



Veiligheidsnetwerk
Oost-Nederland

JAARPLAN 2026

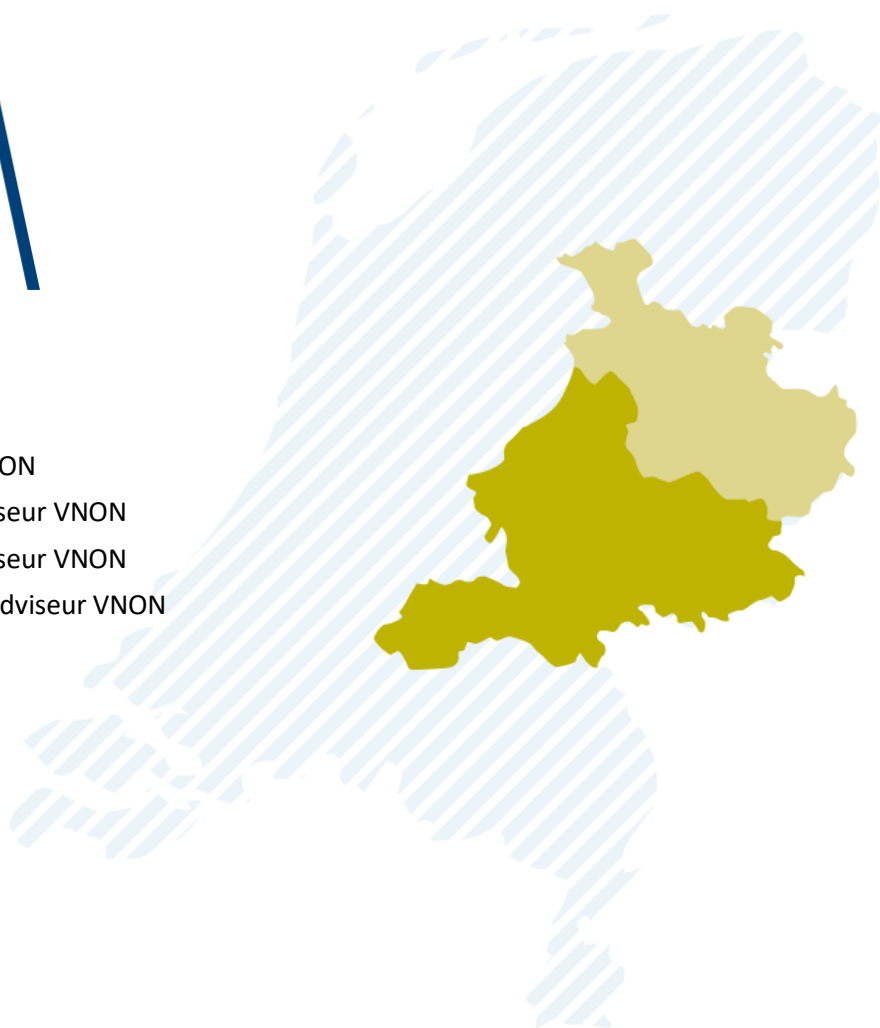
Digitale Weerbaarheid & Online criminaliteit



Mariska Rijneveld
Henk van Ee
Ellen Rossieau
Jop Wieffer

Coördinator VNON
Aanjager / Adviseur VNON
Aanjager / Adviseur VNON
Communicatieadviseur VNON

Versie 09-10-2025



AANLEIDING

Het Veiligheidsnetwerk Oost-Nederland kent een aantal geprioriteerde thema's. De thema's zijn gebaseerd op de integrale veiligheidsplannen van gemeenten in Oost-Nederland en beleidsnota's van de politie en het Openbaar Ministerie. Eén van de geprioriteerd thema's is **Cybercrime en gedigitaliseerde criminaliteit**.

De *City Deal Lokale Weerbaarheid Cybercrime* vanuit het CCV is in 2020 gestart om gemeenten in Nederland te ondersteunen bij het versterken van de cyberweerbaarheid van hun inwoners en lokale sectoren. Door een stevige samenwerking tussen overheden, bedrijfsleven, kennisinstellingen en ministeries wordt gewerkt aan het ontwikkelen en implementeren van effectieve strategieën om de cyberveiligheid op lokaal niveau te verbeteren.

