Van : Programma Digitale Veiligheid en Cybercrime
Aan : Bestuurlijke werkgroep Digitale veiligheid en cybercrime
Datum : 4 november 2025
Onderwerp : Jaarplan 2026
Status : Eindversie

JAARPLAN

Inhoud van dit document
Dit is het (regionale) jaarplan voor 2026 op het thema Digitale veiligheid en cybercrime van gemeenten, OM en politie in Midden-Nederland. Eerst wordt beknopt omschreven wat de huidige situatie is, vervolgens wordt de regionale ambitie omschreven en wordt per doel concreet gemaakt welke acties we op die doelstelling gaan oppakken. Deze acties worden verder uitgewerkt in bijlage 1. Een terugblik op de voortgang in 2025 staat uitgewerkt in bijlage 2.

Wat is er aan de hand?

Een van de keerzijden van digitalisering is de opkomst van cybercrime en gedigitaliseerde criminaliteit. De digitale infrastructuur heeft de wereld verkleind tot binnen enkele klikken: daders kunnen online op grote schaal slachtoffers maken. Dit vraagt om een fundamenteel andere aanpak van criminaliteit. Geografische grenzen doen er steeds minder toe; online criminaliteit is grenzeloos en schaalbaar. Daders opereren wereldwijd, waardoor samenwerking over eenheids- en landsgrenzen heen noodzakelijk is om hen te stoppen. Tegelijkertijd speelt dit probleem ook dichtbij huis: slachtoffers én daders wonen in onze dorpen en steden. Daarom is het niet alleen zaak om landelijk samen te werken, maar juist ook lokaal digitale criminaliteit te voorkomen en te bestrijden.

Tegelijkertijd blijft het lastig om grip te krijgen op de omvang van het probleem. We weten dat digitale onveiligheid zich moeilijk laat vertalen in eenduidige cijfers. Dit komt onder meer door het hoge dark number: veel slachtoffers doen geen aangifte, vaak uit schaamte of omdat ze niet weten waar ze terechtkunnen. Per delictsvorm zijn er grote verschillen in aangiftebereidheid. Uit onderzoek van het CBS blijkt dat in 2024 2,4 miljoen Nederlanders in aanraking zijn geweest met online criminaliteit. Slechts 17% van de slachtoffers heeft hiervan melding en aangifte gedaan bij de politie. 48% melde dit bij een andere instantie, zoals de bank. Zonder volledig beeld kunnen veiligheidspartners hun rol minder goed pakken, terwijl juist dat nodig is om inwoners en ondernemers digitaal veilig te houden.

Online criminaliteit zal blijven toenemen en de verwevenheid met andere veiligheidsthema's (zoals ondermijning) wordt steeds groter. Europol (2025) stelt niet voor niets dat "the internet has become the primary theatre for organised crime." Criminele netwerken gebruiken (onze) digitale infrastructuur om uiteenlopende vormen van georganiseerde criminaliteit ongezien te kunnen plegen: van cyberfraude en ransomware tot witwassen. Het bezit van data zal voor de toekomst een steeds belangrijke rol spelen, het is "a new currency of power – stolen, traded and exploited by criminal actors." (Europol, 2025). Kortom, digitale veiligheid kan niet langer worden gezien als op zichzelf staand thema; het moet worden geïntegreerd in de visies en werkwijzen van andere (bestaande) thema's en domeinen.

Technologische ontwikkelingen zullen de komende jaren grote invloed hebben op online criminaliteit. Zo wordt Kunstmatige Intelligentie (AI) steeds meer ingezet als hulpmiddel om online criminaliteit te plegen, waardoor technische kennis is niet (meer) nodig om online criminaliteit te kunnen plegen (Politie, 2024). Daarnaast wordt het door AI voor inwoners steeds moeilijker om echt van nep te onderscheiden, wat een ondermijnend effect heeft op het vertrouwen in de samenleving. Ook de opkomst van quantumtechnologie zal grote impact hebben in de toekomst. Enerzijds maakt deze ontwikkeling het moeilijk data te beveiliging tegen kwaadwillenden, wat fundamentele veranderingen zal vragen van informatiebeveiliging van inwoners, ondernemers en eigen organisaties. Anderzijds biedt quantum nieuwe kansen: zo wordt bijvoorbeeld het detecteren van en anticiperen op bedreigingen nauwkeuriger en sneller.

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl

De complexiteit en verwevenheid van online criminaliteit vragen daarom niet alleen om landelijke samenwerking, maar juist ook om lokale regie, domein overstijgend werken en handelingsbekwaamheid van professionals. Alleen zo kunnen we inwoners beter beschermen, slachtoffers beter ondersteunen en daders effectiever voorkomen en aanpakken.

Wat willen we bereiken?

De ambitie voor 2023-2026 is (in het DIN, zie bijlage 3) als volgt geformuleerd: in Midden-Nederland gaan we slachtoffer- en daderschap van gedigitaliseerde criminaliteit en cybercrime voorkomen en daders hiervan pakken. Hiertoe hebben we kundige(re) professionals nodig voor wie integraal samenwerken tussen gemeenten, politie en OM vanzelfsprekend is. Data wordt gebruikt om capaciteit gericht in te zetten. De potentiële slachtoffers en daders worden weerbaar tegen gedigitaliseerde criminaliteit en cybercrime.

