26 643 Informatie- en communicatietechnologie (ICT)

29 911 Bestrijding georganiseerde criminaliteit

Nr. 1447 Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 december 2025

Hierbij bied ik uw Kamer, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Justitie en Veiligheid, het onderzoeksrapport '*Cyberweerbaarheid binnen gemeentegrenzen: Uitwerking van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten en het Rijk'* aan*.*

Met deze brief ga ik in op de belangrijkste bevindingen van dit onderzoeksrapport, plaats ik deze in de bredere context van digitale veiligheid bij gemeenten en schets ik de verdere aanpak. Het Bestuurlijk Convenant Digitale Veiligheid Gemeenten (hierna: convenant)[1], dat in december 2022 is ondertekend door de staatssecretaris van Koninkrijksrelaties en Digitalisering, de minister van Justitie en Veiligheid (JenV) en de voorzitter van de Vereniging Nederlandse Gemeenten (VNG), tevens burgemeester van Den Haag, beoogt de gezamenlijke inzet op digitale veiligheid van gemeenten nader uit te werken.

Het convenant betreft de uitvoering van zowel de Nederlandse Cybersecuritystrategie (NLCS) 2022–2028 als van de Nederlandse Digitaliseringsstrategie (NDS). De NLCS geeft richting aan de kabinetsinzet op het versterken van digitale weerbaarheid van Nederland, terwijl de NDS invulling geeft aan de overheidsbrede digitaliseringsambitie. Door als één overheid op te treden in plaats van als afzonderlijke organisaties, zoals de NDS schetst, kan de voortgang op cruciale thema's worden versneld.

Inleiding

De afgelopen jaren is de hybride dreiging sterk toegenomen, mede door de veranderende geopolitieke situatie en de snelle digitalisering van processen. Sabotage, cyberaanvallen en informatieoperaties nemen in omvang en intensiteit toe. Inzicht in onze onderlinge afhankelijkheden is daarbij belangrijker dan ooit. Deze nieuwe en zwaardere dreigingen vragen om een aanzienlijke

[1] Stcrt. 2022, nr. 35231

versterking van de digitale veiligheid in alle sectoren en op alle bestuursniveaus, dus ook binnen het lokaal bestuur.

Het convenant richt zich op drie systeemuitdagingen voor de digitale veiligheid van gemeenten:

1. De vertaling van het fysieke veiligheidsstelsel naar het digitale veiligheidsstelsel en de vraag hoe verantwoordelijkheden, rollen, taken en bevoegdheden zich in deze beide domeinen tot elkaar verhouden.
2. De informatiepositie van gemeenten voor de digitale veiligheid van hun eigen organisatie én van maatschappelijk relevante organisaties, burgers en ondernemers in de gemeenten.
3. Structurele financiering voor uitvoering van de NLCS op lokaal niveau, alsook voor de andere uitdagingen om de digitale veiligheid van gemeenten te bevorderen.

De uitdagingen uit het convenant zijn de afgelopen jaren gezamenlijk vanuit de betrokken partijen bij het convenant – het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), JenV, VNG en de G4-gemeenten - verder uitgewerkt, met als doel om bestaande acties rondom digitale veiligheid in samenhang te bezien. Het convenant focust zich op de eerder genoemde drie systeemuitdagingen op het gebied van digitale veiligheid en het in kaart brengen van de diverse behoeften en lopende initiatieven, en zoekt naar de samenhang tussen deze verschillende trajecten. Uitwerking hiervan omvat niet het overnemen van deze initiatieven, maar het identificeren van overlap of hiaten, zodat bestaande initiatieven elkaar beter aanvullen.

Ter uitwerking van het convenant is het afgelopen jaar een onderzoek uitgevoerd. Dit onderzoek geeft verder inzicht in het cyberlandschap van gemeenten en de verantwoordelijkheden van gemeenten en burgemeesters in het digitale domein via de eerdergenoemde drie systeemuitdagingen.