Vanuit deze City Deal zijn middelen beschikbaar gesteld om interventies te ontwikkelen en onderzoek te doen. Om dit te structureren is er een *cyberwegenkaart* ontwikkeld door het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV). Om gemeenten te helpen, onderscheidt het CCV vier wegen waarop je als gemeente actie moet ondernemen om een cyberweerbare gemeente te worden¹. Het aanjagen van deze wegen bij gemeenten wordt als een belangrijke taak gezien waarvoor vanuit de City Deal specifieke middelen vrij zijn gemaakt.

In het Veiligheidsnetwerk Oost-Nederland (VNON) zijn 2 aanjagers vanaf eind 2023 ieder vanuit hun eigen expertise aan de slag gegaan om het thema digitale weerbaarheid en veiligheid (spoor 3) binnen de 5 districten op de kaart te zetten en de samenwerking met lokale (private) partijen en onderwijs te bevorderen in een netwerkaanpak. Dat heeft onder meer geresulteerd in:

- Thematische bijeenkomsten van het expertteam Cyber ONL;²
- Vorming van thematische werkgroepen op doelgroepen MKB en Jeugd;³
- Steun aan districtelijke werkgroepen en beleidsplannen;
- Samenwerking met CVD/Hogescholen op onderzoek en uitwisseling kennis;
- Bijdrage aan actiedagen Echt Niet vandaag in 2024 en 2025 met inzet diverse interventies;

1 (1) Eigen huis op orde, (2) Cyberincidenten en cybercrimes, (3) Cybercrime en gedigitaliseerde criminaliteit en (4) online aangejaagde ordeverstoring

2 het Expertteam Cyber bestaat uit een vertegenwoordiging van de gemeenten, politie, PVO-ON, CVD/Saxion, OM, CCV, VNG, RIEC-ON

3 Er wordt aangesloten bij de doelgroepenbenadering van het CCV (MKB, ouderen/minder digitaal vaardigen en jeugd)

- Ontwikkeling van een communicatie- en kennisplatform via de website <https://veiligheidsnetwerken.nl/kennisbank/digitale-veiligheid/>, en
- Input op bestuurlijke agenda's.

De subsidieverstreking van de City Deal Lokale Weerbaarheid Cybercrime loopt door tot eind 2025 en krijgt geen vervolg in 2026. Dat zal gevolgen hebben voor de specifieke inzet van de aanjagers, maar ook voor de verdere (door)ontwikkeling van lokale aanpakken en inzet van interventies en samenwerking met partners. Om de opgedane kennis en ervaring niet verloren te laten gaan presenteert het VNON dit Jaarplan 2026. Er wordt aangegeven welke uitdagingen zich kunnen voordoen bij de uitvoering van de actielijnen in dit jaarplan indien er in 2026 geen extra middelen worden toegekend. In een apart hoofdstuk worden de risico's benoemd die hiermee gepaard gaan.

MISSIE

Het Veiligheidsnetwerk Oost-Nederland werkt samen met partners in Oost-Nederland om de digitale weerbaarheid van onze samenleving te versterken en online criminaliteit effectief aan te pakken. Door kennisdeling, gezamenlijke aanpak en proactieve samenwerking streven we naar een veilige digitale omgeving voor alle inwoners en organisaties.

VISIE

Er wordt gestreefd naar een digitaal veerkrachtige regio waar bewoners, bedrijven en maatschappelijke organisaties zich beschermd en weerbaar voelen tegen online criminaliteit. Door samenwerking met publieke en private partners, kennis- en onderwijsinstellingen in de regio zorgen we ervoor dat digitalisering bijdraagt aan een veilige en betrouwbare samenleving. Daarnaast is het van belang dat de regio inzicht krijgt in nieuwe ontwikkelingen, zodat zij 'state-of-the-art' kan blijven en dat innovatie binnen het digitale domein actief wordt meegenomen in de aanpak.