Bovenstaande ambitie is geoperationaliseerd in een vijftal operationele doelen.

1. Integraal sturen vindt plaats op basis van een informatiebeeld.
2. Slachtoffers hebben een hogere meldings- en aangiftebereidheid.
3. Onze professionals zijn bewust en bekwaam ten aanzien van DV&CC.
4. Effectiever (voorkomen en) aanpakken van daders.
5. Onze inwoners weten beter hoe ze hun slachtofferkans kunnen verkleinen.

Wat gaan we daarvoor doen in 2026?

In 2026 bouwen we voort op wat in 2025 in gang is gezet. De terugblik op 2025 staat opgenomen in bijlage 2. Omdat veel ontwikkelingen meerjarig zijn, bevat dit jaarplan geen grote koerswijzigingen. Tegelijk zijn er een aantal ontwikkelingen die invloed hebben op de focus van onze inzet in 2026, namelijk:

1. 2026 is het laatste jaar van de Regionale Veiligheidsstrategie. In 2026 zal de nieuwe veiligheidsstrategie geschreven worden. We gaan ons voorbereiden op de mogelijke doorontwikkeling van het thema en het borgen van de ingezette ontwikkelingen (zoals de werkwijze rondom informatiegestuurd werken, het CISO netwerk, de samenwerking met het RIEC).
2. Digitale weerbaarheid en veiligheid wordt steeds minder beschouwd als op zichzelf staand, maar geïntegreerd in andere thema's. Dit wil zeggen dat ook collega's buiten OOV in toenemende mate de verantwoordelijkheid pakken om online criminaliteit tegen te gaan. Daarnaast wordt (lokaal) ook private partners steeds meer betrokken in de aanpak. Deze aanpak draagt bij aan het structureel verankeren van digitale veiligheid binnen het reguliere werk van gemeenten en partners en zal daarom in 2026 extra aandacht krijgen.
3. Het voorzitterschap van de cyberburgemeesters komt naar onze regio in 2026; Burgemeester Weststeijn (IJsselstein) zal deze rol in 2026 op zich nemen. Dit biedt een mooie kans om de kracht van het land te gebruiken om regionaal zaken voor elkaar te krijgen.

Doel 1: Integraal sturen vindt plaats op basis van een informatiebeeld.
We willen onze capaciteit gericht inzetten om slachtoffer- en daderschap te voorkomen en daders te pakken. Daarvoor is data nodig die ons sturing geeft. Door het combineren van gemeentelijke data met die van politie en OM kunnen de driehoeken gerichter optreden. Ook zetten we in op datadeling binnen publiek-private samenwerking. Alleen door doordacht samen (te) werken houden wij onze inwoners digitaal veilig.

Acties	:	Actie 1: Periodiek aanleveren van een lokaal informatiebeeld online criminaliteit. Actie 2: Toewerken naar een integrale informatiepositie op online criminaliteit.
Monitoring/ Outputafspraak	:	Er is een werkwijze geformuleerd, afgestemd en gecommuniceerd ten aanzien van het delen van een periodiek informatiebeeld online criminaliteit voor de regio.

Doel 2: Slachtoffers hebben een hogere meldings- en aangiftebereidheid.
Partners vertrouwen erop dat aangifte doen van digitale misdaad bijdraagt aan het stoppen ervan. Daarom stimuleren partners inwoners om altijd aangifte te doen als ze slachtoffer zijn van digitale misdaad. Hoe gevoelig het mogelijk ook ligt.

Acties	:	Actie 3: Lokaal en regionaal communiceren. Actie 4: Aangiftebereidheid verhogen.
Monitoring/ Outputafspraak	:	1. In 2027 is de aangifte- en meldingsbereidheid gestegen naar 20% ten opzichte van 2023 waarin dit 16,9% was. (Bron: Veiligheidsmonitor). 2. Ieder kwartaal geven we contentsuggesties voor lokaal gebruik om de meldings- en aangiftebereidheid te vergroten.

Doel 3: Onze professionals zijn bewust en bekwaam t.a.v. DV&CC.
Alles digitaliseert. Daarom moeten professionals in én buiten het veiligheidsdomein weten hoe zij doordacht bijdragen aan het stoppen van digitale misdaad. Ken de online leefwereld. Erken de mogelijkheden. Herken de signalen en gevaren. Vergroot de impact: acteer samen.

Acties	:	Actie 5: De bestuurlijke aanpak tegen online criminaliteit borgen in de regio Midden-Nederland. Actie 6: Kennisuitwisseling organiseren en faciliteren. Actie 7: Voorbereiden op (de impact van) een langdurige digitale verstoring.
Monitoring/ Outputafspraak	:	Gemiddeld één kennisbijeenkomst per maand aan de hand van een leerlijn DVCC.

