PLATFORM IVZ

SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: Ontwikkelplatform digitale criminaliteit | Basisteams en gemeenten in Twente	
Aanleiding van probleem/ uitdaging	De cijfers rondom digitale criminaliteit zijn hoog. Niet alleen is het aantal slachtoffers hoog, ook financiële schade, mentale en emotionele impact op inwoners worden steeds zichtbaarder. De uitingsvormen fenomenen ontwikkelen zich in razend tempo. Deze groeiende impact benadrukt de noodzaak om digitale criminaliteit structureel en integraal aan te pakken. De sleutel tot zo'n aanpak ligt voor een belangrijk deel op lokaal niveau. Lokale betrokkenen staan het dichtst bij inwoners, ondernemers en organisaties die risico lopen slachtoffer (of dader) te worden. Juist daarom is het essentieel dat zij een gedeeld begrip ontwikkelen van het lokale dreigingsbeeld, interventiemogelijkheden en rolverdeling. Hoewel zowel gemeenten als de politie hun eigen taken en verantwoordelijkheden hebben op het gebied van digitale veiligheid, liggen er kansen om de structurele samenwerking te versterken. Gezamenlijke regie en onderlinge afstemming is nodig zijn om effectief op te treden. In de praktijk verschilt de aanpak per gemeente en is de samenwerking afhankelijk van individuele inzet en incidentele projecten. Dat belemmert een duurzame en solide lokale aanpak. Lokale professionals herkennen de noodzaak te acteren op het thema en het belang van samenwerking, maar missen ondersteunende kaders, een gedeeld veiligheidsbeeld en een manier om digitale criminaliteit gezamenlijk en planmatig te benaderen.
Betrokken actoren	Onder de doelgroep scharen we onderstaande rollen bij alle gemeenten en basisteams in Twente. Dit betekent deelname van 14 gemeenteambtenaren (één per gemeente) en minimaal vijf politiemedewerkers. • Digitaal Wijkagent • OS-A / OE-W politie • OOV-er's / gemeentelijk themahouders
Doelstelling	Het structureel versterken van de samenwerking tussen politie en gemeenten op lokaal niveau. **Gedeeld veiligheidsbeeld** Welke fenomenen kennen we? Hoe ziet het speelveld er in mijn gemeente uit? Wat prioriteren we? **Rolduidelijkheid en verantwoordelijkheid** Herkennen en pakken van de (regie)rol en werken aan een interne structuur om digitale criminaliteit aan te pakken, bijvoorbeeld door samen te werken met andere domeinen en partners. **Mindset en handelingsperspectief** Aan de hand van een gedeeld beeld over de aard en omvang van het probleem een concreet handelingsperspectief creëren, bijv. door het inzetten van verschillende interventies. Een ontwikkelplatform waarin politie en gemeenten gedurende een jaar gezamenlijk werken aan kennisopbouw, rolverduidelijking en concrete interventies biedt daarom een krachtig antwoord op deze uitdaging. Hiermee wordt een stevige basis gelegd voor een duurzame, lokale aanpak van digitale criminaliteit. Met meer structuur, meer gezamenlijke inzichten en een heldere rol- en taakverdeling richting de toekomst.
Projectresultaat	Het organiseren van een ontwikkelplatform waarop de basisteams in Twente, samen met betrokkenen op het thema vanuit de bijbehorende gemeenten, werken aan het structureel versterken van de samenwerking op het thema digitale criminaliteit. Voor de periode van een jaar worden de samen te stellen teams gefaciliteerd op met een eigen geformuleerde doelstelling aan de slag te gaan. Door middel van een start-, tussen-, en

Opdrachtnaam: Ontwikkelplatform digitale criminaliteit | Basisteams en gemeenten in Twente	
	eindbijeenkomst delen we kennis over het thema en bundelen we alle opgedane inzichten en resultaten. Deze bijeenkomsten worden daarnaast benut voor kennisverhogen door middel van relevante sprekers. Tijdens de startbijeenkomst wordt stilgestaan bij kennismaking en worden deelnemers begeleid naar een concrete opdracht waar zij de komende periode als teams samen aan gaan werken. De inzichten en resultaten worden tijdens een slotbijeenkomst gebundeld en besproken, waarna er een advies wordt opgesteld over vervolgstappen. Het advies gaat over een mogelijk vervolg van deze samenwerkingsvorm en over het benutten van opgedane inzichten en resultaten Twente breed.
Monitoring / voortgangsbewaking	Projectleider IVZ en politie faciliteren een stand van zaken halverwege het traject en een eindrapportage ten behoeve van de stuurgroep digitale veiligheid en het DVO.
Randvoorwaarden	• Ieder basisteam stelt zijn digitaal wijkagent in de gelegenheid om deel te nemen aan deze samenwerking. • Iedere gemeente verzorgt deelname met collega(s) actief op het thema • Er wordt een procesbegeleider met didactische vaardigheden betrokken om het proces te begeleiden. Deze kan eventueel in de hoek van het Q-lab van de politie Oost NL gevonden worden.
Afbakening	• Het ontwikkelplatform wordt in eerste instantie georganiseerd voor een jaar. • Het is nadrukkelijk de bedoeling dat basisteam met gemeenten hun eigen idee ontwikkelt, waarmee zij gezamenlijk eigenaar zijn het project.
Relatie andere initiatieven en Ontwikkelingen	• In januari 2025 is een bijeenkomst tussen politie en gemeenten georganiseerd gericht op de lokale betrokkenen op dit thema. Deze bijeenkomst werd als waardevol ervaren. • Binnen de nieuwe projectenaanpak vanuit het Platform IVZ Twente zitten diverse projecten die door versterkte samenwerking tussen politie en gemeenten bestendigd kunnen worden.
Risico's / onverwachte zaken /effecten	• Onvoldoende deelname en commitment vanuit politie • Onvoldoende deelname en commitment vanuit gemeenten
Planning en mijlpalen	Q4 2025 commitment vanuit DMO politie en stuurgroep digitale veiligheid Q1 2026 matchmaking politie/gemeente en procesbegeleider benaderen Q2 (maart 2026) Startbijeenkomst Q3 (juni 2026) Voortgangsbijeenkomst Q4 (november 2026) Resultaat bijeenkomst Q4 (december 2026) Evaluatie en adviesrapportage 2027
Financiën	Locaties, sprekers en andere benodigdheden worden zoveel als mogelijk in kind georganiseerd. In geval van kosten, zoals lunch tijdens de gezamenlijke sessies, worden deze 50-50 door Platform IVZ en politie gedragen.
Bronnen	Een structurele lokale samenwerking in de aanpak van digitale criminaliteit wordt aanbevolen vanuit de literatuur en experts op het thema online criminaliteit, zoals in:

Opdrachtnaam: Ontwikkelplatform digitale criminaliteit | Basisteams en gemeenten in Twente	
	Spithoven, R., Jansen, J., Drenth, A.R. & Leukfeldt, E.R. (2022). Redactioneel. Wijk + web. De noodzaak van een lokale aanpak van cybercriminaliteit. Tijdschrift voor Veiligheid. Leukfeldt, E.R., Misana-ter Huurne, E.F.J. & Spithoven, R. (2020). De lokale aanpak van cybercrime. In: C. de Poot, E. Lievens, W. Stol & L. De Kimpe (eds.). P*olitie en cybercrime. Cahiers Politiestudies*, jrg. 2020, nr. 3, p. 203-223. Kort, J. & R. Spithoven (2021) *De coronacrisis als cyberkeerpunt? Op zoek naar lokaal handelingsperspectief in de aanpak van gedigitaliseerde criminaliteit.* Politie, agenda Gebiedsgebonden Politie.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: Speelveldverkenning digitale weerbaarheid jeugd in Twente	
Aanleiding van probleem / uitdaging	Experts en praktijkprofessionals signaleren toenemende zorgen over de online leefwereld van jongeren (sociale media, gaming, chat, platforms). Het gaat om risico's zoals online seksuele grensoverschrijding (o.a. sextortion, onvrijwillige verspreiding van beelden), desinformatie en online haat, maar ook om aanzuigende werking richting digitale criminaliteit (phishing, DDoS, credential stuffing, fraude). Voor overheden, onderwijs en ketenpartners is het een complexe uitdaging hierop aan te sluiten: de digitale omgeving verandert snel, jongeren bewegen zich in besloten of vluchtige kanalen, en de verantwoordelijke actoren zijn versnipperd over domeinen (onderwijs, jeugd, veiligheid, zorg, sociaal, justitie). In Twente zijn uiteenlopende preventie initiatieven actief (binnen scholen, jongerenwerk, Stichting Halt, politie/OM, bibliotheken/mediawijsheid, GGD, bibliotheek, ouders, landelijke loketten). Een regionaal totaalbeeld van het speelveld ontbreekt. Hierdoor benutten we kansen onvoldoende en blijven schaalbare, Twentse afspraken en ondersteuning versnipperd. Wie doet wat en vanuit welke rol? Waar zitten gaten, overlap of kansen voor het versterken van initiatieven? Nieuw momentum: In juni 2025 zijn de nieuwe kerndoelen voor burgerschap en digitale geletterdheid (SLO, primair en voortgezet onderwijs) vastgesteld. Deze kerndoelen verplichten scholen de komende jaren structureel aandacht te geven aan thema's zoals digitale veiligheid, mediawijsheid, online gedrag, en maatschappelijke verantwoordelijkheid online. Dit biedt een goed moment om onderwijs als essentiële partner te betrekken in het regionale preventiespeelveld. Door gezamenlijke inzet kunnen scholen niet alleen voldoen aan de kerndoelen, maar ook bijdragen aan duurzame gedragsverandering en digitale weerbaarheid onder jongeren.
Betrokken actoren	• Expertteam digitale veiligheid Platform IVZ • Themagroep Jeugd en Veiligheid ZVS Twente • Stichting Halt • Jongerenwerk (Kwaliteitskring Twente) • Politie Oost-Nederland • OM • Onderwijs (PO, VO, mbo/hbo, passend onderwijs) • Risk Factory Twente • Brede schil aan partners waaronder Raad voor Kinderbescherming, Reclassering, Jeugdbescherming Overijssel, bibliotheken, …)
Doelstelling	Een eenduidig, actueel overzicht van partijen, interventies en werkzame lijnen, inclusief kansen, knelpunten en randvoorwaarden om preventie op Twents niveau te versterken, met nadrukkelijke koppeling aan de implementatie van de nieuwe kerndoelen in het onderwijs. 1. Het Twentse speelveld van preventie rond online onveiligheid bij jeugd (8-18 jaar) systematisch in kaart brengen: actoren, rollen, doelen, doelgroepen, interventies, dekking per gemeente/onderwijslaag en samenwerkingslijnen. 2. Gezamenlijk zicht krijgen op kansen en belemmeringen (governance, mandaat, expertise, gegevensdeling, toegang tot doelgroepen, financiering, aansluiting op nieuwe kerndoelen). 3. Opleveren van concrete keuzerichtingen en Twentse afspraken: waar schaal je op, waar sluit je aan, welke witte vlekken pak je regionaal op, en hoe borg je kwaliteit en effect.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: Speelveldverkenning digitale weerbaarheid jeugd in Twente	
Projectresultaat	Mogelijke concrete producten: • Speelveldkaart (visual + toelichting): stakeholders, domeinen, initiatieven, interventies, dekking per gemeente/onderwijslaag, …) • Analyse kansen & knelpunten: o.a. aansluiting bij jeugd, deskundigheidsbevordering, rol school/ouders, rol zorg en veiligheid en OOV, verbinding preventie met repressie en nazorg. Twentse routekaart Preventie Online Onveiligheid: • Thematische actielijnen (bijv. sextortion-preventie en afhandeling; mediawijsheid; eerste-delicten cybercrime; meld- en hulpstructuur), • Keuzes 'regionaal organiseren vs. Lokaal uitvoeren', • Governance (regie, werkgroep, kennisdelingskalender), • Indicator voor monitoring • Poppeling met de implementatie van de nieuwe kerndoelen burgerschap en digitale geletterdheid in PO en VO.
Monitoring / voortgangsbewaking	• Stuurgroep ZVS Twente en stuurgroep digitale veiligheid Twente: gezamenlijk opdrachtgeverschap. • Uitvoering door afvaardiging uit themagroep jeugd en veiligheid en expertteam digitale veiligheid samen met diverse samenwerkingspartners binnen de doelgroep Jeugd.
Randvoorwaarden	• (Bestuurlijk) draagvlak van alle partners om écht aan de slag te gaan met digitale weerbaarheid van de jeugd in Twente. • Aansluiting bij bestande regionale overlegtafels (jeugd, veiligheid, onderwijs) • Actieve betrokkenheid en belang vanuit het Twentse onderwijs
Afbakening	• Focus: preventie en vroegsignalering online onveiligheid bij jeugd • Geen casusafhandeling of repressie • Geografisch: regio Twente (alle deelnemende gemeenten). • Definitie digitale weerbaarheid n.n.t.b.
Relatie andere initiatieven en ontwikkelingen	• Er ligt een nadrukkelijke relatie met (momentum) de nieuwe kerndoelen binnen het onderwijs. Het moet zicht geven op en aansluiten bij partners en initiatieven die lopen in Twente. • Deze verkenning ordent en verbindt, geeft keuzes voor Twentse schaal en borging, en ondersteunt scholen bij hun wettelijke opdracht binnen het nieuwe curriculum. • Bij het Veiligheidsnetwerk Oost-Nederland speelt een soortgelijk vraagstuk. Daar waar mogelijk wordt de samenwerking gezocht bij planvorming op Oost-Nederland schaal.
Risico's / onverwachte zaken /effecten	- Versnipperd eigenaarschap/ mandaat - Lage respons vanuit partners en betrokkenen, specifiek het onderwijs.
Planning en mijlpalen	Een nadere planning is uit te werken door de te vormen werkgroep van dit project. Bij goedkeuring is de planning om in Q1 en Q2 de werkgroepvorming en nadere uitwerking vorm te geven, om de rest van 2026 aan de slag te kunnen.

Opdrachtnaam: Speelveldverkenning digitale weerbaarheid jeugd in Twente	
Financiën	Projectbudget benodigd. Nog nader uit te werken. Denk aan mogelijke jongerenparticipatie, visualisaties en uitwerking producten, middelen, bijeenkomsten.
Bronnen	- Definitieve conceptkerndoelen burgerschap en digitale geletterdheid

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: Monitor online leefwereld jeugd in Twente	
Aanleiding van probleem / uitdaging	De digitale leefwereld is voor jongeren een integraal onderdeel van hun identiteit, sociale relaties en gedragingen. Binnen deze online omgevingen ontstaan ook risico's: online grensoverschrijding, desinformatie, (digitale) criminaliteit, polarisatie, prestatiedruk en mentale belasting. Beleidsmatig is er groeiende behoefte aan feitelijke, actuele en kwalitatieve inzichten in de online leefwereld van Twentse jongeren. Veel partijen beschikken nu vooral over losse signalen (incidentmeldingen, schoolenquêtes, Halt-data, jongerenwerkervaringen), maar geen samenhangend Twents beeld. In andere regio's, o.a. Amsterdam (*Jong InZicht – Online Jongeren Trendmonitor*) zijn succesvolle methodieken ontwikkeld om structureel en participatief data te verzamelen over hoe jongeren online communiceren, leren, ontspannen, risico's ervaren en hulp zoeken. In Twente biedt het bestaande netwerk van partijen rondom jeugd en veiligheid en de fysieke bewegingswereld van veel jeugd op Twentse schaal een goede basis om dit te realiseren.
Betrokken actoren	• Jongeren in Twente (met en via jongerenwerkorganisaties) • Jongerenwerk (Kwaliteitskring jongerenwerk Twente) • Themagroep Jeugd en veiligheid ZVS en expertteam digitale veiligheid platform IVZ
Doelstelling	Een structureel instrument gedragen door gemeenten, jongerenwerk, partners én de jongeren zelf om trends, signalen en beleving van jongeren in hun online leefwereld in kaart te brengen, te duiden en te vertalen naar lokaal en regionaal beleid en preventie. • Ontwikkelen van een Twentse Monitor Online Leefwereld Jeugd die halfjaarlijks kwantitatieve en kwalitatieve inzichten oplevert over online gedrag, risico's, kansen en behoeften van jongeren (12-22 jaar). • Verankeren van jongerenparticipatie in het hele proces • Bieden van concrete beleids- en handelingsinformatie voor gemeenten, scholen, jongerenwerk, politie en zorgpartners op basis van de waargenomen trends en ontwikkelingen.
Projectresultaat	• Monitorontwerp en meetkader: opbouw van vragenlijst, kwalitatieve formats, participatiemethoden (storytelling, focusgroepen, online panels). • Online dashboard of factsheetreeks: toegankelijk overzicht van trends, thema's, quotes en duiding. • Jongerenpanel Twente: structurele groep jongeren die mee-ontwerpt, test en interpreteert; gekoppeld aan jongerenwerk. • Handreiking per verschenen monitor: hoe gemeenten en partners de inzichten kunnen toepassen in beleid en interventies.
Monitoring / voortgangsbewaking	• Stuurgroep ZVS en stuurgroep digitale veiligheid Twente gezamenlijk bestuurlijk opdrachtgever. • Samen te stellen werkgroep vanuit themagroep en expertteam met aantal betrokken partijen
Randvoorwaarden	• Ophalen toegevoegde waarde op Twentse schaal.