4 ACTIELIJNEN

1. Netwerkaanpak

a) Thematische werkgroepen

In 2026 wordt de verdere ontwikkeling van de thematische werkgroepen gericht op de doelgroepen MKB en Jeugd versterkt. In deze groepen zijn vertegenwoordigers van gemeenten, politie, (lokale) private partners en onderwijsinstellingen actief. Ze werken multidisciplinair en structureel samen om een integrale aanpak te ontwikkelen en interventies uit te rollen, gericht op het vergroten van de cyberweerbaarheid binnen deze doelgroepen. Voor de doelgroep ouderen/minder digitaal vaardigen is er nog geen werkgroep opgestart. In 2026 wordt hiermee aangevangen.

De thematische werkgroep MKB bestaat uit een samenwerking tussen de politie-eenheid ON, het Platform Veilig Ondernemen Oost-Nederland, het Centrum voor Veiligheid en Digitalisering (waaronder MBO Aventus, HBO Saxion) en het Veiligheidsnetwerk Oost-Nederland. Deze partijen trekken gezamenlijk op bij de ontwikkeling en uitvoering van interventies gericht op het MKB in de oostelijke gemeentes.

b) Domeinoverstijgend werken

In 2025 is gestart met een verkenning op het stimuleren van domeinoverstijgend werken binnen gemeenten. In 2026 wordt samen met de VNG⁴ gekeken of op het thema digitale weerbaarheid/online criminaliteit een verbreding gerealiseerd kan worden vanuit het veiligheidsdomein naar het sociaal domein / zorg / onderwijs / economie. Een voortdurende samenwerking tussen de diverse disciplines binnen gemeenten zorgt voor een effectievere en efficiëntere aanpak. Daarbij wordt digitale weerbaarheid en veiligheid niet meer beschouwd als een op zichzelf staand thema, maar geïntegreerd in een bredere visie die raakt aan andere prioritaire thema's en bestaande kennis, samenwerkingsverbanden, en aanpakken binnen gemeenten.

c) Expertteam Cyber

Het expertteam Cyber komt eens per 2 maanden bij elkaar en heeft in de afgelopen jaren een vaste structuur gekregen (voorbereiding, agendering, bezetting). Door gastsprekers worden de partners (zie voetnoot 1) enthousiast gemaakt en met elkaar verbonden. De kennis die zij tijdens de thematische bijeenkomsten opdoen, nemen zij mee terug naar

⁴ Aanleiding vormt de wegwijzer voor domeinoverstijgend samenwerken binnen gemeenten (VNG, januari 2025)

hun eigen organisatie en gebruiken ze om hun lokale beleidsplannen beter uit te voeren. In deze behoefte om elkaar te blijven ontmoeten moet worden voorzien door voortzetting van de bijeenkomsten van het expertteam Cyber in 2026.

d) Incident Response

Het VNON is actief betrokken bij het project waarin de Fraudehelpdesk, Saxion, PVO-Oost- en Noord-Nederland, Politie-ON daadwerkelijk hulp bieden aan MKB-ondernemers in geval van een cyberincident. Dit project wordt voortgezet in 2026.

e) Learning Communicaties MKB

Er wordt vanuit het VNON actief gewerkt aan het versterken van de samenwerking tussen Saxion en het Platform Veilig Ondernemen Oost-Nederland, met als doel in 2026 de volgende stap te zetten door daadwerkelijk met ondernemers aan de slag te gaan om hun informatiebeveiliging te verbeteren, na alle bewustwordingssessies die eerder hebben plaatsgevonden. Er wordt ingezet op 2 lijnen: een learning community voor professionals hoe het MKB te kunnen ondersteunen. Een 1^e pilot is gestart in de regio Nijmegen. Een 2^e community is gericht op het MKB zelf.