Doel 4: Effectiever (voorkomen en) aanpakken van daders.
Het vrije spel van digitale misdaad moet stoppen. Daartoe moeten professionals weten hoe digitale misdaad zich verweeft met hun werk. Ze werken samen om digitale misdaad te voorkomen en effectiever te stoppen.

Acties	:	Actie 5: De bestuurlijke aanpak tegen online criminaliteit borgen in de regio Midden-Nederland. Actie 8: Adviseren van gemeenten over het doordacht inzetten van interventies die de digitale weerbaarheid van inwoners vergroten. Actie 9: Domein overstijgende aanpak en publiek-private samenwerking lokaal en regionaal vergroten.
Monitoring/ Outputafspraak	:	1. In lijn met de landelijke veiligheidsagenda de minimale instroom van zowel cybercrime als gedigitaliseerde criminaliteit in 2026 met 10% verhogen t.o.v. de minimale instroomdoelstelling van 2025. 2. Minimaal één gecombineerde RIEC-casus per district. 3. De bestuurlijke aanpak van online criminaliteit is geborgd in de organisaties van de gemeenten, OM en politie.

Doel 5: Onze inwoners weten beter hoe ze hun slachtofferkans kunnen verkleinen.
Het vermogen en vertrouwen van onze inwoners staat op het spel. Het geven van handelingsperspectief is nodig om hun vertrouwen en vermogen te beschermen. Dit doen we doelgericht en doordacht (met behulp van data) door de verschillende doelgroepen te kennen en gericht in te spelen o p hun online leefwereld.

Acties	:	Actie 3: Lokaal en regionaal communiceren. Actie 8: Adviseren van gemeenten over het doordacht inzetten van interventies die de digitale weerbaarheid van inwoners vergroten. Actie 9: Domein overstijgende aanpak en publiek-private samenwerking lokaal en regionaal vergroten. Actie 10: Organiseren en aanjagen van een vervolg op de actiedag #EchtNietVandaag
Monitoring/ Outputafspraak	:	1. In 2027 is het aantal slachtoffers in de regio gedaald naar 13% ten opzichte van 2023 waarin dit 15,6% was. (Bron: Veiligheidsmonitor). 2. In ieder district is er een gezamenlijk uitvoeringsprogramma op de aanpak van digitale veiligheid en cybercriminaliteit.

Bijlage 1 Acties 2026

Actie 1: Periodiek aanleveren van een lokaal informatiebeeld online criminaliteit.	
Algemene info	Coördinatie: politie In samenwerking met: bestuursondersteuning politie
Doel	Om te komen tot concrete (samenwerkings)afspraken op strategisch niveau, stellen we periodiek een informatieproduct online criminaliteit beschikbaar voor gemeenten in Midden-Nederland.
Output	- In 2025 is in pilotvorm door de basisteamdriehoeken van de burgemeesters uit de bestuurlijke werkgroep gebruik gemaakt van een informatiebeeld online criminaliteit. Op basis van de evaluatie van de pilot wordt een advies geschreven hoe het informatieproduct kan voorzien in de informatiebehoefte die gemeenten hebben en op welk niveau dit informatieproduct zou moeten landen. - De politie levert periodiek een eenheid breed cyberbeeld en lokale informatiebeelden op voor alle gemeenten in Midden-Nederland. - In de ambtelijke werkgroepen wordt het beeld (in combinatie met het lokale infobeeld) toegelicht en besproken. Op basis daarvan komen de ambtelijke werkgroepen DVCC tot actiepunten voor de lokale aanpak. Indien nodig worden de districtelijke uitvoeringsplannen aangescherpt.
Aandachtspunten	- Iedere gemeente / basisteam heeft een eigen wens met betrekking tot informatiedeling en het bespreken van cijfers. Belangrijk om ruimte te geven voor eigen invulling hierin. - Het schrijven van een informatieproduct kost veel capaciteit van de politieorganisatie. Lokaal (al dan niet samen met de politie) tot actie komen op basis van dit informatiebeeld, is daarom gewenst.

Actie 2: Toewerken naar een integrale informatiepositie op online criminaliteit.	
Algemene info	Coördinatie: Bestuurlijke werkgroep DVCC Deze actie is onderdeel van ‘project 2: integrale informatiepositie’
Doel	Om gerichter te kunnen sturen op lange termijn doelstellingen is een strategisch informatieproduct noodzakelijk. Daarom ontwikkelen we, samen met partners, een structureel informatieproduct.
Output	- In contact komen met partners die informatie kunnen aanleveren voor het strategisch informatiebeeld. We bouwen voort op de (landelijke) samenwerking welke door NH Veilig is gestart. - Zodra er een duidelijker beeld is van de output van het informatieproduct, zal deze worden getoetst aan de informatiebehoefte (ambtelijk en bestuurlijk) in de regio.
Aandachtspunten	- Op initiatief van NH Veilig wordt al (landelijk) nagedacht hoe een integraal strategisch informatiebeeld vorm zou moeten krijgen. De kennis, ervaringen en het netwerk kunnen wij voor de uitwerking in onze regio gebruiken. - Hoe het intern datasysteem vorm krijgt, is afhankelijk van de besluitvorming binnen Stuurgroep RVS.

