

Bijlage – Eindoverzicht Borging van City Deal interventies

In deze bijlage staat het eindoverzicht van alle geborgde City Deal interventies voor de doelgroepen Jeugd, Senioren, MKB en het aandachtsgebied Online aangejaagde orderverstoringen (OAOV) centraal. Dit document is vastgesteld in de stuurgroep van 10 december 2025.

1. Jeugd

	NAAM	GEBORGD?	TOELICHTING
1.	Cyberbreinen in beeld	Ja, via het CCV en Stichting Cyberbrein	Deze pilot heeft de volgende specifieke producten opgeleverd: <ol style="list-style-type: none"> 1. een signaleringskaart, 2. een signaleringsstructuur door middel van training, en 3. maatwerkgerichte interventies voor begeleiden van jonge cyberbreinen (via de Stichting Cyberbrein, tegen vergoeding na 2025). De signaleringskaart en uitleg worden opgenomen op de website van het CCV. De Stichting Cyberbrein verzorgt na 2025 de maatgerichte interventies.
2.	HackShield's cyberbreinen	Ja, via HackShield	Specifiek voor deze quest geldt dat na de eerste uitrol in het schooljaar 2024 – 2025 de klassenquest is doorontwikkeld zodat ook in het schooljaar 2025 – 2026 leerkrachten en gastdocenten de quest (gratis!) kunnen behandelen. In april 2026 worden cybertalenten uitgenodigd bij het jaarlijks door Challenge the Cyber georganiseerde Capture the Flag. Dit verloopt via een separaat traject. Deze specifieke quest is geborgd. In het algemeen geldt dat de Stichting HackShield druk doende is de continuïteit van de stichting zelf te borgen.
3.	The Cyber Journey	Ja, via het CCV	De uitrol van de praatplaat met bijbehorende praatteksten heeft plaatsgevonden tijdens het eindcongres City Deal. Hierna is de informatie ook op de website opgenomen van het CCV. Het is een prachtig middel om met partners de discussie te voeren over online en offline aanwezigheid van ouders, jeugdzorgmedewerkers, politie en andere partners. De praatplaat wordt breed ingezet tijdens het congres. De praatplaat en de praatteksten worden ook opgenomen op de website van het CCV en zijn eenvoudig te gebruiken.
4.	Cyberouders	Ja, via het CCV	De deelnemende gemeenten onderzoeken gezamenlijk welke stappen er genomen moeten worden om een netwerk van cyberouders op te bouwen. Het doel is dat andere gemeenten en partners hiermee een eigen lokaal netwerk van cyberouders kunnen opbouwen. De ontwikkelde materialen voor communicatie en training worden beschikbaar gesteld via het CCV. Inmiddels is er vanuit de pilotgemeenten aangegeven dat zij ook komend jaar zullen blijven doorgaan met ontwikkelen. Daarmee zetten ze een