Inzichten en opbrengsten

Het onderzoeksrapport richt zich inhoudelijk op de eerste twee systeemuitdagingen en draagt daarmee bij aan het inzicht in de derde systeemuitdaging: het vraagstuk van structurele financiering voor de uitvoering van de NLCS op lokaal niveau. Deze inzichten ten aanzien van de financiering worden bovendien betrokken in de totstandkoming van de Investeringsagenda voor de Nederlandse Digitaliseringsstrategie.

In het rapport wordt beschreven welke overeenkomsten en verschillen bestaan tussen incidenten in het fysieke en het digitale domein, en hoe deze zich tot elkaar verhouden. Incidenten en crises kunnen binnen één domein – fysiek of digitaal - optreden of in het andere domein overlopen. Het verloop van incidenten en crises in het fysieke domein wijkt af van het verloop van incidenten en crises in het digitale domein wat betreft de wijze waarop deze opschalen, verlopen in de tijd, de mate van voorspelbaarheid van de schaalgrootte, de mate van verbinding naar andere ketens en netwerken en de duidelijkheid over de locatie van assets.
Het rapport geeft een eerste overzicht van het lokale landschap. Daarbij is gekeken naar de taken en verantwoordelijkheden van gemeenten, de samenwerking met partners in het fysieke en digitale domein, en de behoeften die er bestaan om dit landschap te versterken.

Op dit moment is sprake van een complex landschap wat betreft de uitdagingen die gemeenten hebben rond digitale veiligheid. Het rapport schetst een eerste overzicht, geordend naar vier aandachtsgebieden.[2] Deze vormen een belangrijk kader om inzichtelijk te maken welke verantwoordelijkheden gemeenten hebben, welke opgaven er liggen en hoe Rijk en gemeenten hierin samen kunnen werken.

Deze vier aandachtsgebieden zijn:
1. Interne digitale veiligheid;
2. Ontwrichting binnen gemeentegrenzen als gevolg van een cyberincident;
3. Cybercrime en gedigitaliseerde criminaliteit; en
4. Online aangejaagde openbare-ordeverstoringen.

Een belangrijke opbrengst van dit onderzoek is het overzicht dat is gecreëerd van het lokale landschap op het gebied van beleid, uitvoering en toezicht voor deze vier aandachtsgebieden. Deze analyse is voor een breed geheel aan stakeholders van toegevoegde waarde. Daarnaast biedt het onderzoek een startpunt om het landschap verder te ontwikkelen. In het vervolg van deze brief worden per aandachtsgebied de aanbevelingen en vervolgaanpak uiteengezet.

1. Interne digitale veiligheid

[2] In het rapport aangeduid als incidentcategorieën gebaseerd op de vier routes van de lokale cyberwegenkaart van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV)

Het onderzoeksrapport richt zich in eerste instantie op incidenten waarbij gemeenteprocessen en -systemen worden misbruikt en verstoord, met als mogelijk gevolg dat de dienstverlening aan burgers en bedrijven niet voortgezet kan worden. Gemeenten zijn primair zelf verantwoordelijk voor de digitale veiligheid van gemeentelijke processen en systemen en hebben daarmee taken en verantwoordelijkheden in vrijwel alle fasen van de veiligheidsketen.

Toenemende dreigingen als gevolg van een onzekerder geopolitieke situatie en toename in digitalisering van processen hebben ook hun uitwerking op het gemeentelijke domein. Zo wordt al meerdere jaren door de Informatiebeveiligingsdienst (IBD) van de VNG, het computercrisisteam voor de gemeenten, gewezen op de noodzaak tot het versterken van de digitale weerbaarheid van gemeenten. Digitale veiligheid is namelijk onderdeel van digitale weerbaarheid, een breder thema dat gemeenten bezighoudt in deze context.

