CYBERWEERBAARHEID BINNEN GEMEENTEGRENZEN

Uitwerking van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten en het Rijk

Petra Oldengarm
Frank van Summeren
29 augustus 2025

Opdracht

Dit rapport bevat een eerste uitwerking van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten[1] dat in december 2022 ondertekend is door de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de minister van Justitie en Veiligheid en de burgemeester van Den Haag, tevens voormalig voorzitter van de Vereniging Nederlandse Gemeenten. Het Bestuurlijk Convenant is een actie die voortvloeit uit het Actieplan Nederlandse Cybersecuritystrategie 2022-2028[2]. In dit rapport worden de in het convenant genoemde systeemuitdagingen nader uitgewerkt.

Over de auteurs

Petra Oldengarm is zelfstandig adviseur cybersecurityvraagstukken en adviseert in deze rol zowel de overheid als private organisaties over uiteenlopende strategische thema's. Ze is afgestudeerd in de technische informatica aan de Rijksuniversiteit Groningen. Daarna heeft ze ervaring opgedaan bij diverse werkgevers, zowel in de publieke als private sector. Gedurende meerdere jaren is ze actief in het domein van cybersecurity, waarvan sinds 2018 als zelfstandig adviseur. Naast haar advieswerkzaamheden is Petra Oldengarm (parttime) directeur van Cyberveilig Nederland en gastdocent aan de Universiteit Leiden en de Universiteit Tilburg. Ook is ze toehoorder in de Cyber Security Raad en lid van de Raad van Advies van Bits of Freedom.

Frank van Summeren is partner van RONT Management Consultants (voorheen TNO Management Consultants). Hij studeerde Integrale Veiligheid aan de Avans Hogeschool en Bestuurskunde aan de Radboud Universiteit Nijmegen. Hij is hoofddocent bij de LOI, NTI, NCOI, SBO, BTR en Bestuursacademie van onder andere de HBO-opleidingen Security Management, Integrale Veiligheid en Technische Informatica. Hij is bestuurslid van AIV, lid van de werkveldadviesraad Integrale Veiligheid en projectsecretaris van het Industrial Platform Cyber Security.

[1] https://vng.nl/sites/default/files/2022-12/Convenant_digitale_veiligheid_rijk-gemeenten.pdf
[2] https://www.nctv.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028

INHOUDSOPGAVE

MANAGEMENT SAMENVATTING

Dit rapport bevat een eerste uitwerking van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten[3]. Het rapport gaat in op twee van de drie in dit convenant geformuleerde systeemuitdagingen. Ten eerste 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. Ten tweede een eerste zicht op de informatiepositie van gemeenten voor de digitale veiligheid van hun eigen organisatie en van maatschappelijk relevante organisaties, burgers en ondernemers in de gemeenten.

Deze uitwerking wordt gedaan aan de hand van vier typen incidenten die gemeenten raken (vrij vertaald uit de vier routes van de lokale cyberwegenkaart van het CCV[4]):