			stevige basis neer voor de uitrol naar andere gemeenten. Het CCV zal zorgen voor bredere verspreiding van de ervaringen.
5.	LVB-experience	Ja, via gemeente Breda	Gemeente Breda heeft een prototype Virtual Reality (VR) opgeleverd met card board en app. Dit is een laagdrempelige en makkelijk deelbare manier om onder de doelgroep meer data op te halen over het gebruik van een dergelijke interventie (alvorens tot een echte VR te komen). Voor de doorontwikkeling (2026) onderzoeken zij de vorming van een consortium voor een subsidieaanvraag richting regieorgaan SIA. Met zo'n consortium kan de VR verder getest worden. Tevens kan daarmee het prototype doorontwikkeld worden naar een krachtige en duurzame interventie voor online weerbaarheid van jongeren met een licht verstandelijke beperking.
6.	Digitaal niet te foppen	Ja, via wikiwijsheid.nl en het CCV	Alle ontwikkelde materialen zijn gedeeld en nieuwe materialen worden ook weer gedeeld via onder meer wikiwijsheid en het CCV. De scholen die meededen hebben cyberweerbaarheid in het curriculum opgenomen. Er is contact met schoolbesturen zoals CVO (37 scholen) en OMO (71 scholen). CVO en OMO zullen komend schooljaar digitale weerbaarheid op de agenda van de scholen onder hun bestuur zetten. Komend schooljaar zal ook de PO- en VO-Raad actief dit project blijven promoten richting PO- en VO scholen in Nederland.
7.	Lokale interventie voor geldezels	Ja, via het CCV	Binnen de City Deal is in Haarlem een lokale pilot ontwikkeld gericht op geldezels. Deze is door het CCV landelijk doorontwikkeld en vertaald naar de gevalideerde Leidraad Lokale Aanpak Geldezels, getest in vier gemeenten met een klankbordgroep. Het CCV zal in 2026 de interventie verder ontwikkelen. In samenwerking met JenV wordt gewerkt aan doorontwikkeling en evaluatie, conform het Landelijk Kwaliteitskader en de motie-Mutluer. De inzet bestaat uit twee sporen: continuering van gemeentelijke ondersteuning en verdere vormgeving van de inkeerregeling. Hiervoor is inmiddels een nieuwe subsidie vanuit het ministerie van JenV toegezegd.
8.	Youth Cyber Team	Ja, via het CCV	Youth Cyber Team is recent geïnterviewd ten behoeve van het Eindcongres waarmee de doorontwikkeling is weergegeven in het congres-magazine. Een nieuw rapport is ook verschenen en zal op de website van het CCV opgenomen worden zodra dit openbaar is. Het rolmodelprincipe dat binnen deze interventie is ontwikkeld, kan ingezet worden binnen andere gemeenten. De informatie wordt opgenomen op de website van het CCV.
9.	re_BooTCMP	Ja, via de DIVD Academy.	Het COPS-team is de ontwikkelaar van re_BooTCMP (evenals Gamechangers en Framed!). De belangrijkste stap om de interventie ook voor de toekomst te borgen is, is deze een plek te geven buiten de politie. Datum voor overdracht is 1 januari 2026, waarbij een overgangstermijn nog nader wordt afgestemd. De DIVD Academy heeft een coördinator aangesteld waarmee de overdracht zal worden gerealiseerd.

- **In breder verband** geldt dat de rol van het **CCV** in 2026 ten aanzien van de interventies vanuit de City Deal is, om deze breder onder de aandacht te brengen van gemeenten en daarmee samenwerkende partners, en ook breed toegankelijk te maken. Dit wordt gesteund door onder meer de ontwikkeling van een digitale interventiewijzer die gemeenten helpt bij het kiezen van passende en samenhangende interventies, gekoppeld aan de ontwikkelfasen van jongeren. De koppeling naar lopende onderzoeken zoals het Pathway-onderzoek van Cyberweerbaar NL helpt hierbij.
- **Samenhangende interventies en Human Capital Agenda (hierna: HCA):** De HCA-organisatie heeft een overzicht gekregen van welke interventies wij bieden en wat nodig is vanuit het bedrijfsleven. In december 2025 wordt het overleg vervolgd. Het gaat om interventies die in principe een eigen borging kennen, maar waarbij - door de onderlinge verbinding te versterken - een bredere impact wordt gerealiseerd. Het gaat hier om HackShield, Cyberbreinen in beeld, The Cyber Journey, en re_BooTCMP.
- **Synergie tussen interventies:** Verder zien we een ontwikkeling waarbij DIVD Academy, re-BooTCMP, HackShield, Challenge the Cyber en de Stichting Cyberbreinen ook los van de HCA ontwikkeling steeds nauwer samenwerken, geheel op elkaar aansluit en talenten op de goede plek terecht kunnen komen en begeleid kunnen worden. Met deze beweging worden de interventies die impact hebben op talentontwikkeling blijvend ingezet en los van de City Deal verder ontwikkeld.