De komst van de Cyberbeveiligingswet (Cbw), die de Europese NIS2-richtlijn omzet naar Nederlandse wetgeving, helpt bij het verhogen van de digitale weerbaarheid van gemeenten. De Cbw wordt, onder coördinatie van de minister van Justitie en Veiligheid, in nauwe samenwerking met de betrokken vakdepartementen opgesteld voor entiteiten in de verschillende in de NIS2-richtlijn genoemde sectoren. Gemeenten, alsook gemeenschappelijke regelingen voor zover die kwalificeren als overheidsinstantie, zijn binnen de sector overheid entiteiten waarop de Cbw van toepassing gaat zijn. Daarnaast voeren zij taken uit in andere sectoren die in de NIS2-richtlijn zijn genoemd, zoals wegbeheer, afvalverwerking en afvalwater, waardoor zij ook vanuit die rollen binnen de Cbw vallen. De verwachting is dat de Cbw, net als de onderliggende wetgeving (bijvoorbeeld het Cyberbeveiligingsbesluit (Cbb)), in het tweede kwartaal van 2026 in werking zal treden. Gemeenten krijgen op grond van de Cbw onder meer de plicht om passende maatregelen te nemen ter beheersing van de risico’s voor de beveiliging van hun netwerk- en informatiesystemen (zorgplicht) en een meldplicht voor significante incidenten. De Rijksinspectie voor Digitale Infrastructuur (RDI) gaat toezicht houden op de naleving. Daarnaast krijgen organisaties ondersteuning van een CSIRT bij dreigingen, kwetsbaarheden en incidenten. Het CSIRT doet dat onder meer door het monitoren van cyberdreigingen en kwetsbaarheden, het verstrekken van informatie over cyberdreigingen, kwetsbaarheden en incidenten, en het bij incidenten verlenen van bijstand. Voor gemeenten is het

voornemen om hiervoor de IBD aan te wijzen.

Deze verplichtingen voor gemeenten worden in de uitwerking voor een groot deel ingevuld met bestaande kaders en instrumenten. Zo wordt in relatie tot de zorgplicht onder andere gebruik gemaakt van de Baseline Informatiebeveiliging Overheid (BIO), het normenkader voor informatiebeveiliging dat sinds 2019 door de gehele overheid wordt toegepast. Bij inwerkingtreding van de Cbw heeft het ministerie van BZK het voornemen om de vernieuwde Baseline Informatiebeveiliging (BIO2) voor overheidsorganisaties wettelijk verplicht te stellen. De andere vakministers kunnen nadere regels stellen voor de zorgplicht van hun sectoren. Voor de invulling van het toezicht wordt zoveel mogelijk gebruikgemaakt van bestaande verantwoordingssystematieken. Gemeenten gebruiken hiervoor de verantwoordingssystematiek Eenduidige Normatiek Single Information Audit (ENSIA). Met de komst van nieuwe wetgeving, zoals de Cbw, groeit het belang en de rol van ENSIA. Het uitgangspunt van ENSIA is dat gemeenten informatie slechts één keer hoeven te verzamelen, waarna deze kan worden gebruikt om aan meerdere stelsel- en toezichthouders verantwoording af te leggen. Om dit te realiseren en gemeenten te ontlasten, is het noodzakelijk te investeren in de verdere doorontwikkeling van ENSIA. Bijvoorbeeld door in de toekomst aanvullende stelsels toe te voegen aan ENSIA, zodat gemeenten nog meer ontlast worden. Ook wordt ingezet op het harmoniseren van wetgeving en toezichtstelsels.

Een ander aandachtspunt uit het onderzoeksrapport betreft de risico’s in de leverancierssketen. Deze worden ook in de Cbw en het Cbb geadresseerd. Onderdeel van de eerdergenoemde zorgplicht, en overigens ook van de huidige BIO, is namelijk het door organisaties treffen van maatregelen met betrekking tot de beveiliging van die keten. Dit houdt onder meer in dat zij in beleid de omgang met afhankelijkheden van producten of diensten van leveranciers die invloed kunnen hebben op de beveiliging van hun netwerk- en informatiesystemen moeten bepalen. Organisaties dienen ook te toetsen of rechtstreekse leveranciers voldoen aan de beveiligingseisen die volgen uit hun eigen risicoanalyse. De Inkoopeisen Cybersecurity Overheid (ICO) helpen organisaties om passende eisen te formuleren.