Opdrachtnaam: Monitor online leefwereld jeugd in Twente	
	• Toegang tot en medewerking van jongeren voor participatie
Afbakening	• Focus: beleving en gedrag van jongeren in Twente in hun digitale leefwereld; signalering van risico's en kansen; niet: individuele casuïstiek of repressie. • Geografisch: regio Twente (alle deelnemende gemeenten). De monitor is wel toegankelijk en beschikbaar buiten Twente voor wie er zijn/haar voordeel mee wil doen. • Thema's: n.n.t.b. door te vormen werkgroep (afbakening op zorg & veiligheidsthema's)
Relatie andere initiatieven en ontwikkelingen	• Dit initiatief wordt op een aantal andere plekken met toegevoegde waarde uitgevoerd. Het ophalen van werkwijze en inzichten van bestaande regionale monitors vormt een vliegende start. • Sluit goed aan op de nieuwe kerndoelen binnen het onderwijs. • Sluit goed aan op de ontwikkeling die jongerenwerk doormaakt, waarbij er steeds meer nadruk komt te liggen op online jongerenwerk. • Kennis en herkennen van signalen en trends online past goed bij brede uitrol van vroegsignalering in Twente.
Risico's / onverwachte zaken /effecten	• Onvoldoende toegang en medewerking jongeren voor participatie • Verspinnering of overlap met bestaande monitors
Planning en mijlpalen	Specifieke planning nader te bepalen door te vormen werkgroep. Globale planning is om in Q1 en Q2 een werkgroep samen te stellen en te starten met het project, met als doel om in januari 2027 de eerste monitor te laten verschijnen, met vervolgens een nader te bepalen verschijningsfrequentie.
Financiën	Uit te werken door de werkgroep, met aandacht voor: - Keuze in productvorm: online dashboard en/of visual-pdf uitwerking. - Rol van jongerenparticipatie
Bronnen	Jong Inzicht - De Online Jongeren Trendmonitor - openresearch.amsterdam Online Jongerenwerk: Werken in de online leefwereld van jongeren Straatwaarden: informatiepositie van partners in de online leefwereld.

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: Cyberethiek in mbo-onderwijs Twente	
Aanleiding van probleem / uitdaging	Bijna de helft van de jongeren die ICT-gerelateerd onderwijs volgen doet iets aan cybercrime (Kranenbarg & Roks, 2022). Van het raden van wachtwoorden tot aan het zoeken naar kwetsbaarheden in systemen van organisaties. Zowel uit onderzoek als uit ervaringen van de politie blijkt dat mbo-studenten in een ICT richting een verhoogde kans op potentieel daderschap van criminaliteit hebben. Volgens de onderzoekers is ethiek verweven in ict-onderwijs een cruciale stap om jongeren uit de cybercrime te houden. De gemeente Enschede is voornemens om in 2026 een re_B00TCMP te organiseren, op een iets andere wijze dan dat ze dit in 2025 gedaan hebben. Een event waarbij jongeren met hoge digitale vaardigheden leren over de kansen en uitdagingen die er in de digitale wereld zijn. Het re_B00tcmp sluiten we af met een grote hack challenge waarbij een winnaar wordt bekroond Hiermee ontstaat er een mooie samenwerkingskans om dit event te combineren met cyberethiek lessen binnen het ICT opleiding op het ROC.
Betrokken actoren	• ICT-opleidingen ROC van Twente • Expertteam digitale veiligheid Platform IVZ • Themagroep Jeugd en Veiligheid vanuit de samenwerking op Zorg, Veiligheid en Straf Twente • Preventie met Gezag Enschede
Doelstelling	Met de leerlijn over cyberethiek leren studenten hoe ze hun vaardigheden op een verantwoorde manier kunnen inzetten. Ze ontwikkelen ethisch bewustzijn en worden aangezet om na te denken over de impact van hun digitale handelingen. Door realistische casussen, interactieve opdrachten en discussies ontdekken studenten hoe ze hun talenten op een positieve en legale manier kunnen inzetten. Dit leermiddel helpt toekomstige ICT-professionals niet alleen technisch bekwaam, maar ook ethisch verantwoord te handelen in een wereld waarin digitale keuzes steeds belangrijker worden. Hiermee dragen we bij aan het verkleinen van de kans op crimineel gedrag binnen deze doelgroep in Twente. Tijdens de re_B00TCMP nemen jongeren nemen deel aan verschillende presentaties en workshops waarin ze meer inzicht krijgen in de wijze waarop digitale vaardigheden op een uitdagende en legale manier ingezet kunnen worden.
Projectresultaat	Op de ICT-opleiding van het ROC van Twente worden drie lessen over cyberethiek verzorgd, met als afsluiting een gezamenlijk event re_B00TCMP. In samenspraak met het ROC van Twente en Preventie met Gezag Enschede kiezen we drie van de volgende modules. Het lesmateriaal is gratis beschikbaar en is in samenwerking met de VU, het OM, de politie en mbo digitaal ontwikkeld. • Je hebt altijd een keuze – Wat betekent ethisch handelen in de digitale wereld? • Game on of game over? – Wanneer wordt digitaal experimenteren een risico? • Leads, mag je ze openen? – Hoe ga je om met verdachte berichten en datalekken? • What the hack! – De dunne lijn tussen ethisch hacken en cybercriminaliteit. • Hoe erg is het nu? – Wat zijn de gevolgen van cybercrime voor individuen en bedrijven? • En jij? – Hoe maak jij bewuste keuzes in jouw online gedrag? De lessenreeks wordt afgesloten met het re_B00TCMP. Het re_B00tcmp sluiten we af met een grote hack challenge waarbij een winnaar wordt bekroond.

Opdrachtnaam: Cyberethiek in mbo-onderwijs Twente	
Monitoring / voortgangsbewaking	In samenwerking met het ROC wordt een planning gemaakt voor de inzet van het beschikbare lesmateriaal. Er wordt een evaluatie opgesteld van de ervaringen van studenten, (gast)docenten en de verschillende betrokken partij. Het doel is om bij een positieve evaluatie te onderzoeken hoe de partijen samen kunnen zorgen voor een uitbreiding naar een breder palet opleidingen en het bestendigen van cyberethiek binnen het mbo ICT-onderwijs in Twente.
Randvoorwaarden	• Er zijn voldoende (gast)docenten beschikbaar voor het verzorgen van de lessen cyberethiek
Afbakening	Het betreft in het begin primair de ICT opleiding mbo van het ROC in Hengelo. Mogelijk ook voor andere opleidingsrichtingen (zoals software ontwikkelaar) interessant en relevant.
Relatie andere initiatieven en ontwikkelingen	Zowel voor het PO als het VO is er een lesaanbod op de Risk Factory in Enschede. Hier is er met verschillende scenario's aandacht voor digitale veiligheid. Aandacht binnen het onderwijs in Twente een leeftijdscategorie hoger is hier een goede aanvulling op.
Risico's / onverwachte zaken /effecten	• Onvoldoende ruimte binnen de opleidingsroosters voor de lessen • Er zijn onvoldoende (gast)docenten beschikbaar om de lessen te verzorgen
Planning en mijlpalen	Planning in samenspraak met het ROC en samenwerkende partijen. Q4 2025: afstemming met ROC van Twente over planning + werven in indelen van gastdocenten Q1 2026: start met de lessen binnen de opleiding Q2 2026: event re_B00TCMP Q3 2026: Evaluatie project en mogelijke herhaling en uitbreiding.
Financiën	Het lesmateriaal is gratis beschikbaar (zie link bij bronnen). Het uitgangspunt is dat lessen dan wel vanuit het ROC zelf, danwel met mensen uit eigen netwerk gegeven kunnen worden en daarmee kosten neutraal. Voor de re_B00TCMP is er geld beschikbaar vanuit preventie met gezag Enschede. Ook in te zetten voor ondersteunend materiaal (presentje gastdocent, lesmateriaal drukken etc)
Bronnen	• Cybercrime verminderen? Besteed meer aandacht aan cyberethiek in ict-onderwijs - MBO Digitaal • Cyberethiek: Cyberethiek • re_B00TCMP | politie.nl