2. Senioren

NAAM	GEBORGD?	TOELICHTING
10. Storytelling voor bewustwording in Oost-Brabant	Ja, via het CCV en bij Regiobureau Integrale Veiligheid Oost-Brabant	De concrete producten, zoals de lokaal uitgevoerde campagne en de procesevaluatie, zijn beschikbaar via de website van het CCV. De geleerde lessen uit het traject worden opgenomen in het kennisaanbod van het CCV en gedeeld met regionale en lokale partners. In Oost-Brabant wordt de vrijwilligersaanpak voortgezet en worden er structureel nieuwe bijeenkomsten voor senioren georganiseerd.
11. Netwerksamenwerking cyberweerbare 55-plussers	Ja, via het CCV	De concrete producten, zoals de onderzoeksrapporten van NHL-Stenden en de <i>hand out</i> voor gemeenten, zijn beschikbaar via de website van het CCV. De geleerde lessen uit het proces worden geïntegreerd in het kennisaanbod van het CCV en gedeeld met regionale en lokale partners. In Noord-Nederland blijven de samenwerkingen met betrokken organisaties bestaan en worden gezamenlijk nieuwe activiteiten voor senioren georganiseerd, waarmee de borging van deze interventie is gewaarborgd.
12. Interactieve training cyberweerbaarheid senioren (film Echt of Nep)	Ja, via het CCV	De film is volledig ondergebracht bij het CCV, dat verantwoordelijk is voor beheer, onderhoud en promotie. Er is een online versie beschikbaar en een off line PowerPoint-versie op aanvraag. Toekomstige updates en doorontwikkelingen worden door het CCV uitgevoerd. Belangrijke besluiten, zoals toestemming voor gebruik door de Nederlandse Vereniging van Banken worden in overleg met de VAR genomen. Daarmee is deze interventie geborgd.
13. Serious game cyberweerbaarheid laaggeletterden	Ja, via het CCV	Deze <i>serious game</i> is ondergebracht bij het CCV. Beheer, onderhoud, promotie, toekomstige updates en doorontwikkelingen worden door het CCV uitgevoerd. Daarmee is deze interventie geborgd.
14. Storytelling online fraude	Ja, via het CCV	De e-learning storytelling is ontwikkeld en ondergebracht bij het CCV. Beheer, onderhoud, promotie, toekomstige updates en

			doorontwikkelingen worden door het CCV uitgevoerd. Daarmee is deze interventie geborgd.
15.	Digitale buurtambassadeurs	Ja, via het CCV en de gemeente Breda	Gemeente Breda: Informatie geborgd op site van het CCV en de uitvoering is lokaal geborgd. In Breda zijn er verschillende groepen buurtambassadeurs actief die ondersteund worden door de gemeente. Hiermee wordt er lokaal vervolg gegeven aan deze interventie.
16.	Digitale veiligheid in de wijk	Ja, via het CCV en de gemeente Den Haag	Gemeente Den Haag: Informatie geborgd op site van het CCV en uitvoering is lokaal geborgd. Binnen de gemeente Den Haag zijn er verschillende groepen buurtambassadeurs actief, die ondersteund worden door de gemeente. Hiermee wordt er lokaal vervolg gegeven aan deze interventie.