2. Onderzoek en kennis

a) Uitvoering Onderzoeksagenda CyberweerbaarNL

In 2025 is de Onderzoeksagenda ‘Een sprong naar cyberweerbaarheid’ van CyberweerbaarNL gepresenteerd in het expertteam Cyber⁵. Er is toen gesproken over de meerwaarde om deze agenda samen met betrokken partners uit het werkveld uit te voeren. De onderzoeksvragen in deze agenda, die zich richten op gedrags- en houdingsaspecten die de cyberweerbaarheid beïnvloeden, zijn vooral relevant voor het vraagstuk hoe organisaties deze aspecten kunnen versterken. In 2026 wordt ingezet op het stimuleren van samenwerking met de onderzoekers van de Haagse Hogeschool, de Hogeschool Saxion en NHL Stenden Hogeschool.

b) Kennisdeling platform VNON

Het VNON beschikt over een kennisbank digitale veiligheid en cybercriminaliteit, waarin alle publicaties die binnen het expertteam Cyber zijn besproken, zijn verzameld. Daarnaast zijn factsheets ontwikkeld en gepubliceerd per doelgroep, en wordt een actuele agenda bijgehouden met relevante bijeenkomsten en webinars. In 2026 wordt de voortzetting van deze kennisbank gepland.

⁵ Rutger Leukfeldt, Remco Spithoven, Jurjen Jansen & Carlyn van Amersfoort, 2025

c) Zicht op online criminaliteit

Eind 2025 wordt het dashboard Zicht op Online criminaliteit gelanceerd. Dit dashboard geeft inzicht in zowel daders als slachtoffers van online criminaliteit en bevat naast landelijke trends ook lokale cijfers vanuit verschillende databronnen. Daarnaast biedt het de mogelijkheid om inzicht te krijgen in de overlap van online criminaliteit met traditionele vormen van criminaliteit.

Het VNON neemt deel aan de reviewgroep en draagt zo bij aan de ontwikkeling van het dashboard.

Voor Oost-Nederland is het van belang om het dashboard in 2026 aan te scherpen naar een regionaal en/of lokaal beeld, zodat op bestuurlijk niveau gerichte beleidsvorming kan plaatsvinden.

d) Samenwerking met de Master Veiligheid en Digitalisering

In 2025 is bij het Centrum voor Veiligheid en Digitalisering (CVD) de Master Veiligheid en Digitalisering gestart. Het komende jaar wordt de samenwerking met het CVD verder versterkt door vraagstukken die binnen het VNON spelen, te koppelen aan studenten van deze opleiding voor praktijkgericht onderzoek.

e) Onderzoek naar AI

In 2026 wordt ingezet op het ontwikkelen van richtlijnen en bewustwordingsprogramma's voor verantwoord gebruik van AI om de cyberweerbaarheid van inwoners en bedrijven te versterken.

3. Verbinding met het bestuur

a) Cyberburgemeesters in positie

In Oost-Nederland zijn zes cyberburgemeesters (portefeuillehouders cyber) actief. De meesten van hen zijn recent begonnen in deze nieuwe rol en bevinden zich nog in een verkennende fase, waarin ze hun rol aan het ontwikkelen zijn. Daarnaast groeit de behoefte om de ambtelijke en bestuurlijke lagen op het gebied van cyber meer met elkaar te verbinden. Daarbij wordt onderzocht welke vraagstukken urgent zijn, wat er lokaal en regionaal speelt, welke rol en positie gemeenten daarin innemen, en welke middelen en partijen nodig zijn om de aanpak te ontwikkelen en uit te voeren. In 2026 wordt ingezet om de bestuurders met elkaar te verbinden en sterker in de regio Oost-Nederland te positioneren.

b) Voorbereiding Platform Cyberburgemeesters

Een goede positionering van de zes cyberburgemeesters binnen Oost-Nederland versterkt hun invloed in het Landelijk Platform Cyberburgemeesters. Hierdoor krijgen zij

meer inzicht in de landelijke agenda en kunnen zij belangrijke urgente thema's landelijk prioriteit geven. In 2026 wordt ingezet op een actieve en sterke betrokkenheid van Oost-Nederland in het Landelijke Platform.