Actie 3: Lokaal en regionaal communiceren.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC

Doel	Digitale misdaad is vaak onzichtbaar. Daarom gaan wij, als lokale partners, samen één verhaal vertellen. Dit schept duidelijkheid, herkenning en vertrouwen. Eén verhaal maakt digitale misdaad zichtbaar, bespreekbaar en beter te bestrijden.
Output	- Het communicatiebord online criminaliteit wordt binnen de regio geïmplementeerd. - We organiseren periodiek korte (online) werksessies voor OOV en communicatieadviseurs samen. Tijdens deze bijeenkomst delen we de planning voor dat kwartaal, lokale fenomenen en doen we contentsuggesties. - We verkennen hoe we op dit thema landelijk samen kunnen werken met het vergroten van kennis bij inwoners over bellen naar de politie indien zij slachtoffer zijn geworden van online criminaliteit (PrioDigi/Digitale meldkamer).
Aandachtspunten	- Organisaties hebben zelf een volle contentkalender en afspraken over wanneer wel/niet communiceren. Dit heeft invloed op wat er vanuit de regio gecommuniceerd kan worden. - Het is zoeken naar de behoefte van de organisaties: geen standaard teksten, maar wel een duidelijke aanzet/suggestie voor inhoud.

Actie 4: Aangiftebereidheid verhogen.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC
Doel	In 2025-2026 werken we aan het verhogen van de aangiftebereidheid voor online criminaliteit, omdat dit leidt tot een grotere pakkans en een betere informatiepositie van het lokale bestuur. In 2023 was de (gemiddelde) aangifte- en meldingsbereidheid voor online criminaliteit 16% (Veiligheidsmonitor). In de Veiligheidsmonitor 2027 willen we dat de aangifte- en meldingsbereidheid gestegen is naar 20%. Dit doen we door middel van (lokale en regionale) voorlichtings- en communicatiecampagnes.
Output	- Het vergroten van de kennis van inwoners over de rol van de politie als zij in aanraking gekomen zijn met online criminaliteit (centrale boodschap: bel de politie als je aanraking bent gekomen met online criminaliteit).
Aandachtspunten	- Er wordt onderzoek gedaan door Cyberweerbaar NL naar de slachtofferbehoefte van mensen die in aanraking zijn gekomen met online criminaliteit. De uitkomsten van dit onderzoek zullen relevant zijn voor dit actiepunt, want het doen van aangifte is wellicht niet hun eerste behoefte.

Actie 5: De bestuurlijke aanpak tegen online criminaliteit borgen in de regio Midden-Nederland.	
Algemene info	Coördinatie: politie In samenwerking met Team bestuurlijke aanpak (politie Midden-Nederland)
Doel	De bestuurlijke aanpak van online criminaliteit borgen binnen reguliere werkzaamheden van de verschillende organisaties.
Output	- Blijven inzetten op het vergroten van kennis omtrent dit onderwerp. - We komen met een advies hoe deze aanpak te borgen binnen de politie in Midden-Nederland. - We delen de ervaringen die we in Midden-Nederland hebben opgedaan met de rest van het land.
Aandachtspunten	- Er is capaciteit nodig bij team bestuurlijke aanpak om hier op de lange termijn focus op te kunnen houden en in door te kunnen ontwikkelen. - Er is koud water vrees bij gemeenten voor deze nieuwe aanpak. Daarom is het van belang dat bestuurlijke rapportages op een 'warme' manier landen.

Actie 6: Kennisuitwisseling organiseren en faciliteren.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC

Doel	Het vakmanschap van collega's (binnen en buiten het veiligheidsdomein) moet blijvend worden vergroot, zodat doordacht digitale misdaad kan worden aangepakt. We verkennen hoe we de kennis van het lokale bestuur en politiek kunnen vergroten, gebruikmakend van bestaande gremia.
Output	- We gaan lokaal het gesprek aan over wat er speelt en bieden handelingsperspectief. Enerzijds hoe gemeenten inwoners kunnen bereiken met de juiste interventies, anderzijds welke (lokale) partners (intern) te betrekken. - We zullen minimaal 12 kennisbijeenkomsten organiseren. Samen met ons netwerk bepalen we de thema's waarop de kennisuitwisseling zal plaatsvinden, inhakend op de actualiteit. - We zoeken naar kansen hoe we, gebruikmakend van bestaande gremia, de kennis van het lokale bestuur en politiek kunnen vergroten. - CISO-netwerk Midden-Nederland: • Een netwerk van betrokken CISO's die elkaar, indien nodig, weten te vinden. • Faciliteren van kennisdeling tussen CISO's in de regio. • Borgen van het netwerk in bestaande structuren.
Aandachtspunten	- Volle agenda's verkleinen aanwezigheid bij kennisbijeenkomsten. Belangrijk om het laagdrempelig en makkelijk toegankelijk te houden.