In 2017 de Gezamenlijke Gemeentelijke Uitvoering (GGU) gestart[3]. Via de GGU en het bijbehorende fonds GGU spreken gemeenten standaarden af, kopen ze samen in en werken ze samen aan

[3] Gezamenlijke Gemeentelijke Uitvoering (GGU), vng.nl/ggu

nieuwe diensten en producten. De IBD en ENSIA zijn voorbeelden van die collectieve GGU-diensten voor gemeenten. Gemeenten werken bovendien samen in gezamenlijke inkooptrajecten, bijvoorbeeld voor ICT-systemen.[4] Dit verlaagt de kosten en verhoogt de digitale weerbaarheid. Gemeenten maken via de VNG gebruik van het GGI-Veilig-portfolio, een mantelcontract van producten en diensten voor operationele informatiebeveiliging. Via GGI-Veilig nemen gemeenten onder andere een actieve monitoring- en responsdienst af voor het bewaken van gedrag en acties op het eigen bedrijfsnetwerk. Ook kunnen gemeenten beveiligingsproducten voor de gemeentelijke ICT-infrastructuur afnemen (zoals firewalls, anti-DDoS, end-point protection). Tot slot kunnen gemeenten beveiligingsexpertise-diensten afnemen. Door het gebruik van dit GGI-Veilig-portfolio, in aanvulling op de dienstverlening van IBD en ENSIA, werken gemeenten makkelijker samen om de digitale weerbaarheid te versterken. In het kader van de NDS wordt ook bekeken hoe dit overheidsbreed samen verder uitgewerkt kan worden.

Op korte termijn worden gemeenten op verschillende manieren ondersteund om hun interne veiligheid te versterken. Die ondersteuning vindt plaats door middel van:

a. subsidieverlening;
b. versterking van de IBD-dienstverlening op monitoring en detectie; en een
c. ondersteuningsprogramma IBD.

In de eerste plaats verstrekt het ministerie van BZK verschillende subsidies aan de VNG ten behoeve van gemeenten. Dit gaat bijvoorbeeld om de doorontwikkeling van het project Samen Controleren. In dit project werken gemeenten en de VNG samen om ICT-leveranciers gezamenlijk te controleren op beveiligingsmaatregelen rond hun online software. Hiermee wordt voorkomen dat elke gemeente individueel uitvragen richting leveranciers dienen te doen. Door deze gezamenlijkheid te zoeken, kunnen gemeenten beter grip krijgen op risico’s in hun (digitale) leverancierskеten. Dit project is in pilotvorm met succes doorlopen met de leveranciers van burgerzakensystemen.

In de tweede plaats wordt ingezet op de versterking van de IBD-dienstverlening op monitoring en detectie. De IBD bewaakt de van buiten zichtbare ICT-infrastructuur van gemeenten met behulp van gespecialiseerde software. Gemeenten worden hiermee geholpen

[4] Nieuwe collectieve aanbesteding: GT Hardware – werkplek, VNG.nl/nieuws/nieuwe-collectieve-aanbesteding-gt-hardware-werkplek

bij het signaleren en aanpakken van digitale dreigingen. Op basis van ervaringen uit de afgelopen jaren wordt de software van de IBD in de komende periode vernieuwd.

Tot slot worden gemeenten op de korte termijn ondersteund via het ondersteuningsprogramma aan gemeenten van de IBD om te voldoen aan de zorgplicht van de Cbw. Met behulp van regioaanjagers worden gemeenten ondersteund bij implementatie van de verplichte systematiek van het Information Security Management System (ISMS). Dat is een gestructureerde en systematische aanpak gericht op het beheren en verbeteren van informatiebeveiliging binnen een organisatie. Het versterken van de digitale veiligheid van organisaties is immers een dynamisch proces. Dreigingen, technologieën en processen vergen een continue aanpassing van de te nemen maatregelen.

2. Ontwrichting binnen de gemeentegrenzen als gevolg van een cyberincident

Het onderzoeksrapport presenteert voor het tweede aandachtsgebied een eerste zicht op de rollen, bevoegdheden en verantwoordelijkheden die het lokaal bestuur heeft bij cyberincidenten bij (publieke of private) organisaties en bedrijven binnen de gemeentegrenzen met mogelijk maatschappelijk ontwrichtende impact en effecten op de samenleving.