4. Interventiegerichte aanpak

a) Actiedag Echt Niet Vandaag

Op 2 april 2024 en 2025 is in Oost-Nederland de actiedag 'Echt Niet Vandaag' gestart. Dit is een zelforganiserende preventieve aanpak gericht op het voorkomen van digitale criminaliteit. 'Echt niet vandaag' is een initiatief van de Politie ondersteund door het Platform Veilig Ondernemen Oost-Nederland, Centrum voor Veiligheid en Digitalisering, Rijnbrink, Veiligheidsnetwerk Oost-Nederland en verschillende landelijke en regionale partners. Het doel van deze dagen is om het bewustzijn over digitale criminaliteit te vergroten en mensen weerbaarder te maken. De actiedag is gestart in de regio Oost-Nederland, met het VNON als een van de partners. Inmiddels vindt er een uitrol plaats in andere regio's door heel Nederland. Ook voor 2026 staat weer een actiedag in Oost-Nederland gepland.

b) Structurele PPS in districten en op doelgroep

Om de energie en verbondenheid tussen partners vast te houden wordt in gezet op duurzame samenwerking. Dit gebeurt in de thematische werkgroepen (zie onder 1a). Het traject van het opzetten van structurele publieke-private samenwerking (PPS) met gemeenten kost tijd, inzet en de juiste bestuurlijke aandacht. In 2026 wordt ingezet op deze ontwikkelopgave.

c) Doorontwikkeling interventie-aanpak

In Oost-Nederland zijn de afgelopen jaren diverse interventies ontwikkeld en ingezet voor de drie doelgroepen. Deze variëren van lokale experimenten tot landelijk beschikbare interventies. Er bestaat grote behoefte aan inzicht in welke interventies effectief zijn en welke partijen het beste in staat zijn om specifieke doelgroepen te bereiken. Dankzij de domeinoverstijgende samenwerking (zie onder 1b), de betrokkenheid van onderzoekers van hogescholen (zie onder 2a) en een goed zicht op de problematiek (zie onder 2d), kan de interventie-aanpak in 2026 verder worden geoptimaliseerd.

RISICOFACTOREN

In dit hoofdstuk wordt uiteengezet voor welke uitdagingen voor de uitvoering van dit Jaarplan 2026 het VNON staat, na het stopzetten van de financiële steun uit de City Deal. Gekeken wordt naar alternatieven voor de beoogde rol van het VNON in de verschillende actielijnen en de risico's voor de voortzetting van de activiteiten op digitale weerbaarheid en online criminaliteit.

Actielijn	Rol VNON	Alternatief	Risico's
1. NETWERKAANPAK			
a) Thematische werkgroepen	Gemeenten stimuleren aan te haken bij het netwerk. Verbindende rol tussen de verschillende partners. Lokale initiatieven gericht op de doelgroepen uitrollen over de 5 districten (verbreding). Opgedane kennis en ervaringen delen binnen het expertteam Cyber.	De rol wordt overgepakt door de huidige trekkers van de districtelijke werkgroepen, politie of andere betrokken partners in de werkgroepen.	Een risico is dat deelname aan de werkgroepen en het vervullen van een verbindende rol te veel capaciteit vergt die niet beschikbaar is. Hierdoor wordt de verbindende rol niet volledig vervuld, waardoor de resultaten uit de werkgroepen niet met de gemeenten worden gedeeld. Daarnaast ontbreekt het nog aan voldoende structuur en stabiliteit in alle vijf districten en hebben de trekkers geen regionaal bereik.
b) Domeinoverstijgend werken	Samenwerking met de VNG opstarten. Aanhaken bij bestaande initiatieven vanuit andere domeinen, stimulerende rol en urgentie aangeven op bestuurlijk niveau.	Rol invullen vanuit een bestaande werkgroep/stamtafel/overleg waarin domeinoverstijgend samenwerken op de agenda staat.	Een risico is dat het opzetten van samenwerking met het VNG-initiatief capaciteit vereist die niet beschikbaar is. Digitale weerbaarheid en online criminaliteit is nog onvoldoende geïntegreerd in andere domeinen. Bestaande gremia hebben ieder hun eigen agenda en belangen, handelen vanuit andere contexten en vormen daarmee geen vanzelfsprekende partner.
c) Expertteam Cyber	Inhoudelijke voorbereiding, voorzitterschap, planning, kennisdeling.	Ondersteunende rol wordt overgenomen, al dan niet in roulatie door trekkers districtelijke werkgroepen of valt weer in zijn geheel terug bij de coördinator.	Een risico is dat bij het wegvallen van ondersteuning voor de coördinator het netwerk, de structuur en de kennisdeling opnieuw opgebouwd moeten worden, wat aanzienlijke capaciteit vergt.