3. MKB

	NAAM	GEBORGD?	TOELICHTING
17.	Leergemeenschappen voor cyberweerbare mkb-ers (CVD)	Ja, geborgd bij MKB NL/VNO NCW	Het concept van de leergemeenschap wordt momenteel verder uitgewerkt door MKB Nederland/VNO NCW door het opzetten van zogenaamde leergroepen. Hierbij benadrukken zij dat naast structuur, ook een vertrouwde sfeer en kennis over cyberweerbaarheid belangrijke succesfactoren zijn. Het CCV heeft de werkwijze van interventies met de geleerde lessen geplaatst in de online beschikbare database lokale cyberprojecten.
18.	Digitaal Veiligere Werkvloer met de Digitale Hulpverlener (gemeente Haarlem)	Ja, geborgd bij MKB NL/VNO NCW	VNO-NCW en MKB-Nederland hebben het concept van de digitale hulpverlener (DHV-er) inmiddels verwerkt in het cyber-noodplan en beschikbaar gesteld via www.samendigitaalveilig.nl . En ook aandacht hiervoor gevraagd in diverse nieuwsberichten. Hierbij worden ondernemers (groot en klein) gestimuleerd om een medewerker aan te wijzen die eerste aanspreekpunt is bij cyberincidenten. Het PVO organiseert in 2025 in regio's Rotterdam en Noord-Holland pilotsessies over digitale hulpverlening. Daarna wordt bekeken of het concept aansluit bij de dienstverlening van PVO en een landelijk karakter zou moeten krijgen. De uiteindelijke verantwoordelijkheid voor de implementatie en de opleiding van de DHV-er ligt bij de ondernemer.
19.	Digitale Cybersecurity Ster voor KVO-B (gemeente Veenendaal)	Ja, bij de gemeente Veenendaal	Het toevoegen van een digitaal onderdeel aan het bestaande Keurmerk Veilig Ondernemen bij een bedrijfsterrein in Veenendaal draait nu volledig zelfstandig. Het landelijk opschalen van dit initiatief wordt door PVO en DTC als complex beschouwd, vanwege de aanzienlijke kosten en het beperkte aantal ICT-aanbieders die deze dienst kunnen leveren.
20.	Cynalytics Insights (Cynalitics BV)	Ja, via Cynalitics BV	De interventie Cynalytics insights richtte zich op het verder ontwikkelen van programmeercode om kwetsbaarheden op te sporen achter de firewall van de mkb-er. Deze code is inmiddels openbaar beschikbaar via OpenKat (open source platform). Dit is een actief platform waar ontwikkelaars

			kennis en code met elkaar uitwisselen en hiermee bouwen aan een cyberweerbaarder Nederland.
21.	Geautomatiseerde evidence-based gedragsinterventie Versie 1 en 2 (Haagse Hogeschool)	Ja, via Threadstone i.s.m. de Haagse Hogeschool en PVO NL	<p>Dit is een initiatief van de Haagse Hogeschool en is ontwikkeld in samenwerking met het cybersecuritybedrijf ThreadStone. Dit bedrijf krijgt een lijst van url's van mkb-ers en scant elke mkb-er twee keer op kwetsbaarheden. De resultaten per scan en een totaaloverzicht van de meting worden aangeleverd bij de Haagse Hogeschool. De Hogeschool brengt uitkomsten onder de aandacht van de gescande ondernemer en biedt handelingsperspectief.</p> <p>De uitvoering van de scan is geborgd bij Threadstone.. De Hogeschool ziet de organisatie en het aanjagen per branche of gemeente niet als haar structurele taak. Dit komt na de City Deal te vervallen en moet geborgd worden.. MKB Nederland/VNO NCW zien een rol weggelegd voor een niet-commerciële landelijke partij, die op lokaal niveau in nauw contact staat met ondernemers en op landelijk niveau met brancheorganisaties. Daarom stellen zij voor om PVO NL de rol te geven als aanjager van deze interventie na de City Deal.</p> <p>Er worden momenteel gesprekken gevoerd met PVO NL om in een aantal PVO regio's dit project via een pilot dit te project mogelijk te laten toevoegen aan de standaardtaken.</p>
22.	Detectietools (CVD, NHL Stenden en SecureMe2)	Ja, via het CCV en Cyberweerbaar NL	<p>Dit project wordt momenteel uitgevoerd in Oost-Nederland samen met CVD, PVO Oost-NL, 3 lectoraten en Secureme2). Tien mkb-ers (10-50 fte) krijgen een tool die afwijkend verkeer in het netwerk monitort. Drie lectoraten zijn betrokken en bezien wat deze interventie voor effect heeft op juridisch (wie is verantwoordelijk), technisch (maakt het echt weerbaarder/wat voor tools zijn er) en gedrag (wordt de ondernemer cyberweerbaarder). Het CCV blijft op de achtergrond 4 uur per week betrokken bij het faciliteren van dit project en de eventuele opvolging.</p> <p>De opbrengst van dit project wordt in april '26 verwacht. Momenteel lopen gesprekken vanuit de consortiapartners om dit project op te volgen in oktober '26 naar een landelijke onderzoek waarbij niet scenario's, maar representatief onderzoek centraal staat. Dit is uiteraard in lijn met de resultaten van dit onderzoek.</p>
23.	Pilot multi-channelaanpak digitale preventie helpdesk (PVO Limburg)	Ja, via PVO NL	Na de financiële stimulans van de City Deal heeft de tweede interventie, preventie helpdesk in de regio Limburg, een doorstart gemaakt met partijen uit Limburg (gemeenten, provincie, PVO en onderwijs). Lokaal is deze interventie voorlopig geborgd. Het Limburgse dialect wat gebruikt wordt door de helpdesk en het gebruik van MBO ICT studenten maakt dat deze interventie vooral een lokale oriëntatie heeft en zich niet direct laat opschalen.
24.	Hackhelpdesk: digitale eerstehulpverlening (PVO Zebra)	Ja, via PVO NL	Na de stimulans van de City Deal geheel is de HackHelpdesk is ondergebracht bij PVO NL. Het PVO gebruikt deze tool momenteel landelijk om vragen van ondernemers te kunnen beantwoorden.

