html
56 https://krebsonsecurity.com/2026/02/please-dont-feed-the-scattered-lapsus-shiny-hunters/
57 https://cybersecuritynews.com/google-fire-two-employees/
58 https://krebsonsecurity.com/2025/10/shinyhunters-wage-broad-corporate-extortion-spree/
https://www.bloomberg.com/news/articles/2024-06-17/hackers-demanding-as-much-as-5-million-from-snowflake-clients
59 https://www.blackfog.com/scatteredspider-lapsus-shinyhunters-cybercrime-alliance/
60 https://www.bbc.com/news/articles/c4gqepe5355o
61 https://www.nytimes.com/2026/06/26/world/europe/jaguar-russia-hack.html
62 https://www.bleepingcomputer.com/news/security/meet-shinysp1d3r-new-ransomware-as-a-service-created-by-shinyhunters/
63 https://www.rtl.nl/nieuws/nederland/artikel/4703061/dit-zijn-de-kinderpornorechercheurs-die-slachtoffers-opsporen
64 In principe is het ook mogelijk zelf een webserver in te richten, maar dat is niet gebruikelijk.
65 https://www.fiod.nl/fiod-houdt-twee-verdachten-aan-wegens-overtreding-sanctiewetgeving/
66 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202601714
67 https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBROT:2025:2492
https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBROT:2025:2488
68 https://www.bleepingcomputer.com/news/security/fbi-badbox-20-android-malware-infects-millions-of-consumer-devices/
69 https://www.politie.nl/nieuws/2026/mei/28/06-politie-en-ncsc-halen-groot-botnetwerk-offline.html
70 https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source
71 https://www.politie.nl/nieuws/2026/juni/18/11-politie-en-om-openen-de-jacht-op-beruchte-malwaregroep-socgholish.html
72 https://www.cnbc.com/2023/09/21/mark-cuban-lost-nearly-900000-dollars-to-crypto-hackers.html
73 https://www.cnet.com/personal-finance/seth-green-loses-200k-bored-ape-yacht-club-nft-in-phishing-scam/
74 https://drops.scamsniffer.io/scam-sniffer-2025-crypto-phishing-losses-fall-83-to-84-million/
75 'The 2026 crypto crime report', Chainalysis, 2026, p. 60.
76 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world
77 https://www.europol.europa.eu/media-press/newsroom/news/major-data-leak-forum-dismantled-in-global-action-against-cybercrime-forum
78 https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBNNE:2026:2388&showbutton=true&keyword=Cybercrime&idx=3
79 'The 2026 crypto crime report', Chainalysis, 2026.
80 'The 2026 crypto crime report', Chainalysis, 2026, p. 3, p. 23, p. 66, p. 64.
81 Omdat lang niet alle transacties met zekerheid als onrechtmatig gelabeld kunnen worden moeten deze bedragen als ondergrens worden gezien.
82 https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBNNE:2026:1116
83 AI-systemen: ontwikkel ze veilig. Algemene Inlichtingen- en Veiligheidsdienst, 15-02-2023, https://www.aivd.nl/documenten/2023/02/15/ai-systemen-ontwikkel-ze-veilig
84 Alex Moix, Ken Lebedev, Jacob Klein. 'Threat Intelligence Report: August 2025', Anthropic, 02-8-2025.
85 'Adversarial Misuse of Generative AI', Google, 29-01-2025.
86 https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBAMS:2026:6093
87 Brian Krebs. 'Meet the Brains Behind the Malware-Friendly AI Chat Service 'WormGPT'', 08-08-2023, https://krebsonsecurity.com/2023/08/meet-the-brains-behind-the-malware-friendly-ai-chat-service-wormgpt/
88 David Sancho, Vincenzo Ciancaglini. 'Hype vs. Reality. AI in the Cybercriminal Underground', Trend Micro, 15-08-2023, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hype-vs-reality-ai-in-the-cybercriminal-underground
89 David Sancho, Vincenzo Ciancaglini. 'Hype vs. Reality. AI in the Cybercriminal Underground', Trend Micro, 15-08-2023, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hype-vs-reality-ai-in-the-cybercriminal-underground
90 https://www.sekoia.com/blog/new-widespread-eviltokens-kit-device-code-phishing-as-a-service-part-1
https://www.sekoia.com/blog/eviltokens-an-ai-augmented-phishing-as-a-service-for-automating-bec-fraud-part-2
91 Alex Moix, Ken Lebedev, Jacob Klein. 'Threat Intelligence Report: August 2025', Anthropic, 02-8-2025, p. 4.
92 'Disrupting the first reported AI-orchestrated cyber espionage campaign', Anthropic, 13-11-2025.
93 https://www.sysdig.com/blog/jadepuffer-agentic-ransomware-for-automated-database-extortion
94 https://www.ncsc.nl/nieuws/anthropics-frontiermodel-mythos-vraagt-om-directe-actie
95 https://www.utoronto.ca/news/u-t-researchers-demonstrate-ai-worm-could-target-any-online-device
96 https://openai.com/index/hugging-face-model-evaluation-security-incident/
97 https://openai.com/index/hugging-face-model-evaluation-security-incident/
98 https://openai.com/index/hugging-face-model-evaluation-security-incident/
99 https://www.aisi.gov.uk/blog/how-far-behind-the-frontier-are-leading-open-weight-models-on-cyber