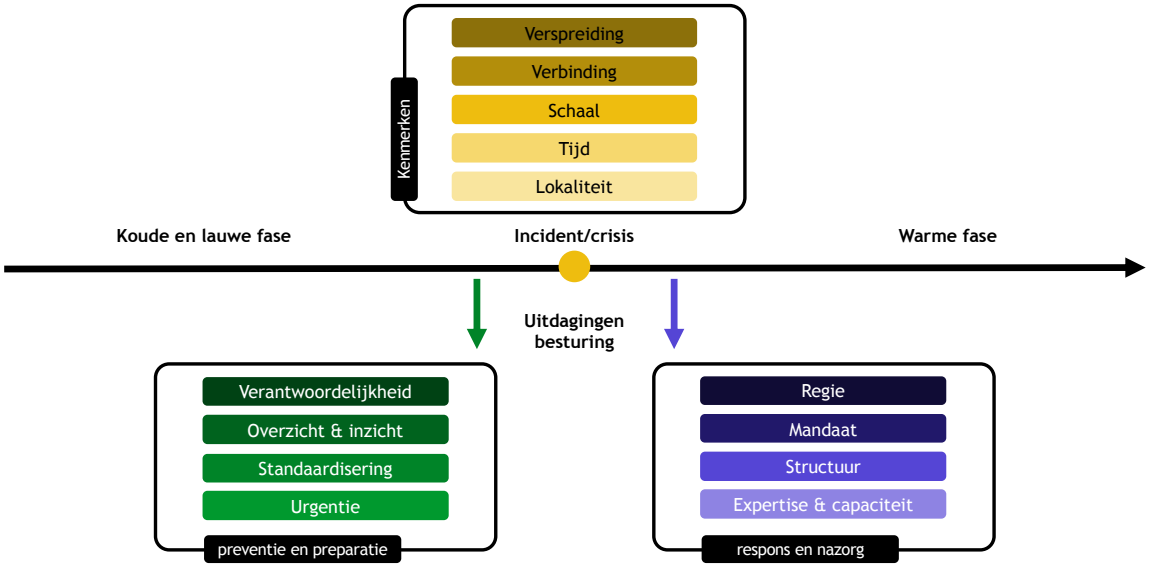
A. Uitval en verstoring van dienstverlening en gemeenteprocessen wegens het niet op orde zijn van de interne digitale veiligheid van gemeenten
B. Ontwrichting binnen gemeentegrenzen als gevolg van een cyberincident
C. Cybercrime en gedigitaliseerde criminaliteit die zich binnen gemeentegrenzen manifesteert
D. Online aangejaagde openbare-ordeverstoringen binnen gemeentegrenzen

Het rapport gaat in de eerste plaats in op de overeenkomsten en verschillen tussen incidenten in het fysieke en digitale domein en de vraag hoe dit soort incidenten zich tot elkaar verhouden. Duidelijk wordt dat deze op vijf kenmerken afwijken van elkaar:

1. Verspreiding: de wijze waarop incidenten en crises opschalen.
2. Verbinding: de mate van verbinding naar andere ketens en netwerken.
3. Schaal: de mate van voorspelbaarheid van de potentiële schaal.
4. Tijd: de wijze van verloop in de tijd.
5. Lokaliteit: de mate van helderheid over de locatie van betrokken assets.

[3] https://vng.nl/sites/default/files/2022-12/Convenant_digitale_veiligheid_rijk-gemeenten.pdf
[4] https://hetccv.nl/themas/cyberveiligheid/cybercrime/beleid-cyberweerbaarheid/lokale-cyberwegenkaart/

Deze verschillen zijn in het rapport nader geduid en vertaald naar acht uitdagingen voor het besturen van incidenten in het digitale domein. Deze acht uitdagingen zijn in het rapport gebruikt als kapstok om de geïnventariseerde uitdagingen nader mee te duiden.