Actie 7: Voorbereiden op (de impact van) een langdurige digitale verstoring.	
Algemene info	Coördinatie: Veiligheidsregio's Midden-Nederland
Doel	Het verbeteren van de voorbereiding op cyberincidenten door bij te dragen aan inzicht in het speelveld, de taken en verantwoordelijkheden binnen de geldende crisisstructuren.
Output	Samen met de Veiligheidsregio's inventariseren we de behoefte ten aanzien van de voorbereiding op (langdurige) cyberincidenten. Op basis van deze inventarisatie komen we tot een concreet plan hoe hierin te voorzien.
Aandachtspunten	- Er is specifieke kennis vereist bij Bureau RVS, als dit op de lange termijn een thema is wat binnen het samenwerkingsverband moet worden opgepakt.

Actie 8: Adviseren van gemeenten over het doordacht inzetten van interventies die de digitale weerbaarheid van inwoners vergroten.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC
Doel	Gemeenten adviseren en ondersteunen bij het bewust en onderbouwd kiezen van interventies die de digitale weerbaarheid van inwoners versterken. In de advisering en ondersteuning ligt de nadruk op het bieden van handelingsperspectief, het vergroten van lokaal eigenaarschap en het stimuleren van domeinoverstijgende samenwerking binnen gemeenten.
Output	- We gaan lokaal het gesprek aan over wat er speelt en bieden handelingsperspectief. Enerzijds hoe gemeenten inwoners kunnen bereiken met passende interventies, anderzijds welke partners binnen de gemeente betrokken moeten worden en hoe zij gezamenlijk eigenaarschap kunnen nemen. - We voeren met politie en gemeenten het gesprek over de vraag hoe nazorg op online criminaliteit vormgegeven kan worden.
Aandachtspunten	- Er is weinig capaciteit en geld beschikbaar om structureel en doordacht een lokaal interventie/weerbaarheidsprogramma in te richten.

Actie 9: Domein overstijgende aanpak en publiek-private samenwerking lokaal en regionaal vergroten.	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC Met betrekking tot het RIEC Midden-Nederland: Bestuurlijke werkgroep DVCC en bestuurlijke werkgroep GOC
Doel	We versterken de (lokale) samenwerking in de aanpak van online criminaliteit. Ten eerste richten we ons op domein overstijgende samenwerking binnen de gemeentelijke organisatie, zodat iedere professional een actieve en betekenisvolle rol vervult binnen deze gezamenlijke opgave. Ten tweede zetten we in op (lokale) publiek-private samenwerking, zodat kennis en informatie wordt gedeeld die leiden tot het gezamenlijk uitvoeren van interventies.
Output	- We leveren een inhoudelijke bijdrage aan het plan van aanpak voor de structurele inbedding van de aanpak van online criminaliteit binnen het reguliere werk van het RIEC Midden-Nederland. - Minimaal vijf RIEC-casussen hebben in 2026 betrekking op online criminaliteit. - We ontwikkelen een factsheet met een overzicht van lokale partners die betrokken kunnen worden bij de aanpak van digitale onveiligheid, inclusief voorbeelden van succesvolle samenwerkingen uit de regio. - We adviseren en ondersteunen gemeenten bij het voeren van domeinoverstijgende gesprekken: wie zijn de interne en externe partners, wat is ieders rol en verantwoordelijkheid, en hoe kan samenwerking worden geborgd?
Aandachtspunten	- Belangrijk om te focussen op de (lokale) samenwerking die er al is en deze uit te bouwen, in plaats van nieuwe samenwerkingen aan te gaan.

Actie 10: Organiseren en aanjagen van een vervolg op de actiedag #EchtNietVandaag	
Algemene info	Coördinatie: bestuurlijke werkgroep DVCC In samenwerking met: Digitaal District (politie), PVO, RIEC-MN
Doel	Het organiseren en regionaal aanjagen van de actiedag #EchtNietVandaag 2027 om: - De digitale weerbaarheid van inwoners en ondernemers in Midden-Nederland te vergroten d.m.v. interventies die effectief en doordacht worden ingezet, passend bij de doelgroepen en aansluitend bij wat er lokaal speelt; - Zichtbaar te maken dat lokale overheden en private en maatschappelijke partners zich samen inzetten tegen digitale criminaliteit; - Een impuls te geven aan het in kaart brengen, verwerken en activeren van het lokale publiek-private netwerk rondom cyberweerbaarheid.
Output	- Het aanzetten van lokale publiek-private netwerken om mee te doen met de actiedag, met aandacht voor passende interventies (aansluitend op actie 8). - Het opleveren en beschikbaar stellen van de Echt Niet Vandaag toolkit, bestaande uit oproepbrieven, inspiratiekaarten voor doordachte interventies en communicatiemiddelen, waarbij gemeenten en partners het hele jaar door toegerust worden om interventies op cyberweerbaarheid te organiseren. - Het binden en betrekken van regionale partners, voortbouwend op de resultaten en het netwerk van de actiedag in 2025 (aansluitend op actie 9). - Vorming van een sterke kerngroep met doelgroep aanjagers staan die stevig in de netwerken van gemeenten, politie, bedrijfsleven, onderwijs, en maatschappelijke partners verankerd zijn. - Regionale en lokale media-aandacht voor online criminaliteit en cyberweerbaarheid, inclusief aandacht voor aangiftebereidheid.