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: Themadag online leefwereld jeugd Twente | donderdag 19 maart 2026	
Aanleiding van probleem / uitdaging	De digitale leefwereld van jongeren is in korte tijd fundamenteel veranderd en ontwikkelt zich voortdurend. Voor professionals, beleidsmakers en betrokkenen rondom jeugd en veiligheid vraagt dit om actuele kennis, gezamenlijke reflectie en handelingsperspectief. De themadag *"Verbonden of Verloren?"* biedt een ontmoetingsplek om inzichten, praktijkervaringen en regionale samenwerking op het snijvlak van jeugd, veiligheid en digitalisering te versterken. De themadag sluit aan bij andere projecten vanuit het programmaplan Jeugd en Veiligheid: *Speelveld preventie online/digitaal en Monitor online leefwereld jeugd in Twente*.
Betrokken actoren	De themadag wordt voorbereid door de volgende betrokkenen: Sylvia Huis in 't Veld – projectleider jeugd en veiligheid Ellen Bolster - Specialist Zorg & Veiligheid Politie en lid themagroep Marleen Kotkamp - Projectleider Preventie met Gezag Almelo en lid themagroep Jop Wieffer – Projectleider Digitale Veiligheid Platform IVZ Twente (en communicatie rondom themdag)
Doelstelling	- Vergroten van bewustwording over de online leefwereld van jongeren en de effecten op veiligheid en weerbaarheid en hulpvragen. - Versterken van de Twentse netwerksamenwerking van betrokkenen rondom jeugd en veiligheid. - Verbinden van kennis en praktijk via workshops, lezingen en ervaringsverhalen. - Inspireren tot actie: wat doet jouw organisatie morgen anders?
Projectresultaat	**Naam themadag: Verbonden of Verloren? Jongeren in het digitale tijdperk** **Datum:** Donderdag 19 maart 2026 **Locatie:** Risk Factory, Twente **Tijd:** 10.30–16.30 uur (inloop + workshops + lunch) Programma (in grote lijnen): **10.30 – Inloop & workshopkeuze** **11.00 – Plenair programma:** • Opening door bestuurder • Ervaringsverhaal • "De online leefwereld van jongeren" – Lezing • Introductie nieuw regionaal jeugdprogramma **12.30 – 13.10 – Netwerklunch** **13.10 –16.00 Break-outs / Workshops (2 rondes):** 1. Exposegroepen 2. Cyberbreinen 3. Online jongerenwerk 4. Sociale media & beïnvloeding 5. Criminele uitbuiting / geldezels 6. Online (seksueel) ongewenst gedrag 7. LVB-jongeren & online gedrag

Opdrachtnaam: Themadag online leefwereld jeugd Twente | donderdag 19 maart 2026	
	8. Docentperspectief online onderwijs 9. Hybride straatwereld **16.00 – Afsluitende opdracht / giveaway: Wat neem jij mee / ga jij morgen anders doen?** **Nazending:** overzicht workshops + factsheet regionaal programma + gadget
Communicatie	- Save the date verspreiden via netwerk Jeugd & Veiligheid Twente en betrokken partners (inclusief jongerenwerk): eind november - Online aankondiging met korte teasertekst en inschrijflink: december - Nazending met factsheet en overzicht opbrengsten.
Randvoorwaarden	Locatie incl. lunch is vastgelegd
Afbakening	Doelgroep themadag: Alle jeugdprofessionals vallende onder de samenwerkende organisaties van de themagroep Jeugd en Veiligheid in Twente.
Financiën	- Doorberekening kosten locatie Risk Factory - Vergoedingen voor spreker/workshops: Sylvia?
Bronnen	- Draaiboek themabijeenkomst 19 maart 2026

PLATFORM IVZ

SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: De rol van gemeenten in de aanpak van Online Criminaliteit | Afstudeeronderzoek	
Aanleiding van probleem / uitdaging	*Dit project betreft het afstudeeronderzoek van de projectleider t.b.v. de deeltijdmaster Veiligheid & Digitalisering.* Online criminaliteit is niet nieuw. Toch blijft het voor lokale overheden een zoektocht welke rol ze hebben in het voorkomen ervan. Vanuit hun verantwoordelijkheid voor openbare orde en veiligheid vervullen gemeenten een rol in de bestrijding van cybercrime en gedigitaliseerde criminaliteit (Vereniging van Nederlandse Gemeenten, 2022). Toch zijn zij zoekende naar de concrete invulling van die rol. Onder lokale overheden leeft vaak het beeld dat cybercrime zich buiten hun invloed afspeelt: daders aan de ene kant van de wereld, slachtoffers aan de andere (Leukfeldt, Spithoven, & Misana-ter Huurne, 2020). Terwijl van gemeenten wordt verwacht dat zij een rol (kunnen) spelen in alle fasen van veiligheid: van proactie en preventie tot nazorg. De probleemanalyse-fase is in juli 2025 afgerond met inbreng van diverse Twentse gemeenten, Veiligheidsnetwerk Oost-Nederland en diverse landelijke experts vanuit het CCV en VNG. De vervolgstap is het ontwerpen, uitvoeren evalueren van een interventie als bijdrage aan de oplossing van het probleem.
Betrokken actoren	• Master Veiligheid & Digitalisering • Saxion Hogeschool / Universiteit Twente • Platform IVZ Twente • Veiligheidsnetwerk Oost-Nederland
Doelstelling	• Het vergroten van de kennis van gemeentelijk medewerkers over het thema online criminaliteit, gericht op de rollen van gemeenten op dit thema. • Het bieden van handelingsperspectief voor gemeentelijk medewerkers om hun rol op het thema online criminaliteit invulling te kunnen geven.
Projectresultaat	Voor het ontwerpgerichte onderzoek is er gekozen op de interventie te richten op de componenten kennis en handelingsperspectief van gemeentelijk medewerkers. Er wordt een E-learning ontwikkeld die kan bijdragen aan het kennisniveau over het thema en de rollen van gemeenten, inclusief handelingsperspectief om verder te werken aan een goede invulling van deze rollen.
Monitoring / voortgangsbewaking	De ontwikkeling van de interventie is onderdeel van een afstudeeronderzoek. Begeleiding vindt plaats vanuit de Universiteit Twente en het lectoraat Online weerbaarheid van de Saxion Hogeschool.
Randvoorwaarden	• Wetenschappelijke onderbouwing van probleemanalyse tot aan interventieontwerp. • Beschikbaarheid van respondenten uit het Twentse netwerk
Afbakening	Uit de probleemanalyse komen diverse factoren die een rol spelen bij de complexiteit rondom de rol van gemeenten op het thema online criminaliteit. Er is gekozen voor een scherpe afbakening op kennis en handelingsperspectief t.b.v. de haalbaarheid binnen het afstudeerproces. Overige factoren binnen de probleemanalyse bieden wel kans voor vervolgonderzoek of een gezamenlijke Twentse aanpak.

Opdrachtnaam: De rol van gemeenten in de aanpak van Online Criminaliteit | Afstudeeronderzoek	
Relatie andere initiatieven en ontwikkelingen	Het onderzoek en de interventieontwikkeling heeft sterk raakvlak met de Twentse gezamenlijke aanpak, waarbij we vanuit een expertteam met gemeenten, politie, OM en partners samenwerking op het thema online criminaliteit.
Risico's / onverwachte zaken /effecten	• De uiteindelijke opgeleverde interventie heeft onvoldoende waardevolle toegevoegde waarde • De afstudeerfase duurt langer dan gepland
Planning en mijlpalen	Q2 2025: Probleemanalyse afgerond (Cijfer: 7) Q1 2026: Interventieontwerp en onderzoeksmethode gereed Q2 2026: Uitvoering en evaluatie interventie Q2 2026: Geplande einddatum afstuderen. 2027: Inzetten, door ontwikkelen of afwijzen van ontwikkelde interventie.
Financiën	N.v.t.
Bronnen	• **Van beleidsprioriteit en urgentie tot gestructureerde aanpak -** Een vooronderzoek naar de rol van gemeenten in de aanpak van online criminaliteit (Wieffer, 2025) • Informatie opleiding Veiligheid & Digitalisering

Opdrachtnaam: Zicht op online criminaliteit - informatiepositie	
Aanleiding van probleem / uitdaging	Om zicht te houden op digitale criminaliteit en de verschillende verschijningsvormen, trends en ontwikkelingen en dader- en slachtofferschap, is een goede informatiepositie belangrijk. De afgelopen projectperiode (2024-2025) stelde de politie in Twente Cyberbeelden beschikbaar. Een document met allerlei informatie gebaseerd op meldingen en aangiftes. Deze cyberbeelden konden zowel op regionaal als lokaal niveau worden uitgedraaid. Sinds medio 2025 worden deze cyberbeelden niet meer door de politie gefaciliteerd. In november 2025 is Zicht op Online Criminaliteit gelanceerd. Het dashboard Online Criminaliteit komt voort uit een samenwerkingsverband tussen verschillende lokale en landelijke overheden, geïnitieerd door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Het is opgezet door dezelfde initiatiefnemers als het dashboard Zicht op Ondermijning, dat ook in de regio Twente veel gebruikt wordt. Het Veiligheidsnetwerk Oost-Nederland is betrokken bij de doorontwikkeling van dit nieuwe dashboard.
Betrokken actoren	- Expertteam digitale criminaliteit - Zicht op Ondermijning / Zicht op Online criminaliteit - Veiligheidsnetwerk Oost-Nederland - Politie
Doelstelling	In Twente hebben we zicht op relevante cijfers en informatie rondom dader- en slachtofferschap. Gemeenten hebben op een toegankelijke manier zicht op de lokale situatie rondom online criminaliteit.
Projectresultaat	• Halfjaarlijkse update voor de regio Twente vanuit het dashboard t.b.v. het experteam, de stuurgroep en gemeenten. • Op aanvraag een update vanuit het dashboard op lokaal niveau.
Monitoring / voortgangsbewaking	Het betreft een nieuw gelanceerd dashboard dat nog volop in ontwikkeling is. Het Veiligheidsnetwerk Oost-Nederland is betrokken bij deze ontwikkelingen. Vanuit Twente kan via het VNON feedback worden gegeven en suggesties worden aangedragen.
Randvoorwaarden	Het dashboard blijft openbaar toegankelijk beschikbaar.
Afbakening	Het betreft een vrije toegankelijk dashboard via een webpagina. Iedereen kan hier naar eigen wens gebruik van maken. De rol van het expertteam betreft het actief betrekken van relevante data op Twents en lokaal niveau en het geven van benodigde duiding bij het dashboard.
Relatie andere initiatieven en ontwikkelingen	De Cyberbeelden zoals deze tot aan 2024 door de politie gegenereerd konden worden zijn niet meer beschikbaar.
Risico's / onverwachte zaken /effecten	• Voor de (potentiële) meerwaarde zijn we afhankelijk van de doorontwikkeling van dit landelijke initiatief.
Planning en mijlpalen	Q2 2026: Update vanuit het dashboard voor de regio Twente