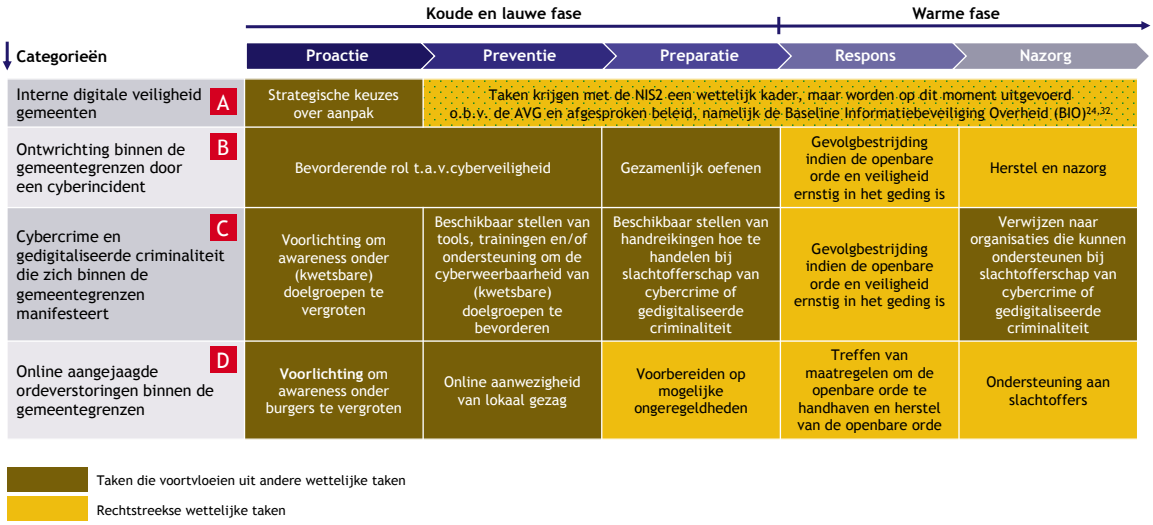


Figuur 1 – Relatie tussen kenmerken van incidenten en crises en de uitdaging voor besturing

Conclusie is dat de analyse van de verschillen tussen het fysieke en digitale domein van toegevoegde waarde is voor het begrip van de problematiek en wat er nodig is voor een betere besturing van incidenten en crises.

Aanbeveling is om deze analyse voortaan als ijkpunt te gebruiken bij beleidsvormende initiatieven op dit gebied én om deze regelmatig (bijvoorbeeld tweejaarlijks) te actualiseren.

Het rapport geeft vervolgens een eerste zicht op het complexe landschap dat is ontstaan op gebied van digitale weerbaarheid van gemeenten en maakt per incidentcategorie inzichtelijk welk beleid er voorhanden is, hoe tussen verschillende stakeholders taken en verantwoordelijkheden zijn verdeeld en welke rechtstreekse wettelijke taken er zijn, en welke taken een breder wettelijk kader hebben. Ook wordt ingegaan op hoe toezicht op gemeenten momenteel is ingericht. Dat levert naast een beeld per incidentcategorie ook een totaalbeeld op. Zo werd zichtbaar dat er veel beleid voorhanden is in de koude en lauwe fase en minder in de warme fase, terwijl de rechtstreekse wettelijke taken van gemeenten zich juist daar vaak bevinden (zie ook onderstaande figuur).



Figuur 2 - Taken en verantwoordelijkheden van gemeenten bij cyberincidenten

Conclusie is dat bij de incidentcategorieën B, C en D de expliciete wettelijke taken en verantwoordelijkheden voornamelijk liggen in de warme fase van incidenten en crises. Deze gaan vooral over incidentgevolgbestrijding op het moment dat de openbare orde en veiligheid in het geding is en over (ondersteuning bij) herstel en nazorg. In incidentcategorie A hebben gemeenten vanzelfsprekend vanaf preventie tot en met nazorg wettelijke taken bij het afhandelen van incidenten die betrekking hebben op de interne digitale veiligheid van gemeentelijke processen en systemen.

Aanbeveling is om te onderzoeken in hoeverre het beleid dat voor de warme fase is geformuleerd afdoende is voor wat er nodig is voor gemeenten of dat er aanvullend beleid (bijvoorbeeld handreikingen) nodig zijn, met het oog op de verschillen in het verloop van incidenten in het fysieke en digitale domein.

Conclusie van dit onderzoek is dat het op een gestructureerde manier in kaart brengen van het landschap, zowel voor wat betreft beleid, uitvoering en toezicht als voor wat betreft uitdagingen die er spelen van belang is voor de bij dit onderwerp betrokken stakeholders.

Aanbeveling is om het overzicht van het landschap regelmatig (bijvoorbeeld tweejaarlijks) te actualiseren, omdat het voortdurend aan verandering onderhevig is, sommige uitdagingen dan zijn opgelost en er nieuwe uitdagingen (kunnen) ontstaan. Uitdagingen zullen in de loop der tijd ook veranderen als het volwassenheidsniveau van gemeenten inzake digitale veiligheid hoger wordt of wanneer belemmeringen in wet- en regelgeving en nationaal beleid zijn opgelost.