	Beoogd resultaat: een regionale actiedag met minimaal 100 onderbouwde en doelgroepgerichte activiteiten gericht op cyberweerbaarheid, uitgevoerd door publieke en private organisaties die gezamenlijk verantwoordelijkheid nemen voor het vergroten van de digitale weerbaarheid van inwoners in Midden-Nederland.
Aandachtspunten	- Uit de procesevaluatie van kernteam #EchtNietVandaag 2025 bleek dat niet elke partner uit het kernteam een rol voor zichzelf weggelegd ziet om een vervolg te geven aan #EchtNietVandaag. De organisatie van #EchtNietVandaag zal dus een andere vorm moeten krijgen. - Kwaliteit moet even zwaar wegen als de kwantiteit van interventies: er moet (meer) worden gestuurd op een onderbouwde keuze voor interventies.

Bijlage 2 Terugblik 2025

In 2025 is gewerkt aan de doelen die in het DIN staan weergegeven. De voortgang hierop is geëvalueerd in de regionaal ambtelijke werkgroep op 27 oktober 2025. Onderstaand wordt per doel de voortgang weergegeven, gebruikmaken van de monitoringsafspraken die we voor 2025 hadden vastgesteld.

Doel 1: Integraal sturen vindt plaats op basis van een informatiebeeld.

Monitoringsafspraak: Tweemaal per jaar lokaal informatiebeeld agenderen op basisteamdriehoek.		In vijf driehoeken is het lokale informatiebeeld twee keer besproken. Binnen deze pilot wordt doordacht hoe deze cijfers het meest effectief besproken kunnen worden. Deze aanpak wordt in 2026 breder uitgezet in de eenheid.

Toelichting:
Binnen de pilot 'informatiebeelden voor de lokale driehoeken' heeft de DRIO informatieproducten aangeleverd voor de driehoeksoverleggen van de burgemeesters uit de bestuurlijke werkgroep. Hierdoor wordt de informatiepositie van de pilotgemeenten vergroot. Echter, het vraagt aandacht op welk niveau deze cijfers besproken dienen te worden. De problematiek is niet altijd van dien aard dat het een gesprek vraagt binnen de driehoek. Dit neemt echter niet weg dat het op ambtelijk niveau van belang is om periodiek vanuit de politie een update te krijgen van de huidige problematiek, zodat preventie gericht ingezet kan worden.
Tegelijkertijd vraagt het aandacht om *integraal* aan de slag te gaan met de cijfers. Gemeenten koppelen niet/weinig aan politie terug wat er met de cijfers gebeurt. Daarnaast worden deze cijfers nog te weinig domeinoverstijgend besproken. Verder blijft het aandacht vragen om dit niet alleen, maar samen met lokale partners, op te pakken.
Ook wordt toegewerkt naar een strategisch informatiebeeld online criminaliteit. Dit gebeurt in een breder kader, want binnen Bureau RVS en RIEC Midden-Nederland wordt, in opdracht van Stuurgroep RVS, gewerkt aan 'vijf dimensies voor een effectieve samenwerking'. Eén van deze 'dimensies' is het project 'integrale informatiepositie', waarin gewerkt naar een structurele integrale informatiepositie gericht op de uitvoeringspraktijk en methodiek ontwikkelingen.
In 2025 is voor dit project de behoefte geïnventariseerd en uitgewerkt hoe dit voor de lange termijn vorm zou kunnen krijgen. In december 2025 wordt hier door Stuurgroep RVS een besluit op genomen.

Doel 2: Slachtoffers hebben een hogere meldings- en aangiftebereidheid.

In 2027 is de aangifte- en meldingsbereidheid gestegen naar 20% ten opzichte van 2023 waarin dit 16,9% was. (Bron: Veiligheidsmonitor).		Volgt in 2027. Uit het rapport Online veiligheid en criminaliteit 2024 van het CBS blijkt dat in 2024 18% van de slachtoffers dit bij de politie heeft gemeld. Een deel hiervan deed uiteindelijk aangifte (16% van de slachtoffers).
Ontwikkelen campagnemateriaal en beschikbaar stellen voor lokaal gebruik om de meldings- en aangiftebereidheid te vergroten.		Er is een communicatiebord ontwikkeld welke door partners gebruikt kan worden in hun communicatie over het onderwerp, maar deze moet nog lokaal worden geïmplementeerd.

Toelichting:
In 2025 is de strategische communicatieboodschap verwoord en gevisualiseerd in een communicatiebord. Dit communicatiebord is gepresenteerd binnen het (dit jaar opgestarte) netwerk van communicatieadviseurs. Het oprichten van dit netwerk en het maken van het communicatiebord heeft tot doel om binnen de regio met één stem te spreken over digitale misdaad en het gemakkelijker te maken hierover lokaal te communiceren.
Het communicatiebord moet nog worden geïmplementeerd en het communicatienetwerk staat nog in de kinderschoenen. Door personele wisselingen binnen Bureau RVS ligt dit helaas op dit moment stil.