Opdrachtnaam: Zicht op online criminaliteit - informatiepositie	
	Q4 2026: Update vanuit het dashboard voor de regio Twente Q2 2027: Update vanuit het dashboard voor de regio Twente Q4 2027: Update vanuit het dashboard voor de regio Twente
Financiën	N.v.t.
Bronnen	Zicht op Online Criminaliteit

Opdrachtnaam: De gemeente en het MKB	
Aanleiding van probleem / uitdaging	Een cyberaanval kan elk bedrijf treffen. Jaarlijks krijgt 1 op de 5 mkb-ondernemers ermee te maken: van een gehackte mailbox tot een ransomware-aanval waardoor de hele bedrijfsvoering stilvalt. Het mkb is een van de doelgroepen waarom de regionale samenwerking zich richt voor het versterken van de digitale weerbaarheid. Tegelijkertijd is het een zoektocht
Betrokken actoren	• Accountmanagers bedrijven Twentse gemeenten • Centrum voor Veiligheid en Digitalisering • Saxion Hogeschool • Netwerkorganisaties rondom mkb en ondernemen (Digitale werkplaats Twente, ROZ Groep,…)
Doelstelling	Gemeenten zijn zoekende in hun rol en activiteiten richting het mkb, als specifieke doelgroep geformuleerd in de aanpak van lokale digitale weerbaarheid. Doelstelling van de drie geformuleerde actiepunten richting deze doelgroep is om hier vanuit de samenwerking tussen Twentse gemeenten stappen in te zetten in 2026.
Projectresultaat	**MKB Cyberalarmcentrale** Veel ondernemers weten in het geval van een cyberincident niet waar ze terechtkunnen. Sinds oktober 2025 draait er in de Stedendriehoek een pilot MKB Cyber Alarmcentrale. Mkb'ers die worden getroffen door een hack, ransomware-aanval of datalek kunnen gratis bellen naar 088 – 786 7352. Experts helpen ondernemers om snel grip te krijgen op de situatie en gidsen hen naar de juiste ondersteuning. Vanaf november 2025 is de pilot uitgebreid naar heel Oost-Nederland. De pilot zal in 2026 worden uitgebreid naar Noord-Nederland, met als doel het op termijn landelijk aan te kunnen bieden. Vanuit het experteam dragen we in samenwerking met gemeenten bij aan het bekend krijgen van deze mogelijkheid voor mkb'ers in de regio, zodat het regionale mkb weet waar zij terecht kunnen in het geval van een cyberincident. **Cyberevent – handreiking** Op diverse plekken in de regio zijn de afgelopen jaren cyberevents georganiseerd, zoals een cyberontbijt. We verzamelen de opgedane ervaringen, betrokkenen partijen en mogelijkheden voor het organiseren van zo'n bijeenkomst. Met een handreiking verkleinen we de stap voor gemeenten voor het organiseren van deze events. **Accountmanagers bedrijven** We willen de het kennisniveau en handelingsperspectief voor accountmanagers bedrijven van gemeenten versterken door middel van een regionale bijeenkomst met deze doelgroep. Als eerste ingang richting lokale ondernemers is dit een belangrijke partner om ook op het gebied van cyberweerbaarheid informatie te kunnen brengen, door te kunnen verwijzen of signalen op te kunnen halen. De sessie wordt in 2026 georganiseerd in samenwerking met het regionaal accountmanagersoverleg.
Monitoring / voortgangsbewaking	In de eerste helft van 2026 wordt een plan van aanpak voor de drie actielijnen mkb uitgewerkt. Het expertteam draagt zorgt voor dit plan van aanpak en bewaakt de voortgang via de reguliere expertteam overleggen.
Randvoorwaarden	• Doorgang van het project cyberalarmcentrale in 2026 met Oost-Nederland als (deel van het) verzorgingsgebied.

Opdrachtnaam: De gemeente en het MKB	
Afbakening	De rol vanuit het expertteam digitale veiligheid betreft bijdragen aan het informeren van het mkb over cyberweerbaarheid, werken aan bewustwording en het kunnen doorverwijzing naar de juiste preventie en hulp. Gemeente of expertteam heeft geen rol in incidentafhandeling van cyberincidenten binnen het mkb.
Relatie andere initiatieven en ontwikkelingen	
Risico's / onverwachte zaken /effecten	• Stoppen van (financiering van) pilot/project MKB cyberalarmcentrale • Accountmanager bedrijven zien geen rol op dit thema
Planning en mijlpalen	Eerste helft 2026: Uitwerking van de drie actielijnen met een plan van aanpak voor '26 en '27.
Financiën	N.v.t.
Bronnen	www.mkbcyberalarmcentrale.nl Als mkb'er je weren tegen cybercrime - Het CCV

Opdrachtnaam: Hackshield – vraag en aanbod gastlessen via Risk Factory	
Aanleiding van probleem / uitdaging	Eind 2022 zijn via het Platform IVZ zeven Twentse gemeenten aan de slag gegaan met Hackshield. In de vorm van een lokale campagne, gastles(sen) en een huldiging werd de interventie lokaal onder de aandacht gebracht en 'cyberagents' geënthousiasmeerd met de game aan de slag te gaan. De meest complex uitdaging van gemeenten blijkt de betrekken van het onderwijs bij deze interventie. In de Risk Factory draait er sinds een aantal jaren een scenario gemaakt in samenwerking met Hackshield.
Betrokken actoren	• Risk Factory • Hackshield • Expertteam Platform IVZ Twente • Externe partijen - gastdocenten
Doelstelling	Het bevorderen van digitale geletterdheid en digitaal burgerschap bij kinderen in de leeftijd van 8-12 jaar door middel van het bevorderen van gastlessen Hackshield in de klas en het verhogen van het aantal 'cyber agents' in Twente.
Projectresultaat	Het uitvoeren van gastlessen 'Hackshield in de klas' bij zoveel mogelijk scholen in Twente (groep 5 t/m 8). **Vraag** Bij het Risk Factory scenario komt meer dan 90% van groepen 8 uit Twente langs. Door middel van diverse communicatie uitingen verzamelen we hier inschrijvingen vanuit docenten en begeleiders voor een gratis gastles van 45 minuten in de klas. Ook kan er op diverse anderen manieren een uitvraag voor het ontvangen van een gastles gedaan worden, bijvoorbeeld in het kader van Echt niet Vandaag. **Aanbod** Vanuit het expertteam is er bij meerdere leden interesse om een aantal keer per jaar een gastles te geven. Ook gaan we een actieve uitvraag bij partners doen om deze pool als gastdocenten verder uit te breiden, waardoor we kunnen voldoen aan de te verwachten vraag.
Monitoring / voortgangsbewaking	We houden bij hoeveel gastlessen er vanuit deze samenwerking gegeven worden. Per half jaar wordt de voorgang besproken tussen het expertteam en de risk factory en eventueel bijgestuurd om tot het projectresultaat te komen.
Randvoorwaarden	• De Risk Factory biedt diverse mogelijkheden voor communicatie. • De pool van gastdocenten is voldoende gevuld
Afbakening	
Relatie andere initiatieven en ontwikkelingen	• Sinds een aantal jaar is een deel van de Twentse gemeenten aangesloten bij Hackshield. Het is een van de bekendste interventies voor de doelgroep jeugd, die op basis van trends en ontwikkelingen hun aanbod steeds door ontwikkelen en hun interventie ook wetenschappelijk laten onderzoeken.