Bij ontwrichting binnen gemeentegrenzen liggen de wettelijke taken, verantwoordelijkheden en bevoegdheden van burgemeesters vooral in de fasen van respons en nazorg. Het gaat dan om incidentgevolgbestrijding als de openbare orde en veiligheid in het geding is. In het onderzoeksrapport komt naar voren dat de rol van gemeenten (en de burgemeester) bij incidenten met ontwrichting nog duidelijker moet worden gedefinieerd, evenals de rol van veiligheidsregio’s: wie is wanneer waarvoor verantwoordelijk en heeft welke taken en bevoegdheden? Ook is er behoefte aan meer inzicht en aan meer helderheid in de rolverdeling voor wat betreft regie, mandaat en ondersteunende structuren voor opschaling en informatiedeling.

De onderzoekers doen verschillende aanbevelingen om de (informatie)positie en het handelingsperspectief voor gemeenten op dit gebied te verduidelijken en te verbeteren, evenals om inzichtelijk te maken welke concrete casuïstiek hieraan ten grondslag ligt. Bovendien moet in een nadere uitwerking worden vastgesteld hoe breed de geïnventariseerde behoeften leven, wat er nodig is en hoe realistisch deze behoeften zijn. Ook moeten

prioriteiten worden gesteld voor de eventuele invulling ervan en moeten hieraan actiehouders worden gekoppeld. Dit onderzoek bevestigt dat hier een behoefte ligt, zoals ook in het convenant is aangegeven. We gaan aan de slag met deze aanbevelingen.

In de praktijk wordt door verschillende gemeenten reeds gewerkt aan oplossingen. Zo hebben de G4-gemeenten hun informatiebehoefte kenbaar gemaakt en werkt de gemeente Den Haag samen met haar partners aan een Stedelijk Crisisplan Digitaal, als lokale uitwerking van het Landelijk Crisisplan Digitaal (LCP-D). Komend jaar gaat de NCTV, samen met de VNG en BZK, aan de slag met scenariosessies waarin wordt ingegaan op diverse cybergerelateerde (dreigings)scenario's gericht op de ontwrichting binnen gemeentegrenzen als gevolg van een cyberincident. Via deze sessies wordt in kaart gebracht wat er verder nodig is. De inzichten die in deze trajecten worden opgehaald, worden meegenomen in de actualisatie van het LCP-D. Het LCP-D is een gezamenlijk, kaderstellend en overkoepelend plan van Rijk en regio, waarop zowel gemeenten als veiligheidsregio's (verlengd lokaal bestuur) hun eigen (operationele) plannen kunnen baseren. De actualisatie van het LCP-D is voorzien in 2026.

De uitkomsten van bovengenoemde trajecten worden ook betrokken bij de doorontwikkeling van het Cyberweerbaarheidsnetwerk. Het Cyberweerbaarheidsnetwerk (CWN) is een netwerk waarin het NCSC en het Digital Trust Center (DTC) samenwerken met andere publieke en private organisaties. Het doel van deze samenwerking is digitale ontwrichting te voorkomen en Nederland digitaal veiliger en weerbaarder te maken.

3. Cybercrime en gedigitaliseerde criminaliteit

De uitwerking van het derde uitgewerkte aandachtsgebied in het rapport ziet toe op gedigitaliseerde criminaliteit en cybercrime met impact op inwoners en organisaties binnen gemeentegrenzen. Cybercrime en gedigitaliseerde criminaliteit betreffen in de meeste gevallen incidenten waarvoor het gebruik van een crisisbeheersingsmethodiek niet het meest passend is. Cybercrime betreft criminaliteit waarbij ICT-middelen van het slachtoffer het doel zijn, zoals computervredebreuk (vaak aangeduid als "hacken"), ransomware en DDoS-aanvallen. Het betreft vaak complexe, grensoverschrijdende criminele werkwijzen die bovendien voortdurend in ontwikkeling zijn. Nederland voert een actief beleid van preventie, opsporing, verstoring en vervolging. Uw

Kamer wordt jaarlijks, meest recent op 27 juni 2025, geïnformeerd over de voortgang van de integrale aanpak van cybercrime, waarin ook de ontwikkeling van bevoegdheden in het digitale domein worden behandeld.[5]

Onderdelen van de aanpak zijn preventiecampagnes, versterking van de mogelijkheden tot grensoverschrijdende vergaring van digitaal bewijs en vastgestelde ambities voor de politie en het Openbaar Ministerie (OM) in de Veiligheidsagenda 2023-2026.