Doel 3: Onze professionals zijn bewust en bekwaam t.a.v. DV&CC.		
Gemiddeld één kennisbijeenkomst per maand aan de hand van een leerlijn DVCC.		Aan de hand van de leerlijn met de thema's online jeugdcriminaliteit, integraal communiceren en informatiegestuurd werken zijn er in 2025 15 kennisbijeenkomsten geweest.

Toelichting:
Om de vakbekwaamheid van professionals in Midden-Nederland te vergroten zijn er in 2025 15 kennisbijeenkomsten georganiseerd. De drie centrale thema's (online jeugdcriminaliteit, informatiegestuurd werken en integraal communiceren) gaven richting aan de inhoud van de sessies. Ook is de cyberoefendriehoek georganiseerd. Deze dag vormde voor alle betrokken disciplines een goede aanleiding om verder aan de slag te gaan met het voorbereiden voor een cybercrisis.

Een aandachtspunt met betrekking tot dit doel is dat het een uitdaging blijft voor collega's om tijd te vinden waarop zij deel kunnen nemen aan kennisbijeenkomsten.

Doel 4: Effectiever (voorkomen en) aanpakken van daders.		
In lijn met de landelijke veiligheidsagenda de minimale instroom van zowel cybercrime als gedigitaliseerde criminaliteit in 2025 met 10% verhogen t.o.v. de minimale instroomdoelstelling van 2024.		Volgt in januari 2026.
Minimaal één gecombineerde RIEC-casus per district.		Vanuit Bureau RVS is ingezet op het leggen van de verbinden en het vergroten van de wederzijdse kennis bij het RIEC en de digitaal specialisten in de districten. Uiteindelijk heeft zijn er in 2025 twee RIEC-casussen opgestart in drie districten.
Minimaal vijf bestuurlijke rapportages opgeleverd tegen personen die zich beziggehouden hebben met online criminaliteit of panden waarbinnen online criminaliteit heeft plaatsgevonden.		In 2025 zijn meer dan 10 bestuurlijke rapportages opgeleverd tegen verdachten van online criminaliteit.

Toelichting:
Binnen het opstarten van de bestuurlijke aanpak van online criminaliteit is eind 2024 en begin 2025 ingezet op het vergroten van de kennis bij politiecollega's van de bestaande mogelijkheden. Uiteindelijk zijn er tot oktober 2025 meer dan 12 bestuurlijke rapportages opgeleverd zijn tegen verdachten van online criminaliteit. Tevens is er binnen de pilot veel tijd besteed aan het in kaart brengen welke (bestuurlijke) mogelijkheden er zijn tegen facilitators (zoals datacenters en hostingpartijen) van online criminaliteit.

Een bestuurlijke aanpak van online criminaliteit lijkt op basis van de resultaten veelbelovend te zijn. Maar het kost veel tijd en vraagt specifieke expertise, omdat dit nieuw terrein is. Een aandachtspunt is dus hoe dit te borgen binnen de politieorganisatie, want het risico is dat als de pilot stopt de aandacht hiervoor ook stopt. Begin 2026 zal een factsheet opgeleverd worden met de resultaten van de pilot en een advies hoe dit te borgen in de aanpak van online criminaliteit.

Daarnaast zijn er, samen met het RIEC, stappen gezet om verdachten van online criminaliteit binnen het RIEC-convenant aan te pakken. Er zijn twee RIEC-casussen opgestart en er zijn twee RIEC-collega's gestart die het thema gaan oppakken binnen RIEC Midden-Nederland.

Alhoewel de wil er binnen het RIEC Midden-Nederland is om met het thema online criminaliteit aan de slag te gaan, loopt men ertegen aan dat het zo omvangrijk is dat het lastig is om een eerste stap te zetten. Daarnaast wonen daders vaak niet in de eigen eenheid, dus dit vraagt ook samenwerking tussen de verschillende RIEC's.

Doel 5: Onze inwoners weten beter hoe ze hun slachtofferkans kunnen verkleinen.		
In 2027 is het aantal slachtoffers in de regio gedaald naar 13% ten opzichte van 2023 waarin dit 15,6% was. (Bron: Veiligheidsmonitor).		Volgt in 2027. Maar uit het meest recente onderzoek van het CBS blijkt dat in 2024 nog een stijging te zien was van 15,6% naar 16% (bron: online veiligheid en criminaliteit 2024).

Toelichting:
Het doel om het aantal slachtoffers van online criminaliteit te laten delen is nog niet meetbaar gerealiseerd. Toch is er in 2025 veel in gang gezet om de digitale weerbaarheid van inwoners te vergroten. Gemeenten, politie en partners hebben inwoners bewust gemaakt van online risico's en handelingsperspectief geboden.