Het tweede deel van het rapport gaat in op de uitdagingen die er liggen in dit landschap voor de komende jaren. Dit heeft geleid tot de formulering van enkele tientallen behoeften die in dit rapport zijn beschreven. Wat lastig is, is om voor deze gevallen op waarde te schatten of de gestelde behoefte breed wordt herkend en erkend, of deze haalbaar is, realistisch is en wie eventueel aan zet is om aan deze behoefte invulling te geven. Bij de verdere uitwerking van het bestuurlijk convenant

zal een nadere uitwerking nodig zijn, waarbij in kaart wordt gebracht welke concrete casuïstiek ten grondslag ligt aan de gestelde behoeften zodat de achterliggende vraag concreet kan worden gemaakt. Bovendien moet in een nadere uitwerking worden vastgesteld hoe breed die behoefte leeft en hoe realistisch ze is. Ook moeten er prioriteiten worden gesteld voor wat betreft de invulling van de behoeften en moeten er eventueel actiehouders aan worden toegekend.

De behoeften die in kaart zijn gebracht zijn weliswaar bij een diverse groep geïnventariseerd (zie bijlage A), maar niet bij veel verschillende organisaties van dezelfde soort. Het geeft een globaal beeld wat er bij sommige organisaties in de keten speelt, maar niet bij een representatief aantal van die organisaties. Wat nodig is voor het vervolg is om op waarde te schatten of de opgehaalde behoeften breed worden herkend en erkend, of deze haalbaar zijn, realistisch zijn en wie eventueel aan zet is om aan deze behoeften invulling te geven.

Conclusie is dat een nadere uitwerking nodig is van de uitdagingen op gebied van de besturing van digitale veiligheid van gemeenten waarbij een grotere en representatieve groep van de verschillende stakeholders om input wordt gevraagd.

Aanbeveling is om in kaart te brengen welke concrete casuïstiek ten grondslag ligt aan de in kaart gebrachte behoeften zodat de achterliggende vraag concreet kan worden gemaakt. Bovendien moet in een nadere uitwerking worden vastgesteld hoe breed de geïnventariseerde behoeften leven, wat er nodig is en hoe realistisch ze zijn. Ook moeten er prioriteiten worden gesteld voor wat betreft de eventuele invulling van de behoeften en moeten er dan actiehouders aan worden toegekend.

De inventarisatie van uitdagingen laat onder andere zien dat er bij verschillende incidentcategorieën tussen de verschillende stakeholders nog best wat discussie bestaat over wie in de keten welke taken en verantwoordelijkheden zou moeten hebben. Ook is er soms onduidelijkheid over regie, mandaat en opschalingsstructuren.

Het verdient de aanbeveling om bij de verdere uitwerking van de uitdagingen (zie aanbeveling in de sectie over generieke conclusies en aanbevelingen) extra aandacht te besteden aan taken en verantwoordelijkheden en regie en mandaat. Soms zal een bijstelling nodig zijn, maar soms kan worden volstaan bij herbevestiging en heldere communicatie.

Ook gaat het rapport voor alle incidentcategorieën in op de informatiebehoefte van gemeenten. Deze behoefte staat in nauw verband met de verantwoordelijkheden, rollen, taken en bevoegdheden van gemeenten. Net als bij de geïnventariseerde uitdagingen is bij informatiebehoefte de vraag in hoeverre deze behoeften breder erkend en herkend worden, of zij haalbaar zijn en realistisch en wat dan eventueel de prioriteiten zijn en wie aan zet is om de behoeften daadwerkelijk invulling te geven.

Aanbeveling is om met gemeenten in gesprek te gaan om de informatiebehoeften verder uit te werken, rekening houdend met het risicoprofiel en omvang van

gemeenten. Daarbij wordt geadviseerd om de informatiebehoefte uit te werken aan de hand van concrete casuïstiek waarin knelpunten eerder zichtbaar zijn geworden en vanuit daar kan worden gekeken wat mogelijk, wenselijk, nodig, maar ook haalbaar en realistisch is om te bewerkstelligen.