25.	MKB Cyber Alarmcentrale (Saxion Hogeschool)	Borging loopt nog	<p>De stuurgroep heeft in juni 2025 het besluit genomen om nog eens aanvullende gelden toe te kennen aan deze interventie. Deze was bedoeld om de externe communicatie van deze interventie voor de pilot in oktober 2025 te professionaleren, een communicatie tool te maken voor de verschillende betrokkende partijen, zodat de mkb-er door elke partij op dezelfde wijze wordt geholpen en om het ontwerp te perfectioneren.</p> <p>Er worden momenteel gesprekken gevoerd vanuit MKB NL, DTC (straks NCSC), JenV om dit project te kunnen borgen. MKB NL zou deze interventie graag willen agenderen voor het nieuwe Actieprogramma Veilig Ondernemen. Het wegvallen van de subsidie laat er voornamelijk niet toe dat het project stopt. De leden van het consortium hebben zelf middelen verzameld om het project in ieder geval nog gedeeltelijk te kunnen opschalen naar Oost en Noord-Nederland.</p> <p>Verschillende publieke en private partijen hebben aangegeven de meerwaarde van dit initiatief te zien. Denk hierbij bijvoorbeeld aan de politie, de Fraudehelpdesk, Cyberveilig NL, DTC/NCSC, MKB NL/VNO NCW, PVO NL, Northwave. Dit onderstrepen ze door in-kind aan te sluiten of financieel ondersteunen.</p> <p>De daadwerkelijke implementatie van het initiatief in het bestaande bestel is echter daarmee nog geen realiteit. Het project voorziet in een behoefte die eerder werd vastgesteld in het Actieprogramma Veilig Ondernemen. De kennis over mogelijke prototypes van een incidentresponse mag niet verloren gaan. Nu wordt dit nog voorkomen doordat inmiddels bijna alle relevante partijen die betrokken zijn bij de opvolging van een cyberincident direct of indirect betrokken.</p> <p>Voor de lange termijn is de borgingsvraag nog onbeantwoord. De kennis en partners die via een informele netwerkstructuur tot stand zijn gekomen vragen om duurzame borging in een landelijk gestructureerd stelsel. Het enige landelijke stelsel, waarbinnen incidentrespons één van de aandachtsgebieden is, is het Cyberweerbaarheidsnetwerk van het NCSC.</p>
26.	Versterken cyberweerbaarheid van ketens (Haagse Hogeschool)	Borging loopt nog	<p>Het onderzoek naar Versterken cyberweerbaarheid van ketens leidt tot een blauwdruk voor effectieve samenwerking aan cyberweerbaarheid binnen ketens van mkb-ers. De meerwaarde van deze blauwdruk is dat cyberweerbaarheid binnen de keten beter kan worden georganiseerd waardoor de cyberveiligheid van de mkb-ers wordt vergroot. Het wordt t.z.t. via de website van het CCV ter beschikking gesteld.</p>
27.	Keurmerk OT Security bij mkb (CCV Keurmerken)	Borging loopt nog, mogelijk t.z.t via afdeling Keurmerken van het CCV	<p>Dit project levert een keurmerk op dat specifiek gericht op het vergroten van de weerbaarheid van OT bij ondernemers en wordt toegevoegd aan het CyRa model. Deze interventie levert een keurmerk op voor de beveiliging van de operationele technologie binnen het mkb.</p> <p>Uit de praktijk blijkt dat er steeds meer apparaten direct op het internet worden aangesloten, zonder dat er duidelijke digitale veiligheidsvoorschriften worden nageleefd. Dit geldt ook voor operationele machines, zoals bijvoorbeeld snijmachines, drukpersen die op het internet worden aangesloten terwijl ze met oude onveilige software werken.</p> <p>Door dit keurmerk komt er, naast de huidige focus op de beveiliging van computers, meer aandacht voor de cyberweerbaarheidseisen van operationele technologie.</p>