Enkele belangrijke resultaten:
- Echt-Nep campagne: Bereikte in 2025 787 senioren (doel: 300). Dankzij het *train-the-trainer*-principe voeren inmiddels 29 gemeenten deze interventie zelfstandig uit.
- Bakfiets "Dubbel beveiligd is dubbel zo veilig": Ingezet in zes gemeenten en inmiddels ook landelijk beschikbaar, waardoor gemeenten er blijvend gebruik van kunnen maken.
- Re_Bootcamp: Een experience voor jongeren (12–25 jaar) met interesse in IT, gericht op het positief stimuleren van jong hacktalent, georganiseerd met o.a. gemeenten en politie en in samenwerking met Defensie, hogescholen, cybersecuritypartijen, stichting cyberbrein en het DIVD.
- Actiedag #EchtNietVandaag: Alle gemeenten en politiebasisteams hebben zich ingezet tijdens de actiedag op 10 september, met 105 preventieve activiteiten gericht op jeugd, senioren en ondernemers.

Naast deze uitgelichte voorbeelden zijn er door het hele jaar heen talloze lokale preventieve activiteiten georganiseerd door gemeenten, vaak in samenwerking met politie, bibliotheken en maatschappelijke organisaties. Toch zijn de interventies nog weinig gebaseerd op wat er lokaal speelt. Met behulp van de informatiebeelden van de politie, zouden interventies gerichter ingezet kunnen worden.

Bijlage 3

Programma Digitale veiligheid & cybercriminaliteit; Doelen-Inspanningen-Netwerk

Ambitie

In Midden-Nederland gaan we slachtoffer- en daderschap van gedigitaliseerde criminaliteit en cybercrime voorkomen en daders hiervan pakken. Hiertoe hebben we kundige professionals waarvoor integraal samenwerken tussen gemeenten, politie en OM vanzelfsprekend is. Data wordt gebruikt om capaciteit gericht in te zetten. De potentiële slachtoffers en daders worden weerbaar tegen gedigitaliseerde criminaliteit en cybercrime.

Doelen

- **Voorkomen Slachtoffer- en daderschap en daders pakken**
- **Kundiger organisaties en medewerkers**

Baten

- Integraal sturen vindt plaats op basis van informatiebeeld
- Slachtoffers hebben een hogere melding- en aangifte-bereidheid
- Onze professionals zijn bewust en bekwaam t.a.v. DV&CC
- Effectiever (voorkomen en) aanpakken daders
- Onze inwoners weten beter hoe ze hun slachtofferkans kunnen verkleinen

Inspanningen en resultaten

Informatiebeeld

- Samenbrengen databronnen (directe en indirecte partners, zicht op cyber): **Informatiebeeld DV&CC**

Communicatie

- Communicatie Campagne: **communicatie-uitingen met groot bereik binnen MN**
- Verhalen verzamelen voor media en relatiebeheer: **publicaties in regionale media**
- Communicatie toolbox ontwikkelen: **toolbox**

Actiegericht (samen)werken

- Overzicht creëren rollen en relaties + afhankelijkheden; **overzicht DV&CC profs**
- Hulp en advies aan **zelfstandige werkgroepen met actieplannen**
- Vergroten handelingsperspectief en innovatie
- Gerichte acties voor slachtoffers, potentiele daders en daders
- Adequaat reageren op signalen slachtoffers zodat ze zich gehoord en geholpen voelen

Kennis- en expertiseoverdracht

- Best practice gespreksronde (binnen en buiten MN); **kennisdeling**
- Driemaandelijkse nieuwsbrief DV&CC MN **Kennisdeling**
- Organiseren themagroepen (o.a. communicatie, ciso); **prof. leergemeenschap**

Cyclisch werken binnen het programma door in te zetten op werkvormen die het Weten (o.a. communicatieuitingen en themagroepen), Kunnen (o.a. workshops en trainingen), Doen (o.a. werkgroepen en actieplannen) en Leren (o.a. evaluaties en leerpunten) mogelijk maken.

Doelgroepen

- Politie: eenheidsleiding, politiechefs, DRIO, recherche, basisteams
- OM: OM-leiding, OvJ's, afdeling Beleid & Strategie
- Gemeenten: burgemeester, GS, GR, Hoofd veiligheid, veiligheidsprofessionals
- Indirect: (potentieel) slachtoffers en daders

Programmastrategie

- Optreden als één overheid
- Smeden van maatschappelijke coalities
- Integrale uitvoeringspraktijk

Randvoorwaarden voor succes

- Het speelveld door en door kennen: wie is waarvan en hoe raakt eenieder aan DV&CC?
- Partners geven ons inzicht in hun organisatie
- Lokale vertaling van (csv) informatie om tot prioritering in casuïstiek te komen
- Versterken van de Informatie en Expertise om meer (beter) effect in de aanpak te bereiken: actiegericht
- Impactvolle communicatie: niet alleen over interventies maar ook op effecten van die interventies
- Samenwerkingskunde: zicht op elkaars ambitie, belangen, mogelijkheden en werken aan relaties
- Partners delen en vertalen visie en afspraken op integrale aanpak in de eigen organisatie (thuisfrontmanagement)
- Ieders betrokkenheid in tijd, geld en het leveren van capaciteit
- Blijvend leren van elkaar

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl

Kroonstraat 25 - Postbus 8300 - 3503 RH - Utrecht - 06 148 73 690 - secretariaat@rvs-mn.nl - www.veiligheidscoalitie.nl