Opdrachtnaam: Hackshield – vraag en aanbod gastlessen via Risk Factory	
	• In september ’25 zijn de definitieve concept kerndoelstellingen digitale geletterdheid opgeleverd voor PO en VO. Deze interventie sluit heel goed aan bij de groeiende benodigde aandacht voor deze thematiek binnen het onderwijs.
Risico’s / onverwachte zaken /effecten	• Er melden zich te weinig scholen aan voor het ontvangen van een gastles. • De pool met gastdocenten is te klein om aan de vraag te kunnen voldoen.
Planning en mijlpalen	• Start tweede helft schooljaar, begin 2026. Wanneer dit onvoldoende haalbaar blijkt start in nieuwe schooljaar september 2026.
Financiën	• Communicatie/inschrijfmiddelen RF/Hackshield • Aanschaf merchandise middelen t.b.v. gastlessen = >1000,-, bekostiging vanuit werkbudget Platform IVZ.
Bronnen	Risk Factory internetveiligheid Meer informatie Hackshield in de klas Overzicht klassequests

Opdrachtnaam: Echt niet Vandaag	
Aanleiding van probleem / uitdaging	Sinds 2024 organiseert de politie Oost-Nederland, in samenwerking met diverse partners, de achtiedag Echt Niet Vandaag. In 2025 is de actiedag in Oost-Nederland ook georganiseerd en deze staat weer gepland voor 2 april 2026. Het doel van de actiedag is om op één dag zoveel mogelijk preventieve acties te organiseren tegen digitale criminaliteit, met zoveel mogelijk betrokkenen en partners. Zo waren er in 2025 meer dan 250+ activiteiten georganiseerd door 200+ organisaties.
Betrokken actoren	- Organisatieteam Echt niet Vandaag - Politie - Veiligheidsnetwerk Oost-NL Twentse gemeenten Twentse samenwerkingspartners
Doelstelling	Het doel vanuit het expertteam is om waar nodig een bijdrage te leveren in het ontwikkelen van ideeën, in contact brengen van betrokkenen en de uitvoering van acties in het kader van Echt Niet Vandaag op 2 april 2026. Het doel van de acties om naast deze eenmalige actie in het kader van digitale veiligheid, hiermee ook netwerkvorming en samenwerking voor de langere termijn te faciliteren.
Projectresultaat	- Zoveel mogelijk activiteiten vanuit Twente ondersteunen in het kader van Echt niet Vandaag. - Het bundelen van deze activiteiten tot de Twentse bijdrage aan de actiedag. - Verzamelen van resultaten na de actiedag met mogelijke opvolgacties van de best practices. - Regionale communicatie op de actiedag zelf
Monitoring / voortgangsbewaking	Op Echt niet vandaag verschijnt in de aanloop naar de actiedag een overzicht van alle acties. Het expertteam verzameld geplande acties, monitort en jaagt aan.
Randvoorwaarden	- Bereidheid bij gemeenten een bijdrage te leveren in de aanloop naar en tijdens de actiedag.
Afbakening	
Relatie andere initiatieven en ontwikkelingen	
Risico's / onverwachte zaken /effecten	Het betreft in eerste instantie enkel de voorbereiding en bijdrage aan Echt Niet Vandaag 2026. Voor de jaren erna is het nog niet duidelijk of de jaarlijkse actiedag plaatsvindt.
Planning en mijlpalen	- Op maandag 10 november '25 heeft een matchmaking-event plaatsgevonden. - Januari '26: ophalen van alle voorgenomen acties in Twente. - Jan '26- 2 april: bijdrage aan de voorbereidingen en ontwikkelingen van acties in Twente - 2 april 2026: actiedag Echt niet Vandaag

Opdrachtnaam: Echt niet Vandaag	
Financiën	- Mei 2026: Bundelen alle gehouden acties en resultaten en evalueren voor mogelijke vervolgacties.
Bronnen	Echt niet vandaag

PLATFORM IVZ

SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: Collegereeks Online aangejaagde ordeverstoringen	
Aanleiding van probleem / uitdaging	Verstoringen van de openbare orde ontstaan steeds vaker online. Gemeenten en politie worden geconfronteerd met fysieke ordeverstoringen die online beginnen of online versterkt worden. Het gaat dan bijvoorbeeld om onrust rondom politieke besluiten, overlast door groepen en individuen en illegale evenementen. De aanpak van dit fenomeen is complex. Hoe signaleer je online op handen zijnde ordeverstoringen (en wie doet dat)? Welke (juridische) instrumenten heb je in welke fases beschikbaar? En hoe kun je snel en effectief handelen bij online aangejaagde ordeverstoringen?
Betrokken actoren	• Expertteam Digitale Veiligheid binnen de regio Twente (projectgroep initiator) • Regionale professionals actief op het thema OOV: gemeentelijke OO-adviseurs, veiligheid & handhaving, communicatie, juridisch adviseurs, politie/regiovertegenwoordiging • Externe opleider (Noordelijke Academie voor het Openbaar Bestuur (NAOB))
Doelstelling	• Een specifieke collegereeks voor OOV- professionals in Twente, gericht op de actuele thema's rondom online aangejaagde ordeverstoringen. • De deelnemers krijgen concrete kennis (trends, kaders, tools) én handelingsperspectief (interventies, samenwerking, monitoring) om hun rol te versterken.
Projectresultaat	• Programma van de collegereeks (6 modules) aangepast naar Twentse context • Een "Twentse Klas": 15-20 deelnemers in regio Twente. Colleges op locaties in Twente. • Uitvoering van de collegereeks met evaluatie (deelname, tevredenheid, leeropbrengsten). • Toolkit of naslagdocument voor deelnemers (en hele Platform IVZ Twente) met handvatten voor het vervolg in de praktijk.
Monitoring / voortgangsbewaking	• Voortgang update na 3 modules richting expertteam en stuurgroep • Na de modules deelnemersfeedback verzamelen (tevredenheid, leeropbrengst). • Na afloop van de reeks: evaluatieverslag met aanbevelingen voor vervolg. • Indicatoren: aantal deelnemers, mate van representatie (gemeenten/partners), tevredenheidsscore, geplande vervolgactie(n).
Randvoorwaarden	• Budget: voor deelname wordt bijdrage vanuit eigen organisatie gevraagd. • Toegang tot deelnemers (professionals in Twente) en commitment van hun leidinggevenden om deel te nemen. • Draagvlak binnen de regionale samenwerking voor het incompany-aanbod. • Mogelijkheid om het programma aan te passen aan de regionale situatie / actuele casuïstiek in Twente.
Afbakening	• De collegereeks richt zich op OOV-professionals in Twente (geen open aanbod/inschrijving) • Deze reeks biedt praktische inzichten en strategieën om online uitdagingen zoals desinformatie en andere online aangejaagde ordeverstoringen effectief aan te pakken
Relatie andere initiatieven en Ontwikkelingen	- Sluit aan op de landelijke ontwikkelingen met groeiende aandacht voor het thema, zowel in kennis als in handelingsperspectief. - Sluit aan op het project 'Versterken samenwerking rondom OAOV in Twente' - Sluit aan op de eerdere masterclass in oktober 2025 in Twente

Opdrachtnaam: Collegereeks Online aangejaagde ordeverstoringen	
Risico's / onverwachte zaken /effecten	- Lage deelname of onvoldoende belangstelling voor het vormen van een klas. - Financiën: de kosten voor de collegereeks kunnen niet vanuit deelnemers gefinancierd worden.
Planning en mijlpalen	- Q1 + Q22026: Afstemming definitieve aanbod met externe opleider - Q1 + Q2 2026: Uitvraag + samenstellen Twentse klas - Tweede helft 2026: Q1 2027: Uitvoering collegereeks - Q2 2027: Evaluatie, toolkit en vervolgstappen t.b.v. Platform IVZ
Financiën	De kosten voor de bestaande collegereeks op locatie bedragen €1000,- per deelnemer. De verwachting is dat de totale kosten voor de collegereeks in Twente ongeveer op hetzelfde bedrag per deelnemer zullen uitkomen. Eind 2025 heeft NAOB een kostenindicatie voor de af te nemen collegereeks afgegeven.
Bronnen	Actuele Collegereeks: Aanpak van online ordeverstoringen in de frontlinie: een praktische collegereeks voor professionals. | Noordelijke Academie voor het Openbaar Bestuur