			Het keurmerk is begin november opgeleverd door het CCV en kan door alle mkb-ers worden gebruikt
28.	Cyberbuddies: van awareness naar adaptatie binnen het mkb (PVO/VAR Rotterdam)¹	Ja, op elementen geborgd	Het project Cyberbuddies: van awareness naar adaptatie binnen het mkb (PVO/VAR Rotterdam) organiseert bedrijfsbezoeken waarbij IT-studenten maatwerkadvies geven en direct uitvoeren om ondernemers te helpen bij het implementeren van cyberveiligheidstips.
29.	Cyberchef (gemeente Amersfoort)	Ja, op elementen geborgd	Het project Cyberchef (gemeente Amersfoort) wil mkb-ondernemers weer chef laten zijn van hun digitale keuken door hen te ondersteunen met IT-studenten en lokale partners.
30.	Friese agrarische sector cyberproof (gemeente Leeuwarden)	Ja, op elementen geborgd	Het project Friese agrarische sector cyberproof (gemeente Leeuwarden) heeft als doel de digitale weerbaarheid van de agrarische sector in Friesland te verhogen door middel van voorlichting, IT-scans, en speciaal ontwikkelde webpagina's en webinars.
31.	Gastveilig Hazeldonk – Digitaal Vitaal Breda (gemeente Breda)	Ja, op elementen geborgd	Het project Gastveilig Hazeldonk – Digitaal Vitaal Breda (gemeente Breda) richt zich op het verbeteren van de fysieke veiligheid en weerbaarheid van bedrijven in het proefgebied Hazeldonk door middel van digitale middelen en procesmaatregelen.
32.	Living Lab Cyberweerbaarheid & Ransomware mkb (gemeente Groningen)	Ja, op elementen geborgd	Het project Living Lab Cyberweerbaarheid & Ransomware mkb (gemeente Groningen) richt zich op het veilig laten ondernemen van het mkb in Noord-Nederland door middel van een branchegerichte aanpak, het vergroten van bewustwording bij ondernemers, en samenwerking tussen overheid en bedrijfsleven.
33.	Watersportbedrijven en havens cyberveilig (gemeente Súdwest-Fryslân)	Ja, op elementen geborgd	Het project watersportbedrijven en havens cyberveilig (gemeente Súdwest-Fryslân) richt zich op het weerbaarder maken van watersportbedrijven binnen de gemeente Súdwest-Fryslân op het gebied van cyberveiligheid en het vergroten van bewustwording over de risico's die ze lopen.
34.	Sterkere schakels versterken de keten! (RIVOB)	Ja, op elementen geborgd	Het project Sterkere schakels versterken de keten! (RIVOB) richt zich op het vergroten van de cyberweerbaarheid van kleinere ondernemers door hen tien uur gratis hands-on ondersteuning te bieden via een 'Shared Cyberprofessional' en hulpkaarten te ontwikkelen waarmee de ondernemer zelf aan de slag kan.
35.	Pilot cyberassistentie (RIVOB)	Ja, op elementen geborgd	Het project pilot cyberassistentie (RIVOB) ondersteunt vijftig ondernemers bij het opzetten van een solide basis voor hun cyberweerbaarheid met behulp van een gedeelde cyberprofessional voor 50 uur, en creëert een blauwdruk voor andere organisaties om het mkb beter te ondersteunen in hun cyberweerbaarheid.