Actielijn	Rol VNON	Alternatief	Risico's
d) Incident Response	Toevoegen van inhoudelijke kennis, het faciliteren en vormgeven van de communicatie naar betrokken partners en het creëren van draagvlak.	De communicatie verloopt via de aangesloten partners (CVD, PVO-ON, Politie).	Een risico is dat het draagvlak voor het initiatief afneemt, waardoor de stabiliteit van de opgebouwde publiek-private samenwerking in gevaar komt.
e) Learning Communities MKB	Het VNON brengt inhoudelijke kennis in van de MKB-wereld en faciliteert de verbinding tussen de partners. Het zorgt ervoor dat andere gemeenten gestimuleerd worden om met dit concept aan de slag te gaan.	De communicatie en verbinding verloopt via de (trekkers van de) districtelijke werkgroepen onderling.	Door het wegvallen van de faciliterende en inhoudelijke rol van VNON bestaat het risico dat de opgedane kennis versnipperd raakt en opnieuw moet worden verzameld en ontwikkeld.
2. ONDERZOEK EN KENNIS			
a) Uitvoering Onderzoeksagenda CyberweerbaarheidNL	Het VNON vervult een verbindende rol tussen onderzoek en praktijk door de behoeften van gemeenten te koppelen aan de onderzoeksagenda.	Onderzoekers zoeken zelf aansluiting met de praktijk en creëren en benutten hun eigen netwerk om behoeften in kaart te brengen en (deel)onderzoeken te starten met (o.a.) gemeenten.	Een risico is dat het extra tijd en inzet kost voor de onderzoekers, omdat het ontbreekt aan een platform om behoeften en resultaten op te halen en te delen, zoals een expertteam Cyber. Dit kan vertragend werken voor de uitvoering van de agenda.
b) Kennisdeling Platform VNON	Onderhoud en beheer van de kennisbank. Doorontwikkeling factsheets.	Beheer en onderhoud wordt overgedragen aan	Een risico is dat het ontbreken van een actueel kennisplatform en overzicht op activiteiten ertoe leidt dat elke gemeente opnieuw documentatie en kennisbijeenkomsten moet zoeken. Hierdoor gaat waardevolle kennisdeling verloren.
c) Zicht op online criminaliteit	Leveren van input in de reviewgroep, verbinding tussen gebruikers (gemeenten) en ontwikkelaars (MinBZK).	Deelname aan de reviewgroep wordt overgedragen aan andere betrokkenen in regio Oost-Nederland.	Een mogelijk risico is dat het niet mogelijk is om op regionaal niveau de belangen goed te behartigen als slechts één gemeente betrokken is. Hierdoor kan de effectiviteit van de inzet en samenwerking worden ondermijnd.