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: OAOV – Samenwerking bij online onrust in Twente	
Aanleiding van probleem / uitdaging	Verstoringen van de openbare orde ontstaan steeds vaker online. Gemeenten en politie worden geconfronteerd met fysieke ordeverstoringen die online beginnen of online versterkt worden. Het gaat dan bijvoorbeeld om onrust rondom politieke besluiten, overlast door groepen en individuen en illegale evenementen. Een belangrijke eerste fase is het online monitoren/onderzoeken van (mogelijk) op handen zijnde verstoringen van de openbare orde. Hiervoor bestaan, zowel voor de gemeente als de politie, verschillende mogelijkheden en onmogelijkheden. Ook speelt wetgeving rondom bevoegdheden en privacy hierin een belangrijke rol. De behoefte van gemeenten en politie voor een goede online informatiepositie bij (mogelijk) op handen zijnde verstoringen van de openbare orde is actueel en relevant. Het is belangrijk dat betrokken partijen de juiste rolverdeling en afspraken hebben, om met elkaar te kunnen voldoen aan deze goede online informatiepositie vanuit de juiste bevoegdheden en passend bij gedeelde wetgeving. Uit recente casuïstiek is gebleken dat rolverdeling, afspraken, kansen en beperkingen niet altijd duidelijk zijn.
Betrokken actoren	- Twentse gemeenten - Politie (basisteams in Twente) - Veiligheidsregio Twente (omgevingsanalyse)
Doelstelling	Het versterken van de samenwerking tussen gemeenten en politie in Twente op het doen van online onderzoek in het kader van online aangejaagde ordeverstoringen. Betrokken actoren hebben een gezamenlijk beeld bij hoe ze hierin met elkaar samenwerken.
Projectresultaat	Een gezamenlijke sessie tussen relevante gemeentelijke rollen en politierollen binnen de basisteams. Het programma van deze bijeenkomst richt zich op het kennen van elkaar, de verschillende rollen en bevoegdheden en doorvertaling naar hoe de samenwerking er in de praktijk uit moet zien op basis van actuele Twentse casuïstiek.
Monitoring / voortgangsbewaking	Het programma wordt als samenwerking tussen het expertteam van het Platform IVZ Twente en de politie district Twente samengesteld. Zij bewaken gezamenlijk de deelname aan de bijeenkomst als ook de uitkomsten en eventuele vervolgacties voortkomend uit de bijeenkomst.
Randvoorwaarden	Vertegenwoordiging vanuit alle gemeenten en politie basisteams, met collega's die een (mogelijke) actieve rol hebben in het proces van online monitoring/onderzoek bij online aangejaagde ordeverstoringen.
Afbakening	Het programma richt zich specifiek op de fase van online monitoring/onderzoek. De andere fases (zie een overzicht van de fases bij de bronnen) vallen buiten de scope.
Relatie andere initiatieven en Ontwikkelingen	- In 2025 is er een sessie op het thema online aangejaagde ordeverstoringen geweest met deelname van gemeenten en politie. Hierbij werd gewerkt met het barrièremiddel van het CCV. - Collegereeks OAOV in Twente (ander project in de projectenaanpak) - Nieuwe wetgeving in de maak gericht op bestuurlijk en politioneel handelingsperspectief.
Risico's / onverwachte zaken /effecten	- Onvoldoende deelname/opkomst vanuit gemeenten en politie

Opdrachtnaam: OAOV – Samenwerking bij online onrust in Twente	
Planning en mijlpalen	Q3 2026: vormgeven programma, uitnodiging en praktische organisatie Q1 2027: Uitvoering bijeenkomst Q2 2027: benutten van opbrengsten van de bijeenkomst voor vervolgacties
Financiën	De bijeenkomst wordt zowel qua locatie als qua betrokkenen in kind samengesteld en uitgevoerd.
Bronnen	Online aangejaagde ordeverstoringen - Het CCV

Opdrachtnaam: S&S Lab – Implementatie interventie digitale weerbaarheid	
Aanleiding van probleem / uitdaging	In het Safety&SecurityLAB werken studenten, docenten en onderzoekers samen met (veiligheids)professionals aan innovatieve en duurzame oplossingen voor vraagstukken op het gebied van safety & security. Studenten van de opleiding Integrale Veiligheidskunde en de studierichting Security Management gaan samen met het werkveld op zoek naar slimme oplossingen op het gebied van veiligheid. De afgelopen jaren is er meerdere keren regionaal een S&S lab ronde geweest met Twentse gemeenten op het thema digitale veiligheid.
Betrokken actoren	Saxion Hogeschool – Integrale veiligheidskunde & Security management
Doelstelling	Twentse gemeenten kunnen door een groepje studenten van het S&S lab een interventie laten implementeren. Hiermee werkt de gemeente verder aan de digitale weerbaarheid van de lokale samenleving.
Projectresultaat	Het resultaat bestaat uit een implementatieplan inclusief eerste implementatie bij deelnemende gemeenten. De gemeente heeft inzichtelijk welke interventie, voor welke doelgroep geïmplementeerd is en wat en wie ze nodig hebben voor het bestendigen van deze interventie. De interventie is ook minimaal één keer als pilot uitgevoerd om ervaringen op te doen. De regionale begeleiding voor de deelnemende gemeenten wordt verzorgd door het expertteam in de vorm van een gezamenlijke start- en eindbijeenkomst. De resultaten van de projecten worden gebundeld en gedeeld met alle Twentse gemeenten.
Monitoring / voortgangsbewaking	• Regionaal vindt er een gezamenlijke start- en eindbijeenkomst plaats • Tussen de start en het eind heeft de gemeente afstemmingsmomenten met het groepje studenten • De begeleiders vanuit het Saxion bewaken de voortgang door de studenten t.b.v. hun op te leveren eindproducten.
Randvoorwaarden	• Een randvoorwaarde voor het regionaal oppakken van dit project is voldoende deelnemende gemeenten (minimaal 5). • Een randvoorwaarde voor een potentieel succesvol eindproduct is de keuze en afbakening in interventie in doelgroep bij de aanvang het van het project.
Afbakening	In samenspraak met deelnemende gemeenten wordt een interventie en doelgroep gekozen op het brede thema digitale veiligheid. Dit kan over interne digitale veiligheid gaan, cybercrisis, digitale criminaliteit of online aangejaagde ordeverstoringen
Relatie andere initiatieven en ontwikkelingen	Deze samenwerking borduurt voort op eerdere S&S lab trajecten met het Saxion en gemeenten op dit thema.
Risico's / onverwachte zaken /effecten	Onvoldoende deelnemende gemeenten. Bij minder dan 5 deelnemende Twentse gemeenten kunnen zij wel met een groepje S&S lab studenten aan de slag, maar vindt er geen samenwerking plaats vanuit het regionale expertteam digitale veiligheid

Opdrachtnaam: S&S Lab – Implementatie interventie digitale weerbaarheid	
Planning en mijlpalen	Q4 2026: uitvraag deelname gemeenten februari 2026: kickoff bijeenkomst juni/juli 2026: eindbijeenkomst. Juli 2026: bundeleden uitkomsten en resultaten. Q4 2026: Evaluatie editie 2026 Q1 2027: uitvoering nieuwe reeks
Financiën	Geen kosten voor gemeenten. Bijeenkomsten worden georganiseerd op locaties van betrokken organisaties zelf.
Bronnen	Saxion Safety & SecurityLAB | Hogeschool Saxion

PLATFORM IVZ
SAMEN STERK VOOR EEN VEILIG TWENTE

Opdrachtnaam: Nieuwsbrief digitale veiligheid	
Aanleiding van probleem / uitdaging	De ontwikkelingen op het thema digitale veiligheid gaan snel. Binnen de regionale samenwerking bestaat de behoefte om het collega's, het platformIVZ e betrokken partners structureel te informeren over lopende activiteiten, relevante ontwillingen en goede voorbeelden. Momenteel is er geen eenduidig communicatiekanaal voor terugkerende updates. Hierdoor bestaat het risico dat kennis versnipperd raakt, belangrijke initatieven onvoldoende zichtbaar zijn en betrokkenheid vermindert.
Betrokken actoren	• Expertteam digitale veiligheid Platform IVZ • Communicatie Platform IVZ
Doelstelling	We willen kennisdeling en samenwerking verder bevorderen door het opzetten van een digitale nieuwsbrief. Een nieuwsbrief die: - 3x per jaar verschijnt - Platform IVZ, gemeenten, partnerns actief informeert over activiteiten, resultaten en ontwikkelingen. - Dienst als middel voor inspiratie, goede voorbeelden en relevante kennisuitwisseling - Bijdraagt aan meer betrokkenheid en zichtbaarheid van de regionale samenwerking op digitale veiligheid.
Projectresultaat	• Een volledig ingericht nieuwsbriefformat, voorzien van inhoud door het expertteam • Een opgebouwde en actuele adressenlijst (inclusief opt-in mogelijkheid voor nieuwe inschrijvers). • Eerste (pilot) editie van de nieuwsbrief (Q1 2026). • Een publicatieplanning voor 2026 t/m 2027.
Monitoring / voortgangsbewaking	• De voortgang wordt besproken in de reguliere overleggen van het expertteam Digitale Veiligheid. • Na elke editie wordt een korte evaluatie uitgevoerd (open rate, clicks, input van partners). • Eventuele optimalisaties worden doorgevoerd in het format en de inhoudsplanning.
Randvoorwaarden	- Beschikbare tool (tool Spotler is beschikbaar voor het Platform IVZ) - Beschikbaarheid van actuele en relevante contactadressen - Beschikbaarheid van communicatieondersteuning vanuit Platform IVZ
Afbakening	De inhoud van de nieuwsbrieven richt zich op informatie vanuit of relevant voor de Twentse samenwerking op het gebied van digitale veiligheid.
Relatie andere initiatieven en ontwikkelingen	
Risico's / onverwachte zaken /effecten	- Er bestaan al een aantal nieuwsbrieven van regionale samenwerkingsprojecten, waaronder op het thema zorgfraude en zorg, veiligheid en straf.
Planning en mijlpalen	- Ontwikkelen nieuwsbriefformat in Spotler Q1 2026 - Pilot-editie maken Q1 2026