Wat verder opvalt in de gesprekken over informatiebehoefte is dat de term 'informatie' in de gesprekken diffuus blijft en niet nader gespecificeerd.

Aanbeveling is om bij een verdere uitwerking van de informatiebehoefte van gemeenten het informatiemodel uit het Programma Cyclotron[15] te gebruiken om de behoefte zo concreet mogelijk te maken.

Vanuit het perspectief van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten is het uitdagend om uit de brede set van behoeften en uitdagingen er enkele te kiezen om mee aan de slag te gaan. Het publiek maken van dit rapport stimuleert verschillende organisaties binnen dit domein mogelijk om zelf de lopende activiteiten te evalueren en prioriteren.

Tegelijkertijd kan het centraal oppakken van enkele grote thema's vanuit het Bestuurlijk Convenant een impuls geven aan de ontwikkeling van de digitale veiligheid in het lokale domein.

In het rapport worden daarnaast enkele suggesties gedaan voor thema's die zich lenen voor verdere uitwerking binnen het bestuurlijk convenant en die uit de gesprekken en beleidsdocumenten als overkoepelende onderwerpen naar boven zijn gekomen. Op sommige van deze thema's lopen al initiatieven. In dat geval is het advies om aan deze initiatieven de uitkomsten van dit onderzoek mee te geven en de voortgang op afstand te monitoren. Andere thema's lenen zich voor een apart vervolg, mogelijk op te pakken vanuit het Bestuurlijk Convenant Digitale Veiligheid Gemeenten.

Hoe deze vervolgstappen worden vormgegeven zal nog verder moeten worden uitgewerkt. Voor wat betreft de periodieke meting (overkoepelend onderwerp) worden nog enkele aanvullende suggesties gedaan.

Om meer grip te krijgen op digitale veiligheid binnen de vier incidentcategorieën is een goede vervolgstap om op deze categorieën verder in te zoomen per gemeente, voor grote, middelgrote en kleine gemeenten. Een aanpak hiervoor kan zijn om een landelijke meting op zetten op de vier incidentcategorieën, die in feite de vier routes zijn van de lokale cyberwegenkaart van het CCV.

De uitkomsten van een dergelijke meting vormen belangrijke input voor het creëren van een nationaal beeld van de mate van cyberweerbaarheid op de vier incidentcategorieën. Die is enerzijds lokaal bruikbaar voor gemeenten bij het maken van eigen keuzes. Anderzijds is het (geanonimiseerd) input voor de prioritering op regio's en ook een nationale keuze voor het investeren in weerbaarheidsinitiatieven.

Daarmee biedt het ook waardevolle input voor de meerjarenagenda in het kader van het Bestuurlijk Convenant.

Mocht een brede meting niet (direct) haalbaar zijn, dan kan gestart worden met het aanreiken van een meetinstrument aan gemeenten waarmee zo'n meting kan worden uitgevoerd. Bij succesvolle toepassing binnen meerdere gemeenten ontstaat dan wellicht draagvlak voor een meting bij alle gemeenten.

INLEIDING

Bij het tot stand komen van de Nederlandse Cybersecurity Strategie 2022-2028 (NLCS)[5] is vastgesteld dat er meer specifieke aandacht nodig is voor de digitale veiligheid van gemeenten. Daarom is er eind 2022 een bestuurlijk convenant[6] gesloten dat in december 2022 ondertekend is door de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, de minister van Justitie en Veiligheid en de burgemeester van Den Haag, tevens voormalig voorzitter van de Vereniging Nederlandse Gemeenten. Het Bestuurlijk Convenant is een actie die voortvloeit uit het Actieplan Nederlandse Cybersecuritystrategie 2022-2028. In dit convenant wordt gesproken over drie systeemuitdagingen die verder moeten worden uitgewerkt. Het betreft:

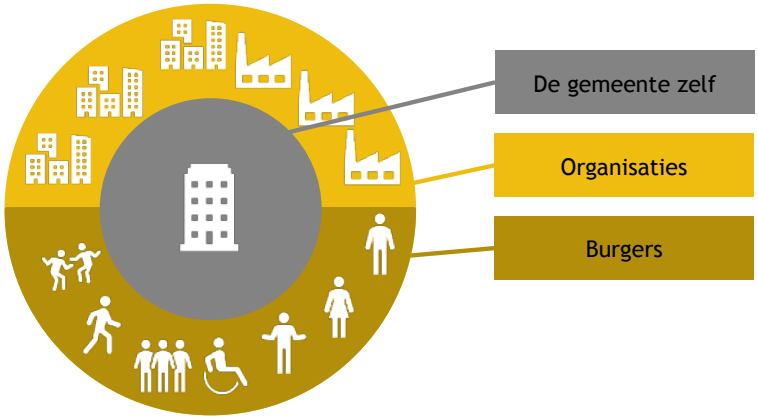
1. De vertaling van het fysieke veiligheidsstelsel naar het digitale veiligheidsstelsel en de vraag hoe verantwoordelijkheden, rollen, taken en bevoegdheden zich in deze beide domeinen tot elkaar verhouden.
2. De informatiepositie van gemeenten voor de digitale veiligheid van hun eigen organisatie én 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 (eigen organisatie én bewoners/organisaties in de gemeente) te bevorderen.

In dit rapport wordt ingegaan op de eerste twee vraagstukken. Dit wordt gedaan aan de hand van verschillende typen incidenten die spelen in en/of gerelateerd zijn aan het digitale domein en die bij de start van deze opdracht aan de onderzoekers zijn meegegeven.

[5] https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028
[6] https://vng.nl/sites/default/files/2022-12/Convenant_digitale_veiligheid_rijk-gemeenten.pdf

TYPEN CYBERINCIDENTEN

De uitdagingen voor gemeenten binnen het cyberdomein kunnen worden geïllustreerd aan de hand van verschillende typen cyberincidenten. Deze cyberincidenten kunnen optreden bij de gemeente zelf, maar ook bij organisaties binnen gemeentegrenzen, bijvoorbeeld bedrijven en (semi-)publieke organisaties, en bij burgers (zie Figuur 3).



Figuur 3 - Cyberincidenten met betrekking tot de gemeente zelf, organisaties en burgers

Het gaat om de volgende typen cyberincidenten:

1. Gericht op de **gemeente** zelf:
   a. Incidenten waarbij gemeenteprocessen en -systemen worden misbruikt/verstoord (inclusief OT/IoT in de buitenruimte).
2. Gericht op **organisaties** (bedrijven en (semi-) publieke organisaties) binnen de gemeentegrenzen:
   a. Incidenten bij instellingen met maatschappelijke impact ((semi-)publiek, lokaal-vitaal, …).
   b. Incidenten met infrastructuur (van private organisaties) die verbonden is met het Internet en aanwezig is in de openbare ruimte (OT/IoT).
   c. Misbruik van bedrijven voor criminele activiteiten (werknemers of bedrijven als instrument).
   d. Digitale criminaliteit gericht op bedrijven (bedrijven als target).
3. Gericht op **burgers** binnen de gemeentegrenzen:
   a. Misbruik van burgers voor criminele activiteiten (burger als instrument).
   b. Digitale criminaliteit gericht op burgers (burger als target).
   c. Lokaal daderschap digitale criminaliteit (burger als crimineel).
   d. Online aangejaagde openbare-ordeverstoring en desinformatie die leiden tot bijvoorbeeld maatschappelijk onbehagen of impact hebben op de democratische rechtsorde.