Gedigitaliseerde criminaliteit is “klassieke” criminaliteit die wordt gepleegd met behulp van digitale middelen. De term wordt voor veel vormen van criminaliteit gebruikt, waaronder online fraude, online drugshandel en de verspreiding van beeldmateriaal van seksueel kindermisbruik. In de Veiligheidsagenda 2023-2026 zijn voor deze vormen ambities voor de opsporing vastgesteld. Voor online fraude is in 2022 de publiek-private samenwerking ‘Integrale aanpak online fraude’ ingericht, waar de VNG aan deelneemt.

Binnen de City Deal Lokale Weerbaarheid Cybercrime zijn innovatieve cyberprojecten ontwikkeld. Het gaat om initiatieven ter preventie van cybercrime en gedigitaliseerde criminaliteit bij kwetsbare doelgroepen, zoals mkb, jongeren en senioren. Voor gemeenten is het belangrijk dat deze succesvolle projecten duurzaam beschikbaar zijn en actief worden verspreid. Dit jaar wordt samen met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en andere partners gewerkt aan de borging van de City Deal Lokale Weerbaarheid Cybercrime, waarbij de nadruk sterker op lokale implementatie komt te liggen. Zo kunnen gemeenten nu en in de toekomst aan de slag met de ontwikkelde kennis, netwerken en de meest succesvolle projecten om de cyberweerbaarheid van hun inwoners en bedrijven te verhogen.

Bij de aanpak van cybercrime en gedigitaliseerde criminaliteit zijn gemeenten vooral actief bij voorlichting aan specifieke of kwetsbare doelgroepen, het beschikbaar stellen van tools, trainingen en informatie en het doorverwijzen van slachtoffers naar hulpverlenende instanties. Om deze taken effectief te kunnen invullen is een goede informatiepositie ten aanzien van dader- en slachtofferschap in de gemeente van belang. Daarom voert het CBS periodiek de Monitor Online Veiligheid en Criminaliteit uit en is in opdracht van het ministerie van JenV en in nauwe samenwerking met gemeenten, op initiatief van de gemeente Utrecht, momenteel een dashboard Zicht op Online Criminaliteit ontwikkeld. Dit

[5] Kamerstukken II, 2024/25, 26 643, nr. 1357

dashboard toont analyses die inzicht geven in slachtoffers en daders van online criminaliteit. Deze kennis helpt gemeenten om bestuurlijk gevolgen te onderbouwen, handelingsperspectief te bieden en gerichte preventieve maatregelen mogelijk te maken.

Burgemeesters hebben een wettelijke taak bij gevolgbestrijding als de openbare orde en veiligheid in het geding is in de responsfase. Voor zover cybercrime en gedigitaliseerde criminaliteit gevolgen hebben voor de handhaving van de openbare orde, of bij ernstige vrees voor het ontstaan van verstoringen van de openbare orde, zijn burgemeesters bevoegd op grond van hun gemeentelijke wettelijke bevoegdheden om maatregelen te treffen.

4. Online aangejaagde openbare-ordeverstoringen

De uitwerking van het vierde aandachtsgebied wordt bezien vanuit het perspectief van online aangejaagde openbare-ordeverstoringen binnen gemeentegrenzen. Daarbij is vanuit het onderzoeksrapport geconstateerd dat gemeenten behoefte hebben aan meer duidelijkheid omtrent bestaande bevoegdheden in het online domein, waaronder de vraag of- en welke bevoegdheden uit het fysieke domein online inzetbaar (moeten) zijn.