Opdrachtnaam: Nieuwsbrief digitale veiligheid	
	- Start periodieke verschijning (3x per jaar) 2026 en verder - Evaluatie jaar 1 Q1 2027
Financiën	De tooling is reeds beschikbaar voor het Platform IVZ.
Bronnen	

Opdrachtnaam: Slachtofferschap - ervaringsdeskundigen	
Aanleiding van probleem / uitdaging	Digitale criminaliteit is alom aanwezig, maar tegelijkertijd vaak heel onzichtbaar. In tegenstelling tot fysieke criminaliteit (zoals een inbraak in de straat), voltrekt digitale criminaliteit zich achter gesloten schermen. Slachtoffers vertellen er weinig over, er is vaak schaamte, en slechts ongeveer 20% doet daadwerkelijk aangifte. Hierdoor blijft de impact op de (lokale) samenleving grotendeels onzichtbaar, wat leidt tot een lage risicoperceptie en minder preventieve maatregelen. Tijdens een eerdere regionale campagne bleek dat één ervaringsverhaal in bereik en interactie tot drie keer beter presteerde dan reguliere campagneonderdelen. Dit bevestigt de kracht van echte verhalen bij het zichtbaar en bespreekbaar maken van digitale criminaliteit.
Betrokken actoren	- Expertteam digitale veiligheid - Communicatie VRT/gemeenten - Externe videopartij - Slachtoffers / ervaringsdeskundigen vanuit verschillende doelgroepen: jeugd, mkb, minder digitaal vaardigen.
Doelstelling	- Digitale criminaliteit zichtbaarder maken voor inwoners van Twente door echte ervaringen toegankelijk te delen. - Stimuleren dat inwoners risico's herkennen en adequaat handelen (preventie, melding, hulp zoeken). - Verminderen van schaamte en taboe rondom slachtofferschap. - Partners voorzien van professioneel, herbruikbaar, white-label campagnemateriaal
Projectresultaat	- Drie videoportretten van slachtoffers/ervaringsdeskundigen, één per doelgroep. - White-label export van elke video, zodat partners hun eigen logo's/huisstijl kunnen toevoegen. - Drie geschreven ervaringsverhalen (artikelvorm), vrij inzetbaar online of in print + foto. - Handleiding voor partners hoe zij het materiaal kunnen toepassen in voorlichting, presentaties, social media en trainingen. - Een gezamenlijke lanceringsplanning voor Twentse partners
Monitoring / voortgangsbewaking	
Randvoorwaarden	- Toestemming en goede begeleiding van de betrokken ervaringsdeskundigen (veiligheid, anonimiteit indien gewenst). - Budget voor professionele video- en tekstproductie. - Duidelijke afspraken over rechten, white-label formats en distributie. - Bereidheid van partners om de content toe te passen.
Afbakening	- Het project richt zich op slachtofferschap en ervaringsverhalen; geen volledige bewustwordingscampagne. - Er worden drie verhalen ontwikkeld; uitbreiding kan later besloten worden.
Relatie andere initiatieven en ontwikkelingen	- Vervolg op eerdere succesvolle inzet van ervaringsverhalen in de regio. - Draagt bij aan verlagen van cyberschaamte in de regio - Draagt mogelijk bij aan meldings/ aangiftebereidheid in de regio

Opdrachtnaam: Slachtofferschap - ervaringsdeskundigen	
Risico's / onverwachte zaken /effecten	- Budget niet beschikbaar - Niet kunnen vinden van slachtoffers die mee willen doen. - Partners zetten materiaal te beperkt in.
Planning en mijlpalen	Q3 2026: Werkgroepje uit expertteam in samenwerking met communicatie gemeenten/VRT. Q3 2026: Werven van deelnemers Q3 2026: Offertetraject met videopartij en planning Q4 en Q1 2027:ontwikkeling materialen Q2 2027: lancering
Financiën	Benodigde financiering voor het ontwikkelen van de drie video's en artikelen: €5000,-
Bronnen	https://twenteveilig.nl/het-verhaal-van-heidi

Opdrachtnaam: Cyberoefendriehoek in Twente	
Aanleiding van probleem / uitdaging	Gemeenten worden in toenemende mate geconfronteerd met digitale risico's die een directe impact hebben op hun bestuurlijke en maatschappelijke continuïteit. Denk aan ransomware, datalekken, desinformatiecampagnes of verstoring van gemeentelijke dienstverlening. In Nederland hebben de VNG, het Openbaar Ministerie en de Politie de afgelopen jaren de Cyberoefendriehoek ontwikkeld: een oefenconcept waarin de bestuurlijke driehoek (burgemeester, politie en OM) gezamenlijk een realistisch cybercrisisescenario doorloopt. Het doel is bestuurlijke voorbereiding, samenwerking en handelingsperspectief te versterken. Er is landelijk positieve ervaring opgedaan met deze aanpak, onder meer in Limburg en regio Rotterdam. Vanuit het OM en RIEC in Limburg is er de afgelopen tijd hard een vernieuwde versie van de cyberoefendriehoek ontwikkeld die in opnieuw december uitgevoerd wordt.
Betrokken actoren	Regionaal: Stuurgroep Digitale Veiligheid Twente, gemeenten Twente (burgemeesters, CISO's, OOV), Politie Oost-Nederland, Openbaar Ministerie, Veiligheidsregio Twente, RIEC Oost-Nederland. Landelijk: ondersteuning met voorbeelden vanuit VNG, OM, Bureau RVS.
Doelstelling	• Onderzoeken of en hoe de Cyberoefendriehoek in Twente kan worden georganiseerd. • Versterken van het bestuurlijke en operationele crisisbewustzijn rondom digitale incidenten bij gemeenten, politie en OM. • Bevorderen van samenwerking, rolverduidelijking en informatie-uitwisseling binnen de driehoek tijdens cyberincidenten.
Projectresultaat	Conceptvoorstel Cyberoefendriehoek Twente, inclusief: • Regionale scope en deelnemende gemeenten. • Betrokkenheid OM, politie, CISO's en adviseurs crisisbeheersing. • Beschrijving scenario en werkvorm (aansluitend op VNG/OM-format). • Planning voor de eerste cyberoefendriehoek • Voorstel richting stuurgroep voor het structureel organiseren van een jaarlijkse cyberoefendriehoek op basis van evaluatie.
Monitoring / voortgangsbewaking	Zie planning en mijlpalen
Randvoorwaarden	- Duidelijk bestuurlijk draagvlak/mandaat - Betrokkenheid en beschikbaar van: burgmeesters, HovJ/OM, CISO's gemeenten, OOV-gemeenten. - Betrokkenheid Veiligheidsregio Twente - crisisbeheersing
Afbakening	• Focus: bestuurlijke oefening, geen technische simulatie. • Doelgroep: burgemeesters, gemeentesecretarissen, CISO's, adviseurs crisisbeheersing, OM en politie. • Geografisch: regio Twente • Thema's: bestuurlijke besluitvorming, communicatie, juridische afwegingen
Relatie andere initiatieven en	• Aansluiting bij landelijke Agenda Digitale Veiligheid • Positieve ervaringen met deze oefenvorm elders in het land

Opdrachtnaam: Cyberoefendriehoek in Twente	
Ontwikkelingen	
Risico's / onverwachte zaken /effecten	Capaciteitsvraag bij partners in relatie tot andere lopende regionale projecten en oefenstructuur en planning (project weerbaarheid vanuit de VRT, systeemoefeningen). Op de benodigde actoren wordt in het kader van crisisvoorbereiding en oefenen al een stevig beroep gedaan. Het voornemen om een cyberoefendriehoek te organiseren moet plaatsvinden in samenhang met de planvorming van crisisbeheersing van de VRT.
Planning en mijlpalen	Inventarisatie en verkenning (Q1 en Q2 2026) • Verzamelen ervaringen van andere regio's (VNG, OM, RIEC Limburg, Bureau RVS). • Afstemmen met Politie, OM en Veiligheidsregio Twente over deelname. • Verdere uitwerking van een planning, rekening houdend met oefenstructuur VRT, project weerbaarheid en beschikbaarheid vanuit betrokken partijen
Financiën	Indicatie benodigde middelen voor voorbereiding, oefenmiddelen, locatie en evaluatie: €5000
Bronnen	• Stappenplan Cyberoefendriehoek • Voorbeeldannotatie cyberoefendriehoek – VNG 2023 • Voorbeeldprogramma cyberoefendriehoek – VNG/OM/Politie- 2023 • Voorbereiding deelnemers cyberoefendriehoek – rotterdam nov. 25 Handboek tafelcoaches – rotterdam nov. 25