¹ De projecten 28 t/m 35 zijn niet geborgd in zijn totaliteit, ze zijn op elementen geborgd (zoals vastgesteld in de stuurgroep van 18 juni 2025). Volgens PVO NL en het Digital Trust Center (DTC) heeft het wel organisaties geïnspireerd om bepaalde delen over te nemen. Daardoor komen bepaalde kenmerken van dit project terug in projecten van andere organisaties in Nederland zoals bijvoorbeeld MKB Nederland/ VNO NCW, PVO, Cyberweerbaarheidscentra.

--	--	--	--

4. Online aangejaagde ordeverstoringen (OAOV)

	NAAM	GEBORGD?	TOELICHTING
36.	Offline aangejaagde online ordeverstoringen	Ja, via het CCV en de gemeente Alkmaar	Gemeente Alkmaar blijft contactpersoon en is projecteigenaar. CCV plaatst het op de website. Ook wordt de informatie in andere, bestaande instrumenten gecoördineerd. Na ontwikkeling kunnen de instrumenten via het CCV geborgd en op de website van het CCV beschikbaar gesteld worden.
37.	Versterking kennispositie gemeenten regio's Midden-Nederland en Oost-Nederland op het terrein van online onderzoek en analyse van hun uitvoeringspraktijk	Ja, via het CCV en Bureau RVS	Momenteel is bureau RVS eigenaar. In 2026 wordt de interventie geïncorporeerd in de actieagenda van de bestuurlijke werkgroep Maatschappelijke onrust van de regio Midden-Nederland, die samen met de overige actieplannen is vastgesteld door het Regionaal Veiligheidscollege van Midden-Nederland.
38.	Ontwerp handreiking: inzet noodbevelsbevoegdheid in geval van OAO	Ja, via het CCV en de gemeente Utrecht	De gemeente Utrecht is op dit moment eigenaar, vervolgens wordt de handreiking op de website van het CCV geplaatst. Zo wordt de interventie geborgd en onder de aandacht gebracht bij gemeenten, politie en OM.
39.	Training Online Aangejaagde Ordeverstoringen	Ja, via het CCV en de VAR, Werkgroep Cyberveiligheid Noord-Nederland, RIVB.	Momenteel zijn de VAR, Werkgroep Cyberveiligheid Noord-Nederland, NHSV en RIVB-eigenaar. In 2026 zal het CCV de modules beschikbaar stellen via de website.
40.	"ConNect: Samen bouwen aan een online interventiematrix"	Ja, via het CCV, de gemeente Amsterdam en Actiecentrum Veiligheid en Zorg (Veiligheidshuis)	Het project staat beschreven op de website van het CCV, de factsheet is daar te downloaden. Ook is de informatie verwerkt in het barrièremodel Online Aangejaagde Orde Verstoringen. Dit model wordt actief door gemeenten gebruikt. Het Actiecentrum Veiligheid en Zorg (Veiligheidshuis) is momenteel eigenaar.

Het CCV is momenteel in gesprek met de Directie Veiligheid en Bestuur (DVB van het ministerie van JenV m.b.t. een werkplan voor 2026 op OAOV. Onderdeel van die activiteiten is om met de regio's in gesprek te gaan hoe de City Deal projecten geïmplementeerd kunnen worden.