Actielijn	Rol VNON	Alternatief	Risico's
d) Samenwerking met de Master Veiligheid en Digitalisering	Verbinden van (regio- en domein-overstijgende) vraagstukken in het domein van Veiligheid en Digitalisering die spelen bij gemeentes met studenten van deze Masteropleiding vanuit het CVD	Rechtstreeks contact vanuit individuele gemeentes met de coördinator van de Master.	Er bestaat een risico dat dezelfde vraagstukken worden aangepakt die elders al zijn behandeld, waardoor belangrijke regio-overstijgende vraagstukken mogelijk niet op de juiste wijze worden aangepakt.
e) Onderzoek naar AI	Het faciliteren van samenwerking tussen onderzoeksinstellingen en gemeenten om behoefte inzichtelijk te maken.	De impact van AI wordt vanuit de gemeenten / districten onderzocht, dan wel er wordt voor dit onderzoek aansluiting gezocht met de onderzoeksagenda (zie 2A).	Het risico is dat bij het ontbreken van een ondersteunende rol de afstemming tussen de behoefte en de onderzoeksvraag niet adequaat plaatsvindt, aangezien alle betrokken partijen zelfstandig moeten handelen.
3. VERBINDING MET HET BESTUUR			
a) Cyberburgemeesters in positie	Opstarten en inhoudelijk voorbereiden van bestuurlijk draagvlak door inspiratiebijeenkomsten voor bestuurders en ambtelijke laag.	De (ondersteuners van de) 6 portefeuillehouders organiseren zelf een regionaal platform en halen input uit de districten om rol en behoeften scherp te krijgen.	Een risico is dat het verhelderen en versterken van de positie en rol van cyberburgemeesters tijdrovend is en niet vanzelf gaat, waardoor de werking en effectiviteit van hun rol mogelijk onder druk komen te staan.
b) Voorbereiding Platform Cyberburgemeesters	Inhoudelijke voorbereiding Platform Cyberburgemeesters voor de 6 portefeuillehouders in Oost-Nederland.	Deze rol ligt bij de coördinator van het VNON.	Een risico is dat de coördinator geen ondersteuning meer kan oproepen voor de inhoudelijke voorbereiding van de zes portefeuillehouders, wat leidt tot extra tijdsinvestering. Dit kan nadelig zijn voor het versterken van de regionale positie van de cyberburgemeesters in Oost.

4. INTERVENTIEGERICHTE AANPAK			
a) Actiedag Echt Niet Vandaag	Aanjagen van activiteiten binnen alle 67 gemeenten, verbinden van partners, het stimuleren van duurzame samenwerking tussen partijen.	Het kanaal tussen de organisatie Echt Niet Vandaag en gemeenten wordt ingevuld door individuele contacten tussen betrokken partners.	Een risico is dat gemeenten niet vanzelf gestimuleerd worden om deel te nemen aan de actiedag, en dat de netwerken en thematische werkgroepen die uit de actiedag voortvloeien niet meer worden ondersteund, waardoor deze netwerken mogelijk verloren gaan.
b) Structurele PPS in districten en op doelgroep	Opzetten ontwikkeltraject strategische en operationele PPS met gemeenten op het thema digitale weerbaarheid en online criminaliteit.	Geen alternatief	Een risico is dat zonder de juiste expertise er geen systematische inrichting van strategische partnerschappen en borging daarvan zal plaatsvinden. De strategische positie van gemeenten in publiek-private samenwerkingen (PPS) zal zwak zijn.
c) Doorontwikkeling interventieaanpak	Verbinden partijen, aanjagen interventieaanpak in districtelijke en regionale beleidsplannen.	Deze taak wordt overgelaten aan de individuele betrokkenen in gemeenten.	Een risico is dat men terugvalt op de eigen kerntaak binnen het veiligheidsdomein, zonder voldoende tijd en ruimte voor een gestructureerde interventieaanpak. Hierdoor blijven gemeenten hangen in incidentele activiteiten en facultatieve interacties met partijen.

CONCLUSIE

De afwezigheid van de ondersteunende rol van het VNON brengt ernstige risico's met zich mee: alle opgebouwde kennis, samenwerkingsverbanden en netwerken zullen onder druk komen te staan, terwijl het proces van het structureren en versterken van de online weerbaarheid niet vanzelf voortgezet zal worden. De regionale en gemeentelijke structuren die momenteel nog onvoldoende verankerd zijn, vormen in hun huidige staat geen solide basis voor verdere ontwikkeling. Zonder gerichte ondersteuning is het onmogelijk om de regio Oost-Nederland effectief te positioneren en de belangrijke stappen binnen de vier actielijnen te zetten. Het gebrek aan capaciteit en prioritering op zowel ambtelijk als bestuurlijk niveau onderstrepen dat zonder deze ondersteuning de ambities op het gebied van online criminaliteit en weerbaarheid slechts moeilijk te realiseren zijn.