Ook is de wens naar voren gekomen naar explicitering van bevoegdheden ten behoeve van online onderzoek en analyse met het oog op handhaving van de openbare orde. Hiertoe is een juridische verkenning uitgevoerd en een handreiking opgesteld. VNG heeft een praktisch protocol opgesteld hoe gemeenten de werkwijzen rondom online onderzoek kunnen vastleggen.[6]

De vraagstelling die nu speelt, is hoe (met welke instrumenten) eerder zicht kan worden verkregen op situaties die online spelen voordat deze zichtbaar worden in het fysieke domein. Ten aanzien van het vraagstuk van online aangejaagde ordeverstoringen is uw Kamer bij brief van 5 juli 2023 voor het eerst geïnformeerd over de aanpak van online aangejaagde verstoringen van de openbare orde.[7]
Bij brief van 14 mei 2024 is uw Kamer uitvoeriger geïnformeerd over de aanpak daarvan en heeft uw Kamer daarbij een overzicht van activiteiten in dat kader ontvangen.[8] In navolging daarvan is

---

[6] Hulp voor gemeenten bij online onderzoek, vng.nl/nieuws/hulp-voor-gemeenten-bij-online-onderzoek
[7] Kamerstukken II, 2022/23, 28 684, nr. 726.
[8] Kamerstukken II, 2023/24, 28 684, nr. 739.

uw Kamer recent opnieuw geïnformeerd over de diverse beleidsinitiatieven en activiteiten hierover.[9] Mede in reactie op het onderzoeksrapport verwijs ik in dit verband kortheidshalve naar de inhoud van die brief.

Voor zover het gaat om bevoegdheden inzake gegevensvergaring ten behoeve van de handhaving van de openbare orde merk ik op dat een conceptwetsvoorstel hierover in voorbereiding is.[10] Het conceptwetsvoorstel wordt na verwerking van de reacties uit de internetconsultatie door de minister van Justitie en Veiligheid ter advisering aangeboden aan de Raad van State.

Vervolgstappen

De vervolgstap is om mogelijke overlap of hiaten in de verantwoordelijkheidsverdeling en lopende activiteiten te identificeren en waar nodig bij te sturen. Onder coördinatie van het ministerie van BZK werken alle betrokken partijen momenteel aan het bepalen van de korte- en lange-termijnstappen binnen bovengenoemde systeemuitdagingen. Daarbij ligt de nadruk op uitdagingen die verdere versterking behoeven of beter met elkaar verbonden moeten worden.

Zoals reeds aangegeven maakt het convenant onderdeel uit van de Nederlandse Digitaliseringsstrategie (NDS), waarover ik uw Kamer juli jl. heb geïnformeerd. Hoewel dit rapport zich primair richt op de rollen, verantwoordelijkheden en bevoegdheden van burgemeesters, kunnen de verkregen inzichten -waar relevant- ook worden benut voor de andere bestuurslagen die betrokken zijn bij de NDS.

De voortgang op de uitvoering van het convenant wordt meegenomen in de rapportagelijn van de NDS. Daarnaast zal, conform het eerdere verzoek van uw Kamer, in de jaarlijkse voortgangsrapportage van de Nederlandse Cybersecuritystrategie (NLCS) tevens worden gerapporteerd over de stand van zaken rond de uitvoering van het convenant. Vertegenwoordigers van het lokaal bestuur zijn nauw betrokken bij dit proces en leveren input voor de verdere uitwerking van de gezamenlijke uitdagingen binnen het convenant. In 2027 vindt een evaluatie plaats waarin wordt gekeken naar het al dan niet voortzetten van het convenant gezien de afloop van de looptijd van de NLCS. Deze evaluatie wordt

[9] Kamerstukken II, 2025/26, 28 684, nr. 814
[10] Wet gegevensvergaring openbare orde, internetconsultatie.nl/gegevensvergaringopenbareorde

bovendien gebruikt om te kijken of actualisatie van het cyberlandschap van gemeenten gewenst en uitvoerbaar is, ter invulling van een generieke aanbeveling uit het rapport.

De bevindingen uit dit onderzoeksrapport en de opvolging van de daarin gedane aanbevelingen zullen tevens worden betrokken bij de verdere uitwerking van de Investeringsagenda voor de Nederlandse Digitaliseringsstrategie, die komend jaar separaat aan uw Kamer wordt aangeboden. Deze agenda vormt een belangrijk instrument om gericht te investeren in de structurele versterking van de digitale weerbaarheid van het lokaal bestuur.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
E. van Marum