Bij nadere bestudering van deze incidenttypen blijkt dat ze goed te mappen zijn op de vier routes van de lokale cyberwegenkaart van het CCV[7] die vrij vertaald gaan over:

[7] https://hetccv.nl/themas/cyberveiligheid/cybercrime/beleid-cyberweerbaarheid/lokale-cyberwegenkaart/

A. Uitval en verstoring van dienstverlening en gemeenteprocessen wegens het niet op orde zijn van de interne digitale veiligheid van gemeenten (1a)
B. Ontwrichting binnen gemeentegrenzen als gevolg van een cyberincident (2a, 2b)
C. Cybercrime en gedigitaliseerde criminaliteit die zich binnen gemeentegrenzen manifesteert (2c, 2d, 3a, 3b, 3c)
D. Online aangejaagde openbare-ordeverstoringen binnen gemeentegrenzen (3d[8])

Onderstaande tabel laat zien hoe de negen typen incidenten mappen op de vier categorieën. Het onderwerp desinformatie (uit incidenttype 3d) is in dit onderzoek buiten beschouwing gelaten.

#	Incidenttype	Incidentcategorie
1a	Incidenten waarbij gemeenteprocessen en -systemen worden misbruikt/verstoord	A. Interne digitale veiligheid gemeenten
2a	Incidenten bij instellingen met maatschappelijke impact	B. Ontwrichting binnen de gemeentegrenzen door een cyberincident
2b	Incidenten met infrastructuur (van private organisaties) die verbonden is met het Internet en aanwezig is in de openbare ruimte	
2c	Misbruik van bedrijven voor criminele activiteiten	C. Cybercrime en gedigitaliseerde criminaliteit die zich binnen de gemeentegrenzen manifesteert
2d	Digitale criminaliteit gericht op bedrijven	
3a	Misbruik van burgers voor criminele activiteiten	
3b	Digitale criminaliteit gericht op burgers	
3c	Lokaal daderschap digitale criminaliteit	
3d	Online aangejaagde openbare-ordeverstoringen die leiden tot maatschappelijk onbehagen	D. Online aangejaagde openbare-ordeverstoringen

Tabel 1 - Mapping incidenttypen op categorieën

Bij de verdere uitwerking is uitgegaan van deze vier incidentcategorieën, om de analyse beter behapbaar te maken.

OVER DIT DOCUMENT

Dit document bevat een eerste uitwerking van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten voor de genoemde vier incidentcategorieën (zie Tabel 1) voor de eerste twee systeemuitdagingen (taken/rollen/verantwoordelijkheden en informatievoorziening). Deze systeemuitdagingen hebben een brede reikwijdte omdat deze problematiek complex van aard is en er veel verschillende stakeholders bij zijn betrokken. Met dit rapport wordt beoogd een eerste inzicht te geven in de problematiek, in de uitdagingen die er op dit moment spelen en wordt richting gegeven aan mogelijke oplossingen. Daarmee is het een rapport op strategisch niveau en biedt het een eerste aanzet voor beleid en strategie op dit thema.

[8] Onder 3d valt ook desinformatie, maar dit onderwerp is vooralsnog buiten de scope van de uitwerking van het Bestuurlijk Convenant geplaatst en wordt mogelijk in een later stadium alsnog verder uitgewerkt

In de opvolging van het rapport moet aan deze inzichten tactisch en operationeel invulling worden gegeven. Dat kan bijvoorbeeld met behulp van actieagenda's, verder uitgewerkte taakverdelingen, prioriteitstellingen, etc. Een deel van deze invulling kan worden opgepakt in een vervolgprogramma in relatie tot het convenant, maar een deel kan ook lokaal door betrokken organisaties zelf verder worden uitgewerkt.

Het rapport schetst om te beginnen de verschillen tussen het digitale en fysieke veiligheidsstelsel. Vervolgens geeft het een overzicht van het huidige landschap voor wat betreft beleid, uitvoering en toezicht. Tot slot gaat het in op de belangrijkste uitdagingen voor de komende jaren voor het vergroten van de cyberweerbaarheid van gemeenten. Het eindigt met enkele conclusies en aanbevelingen die kunnen helpen om focus aan te brengen in de veelheid van uitdagingen die er liggen voor de toekomst.

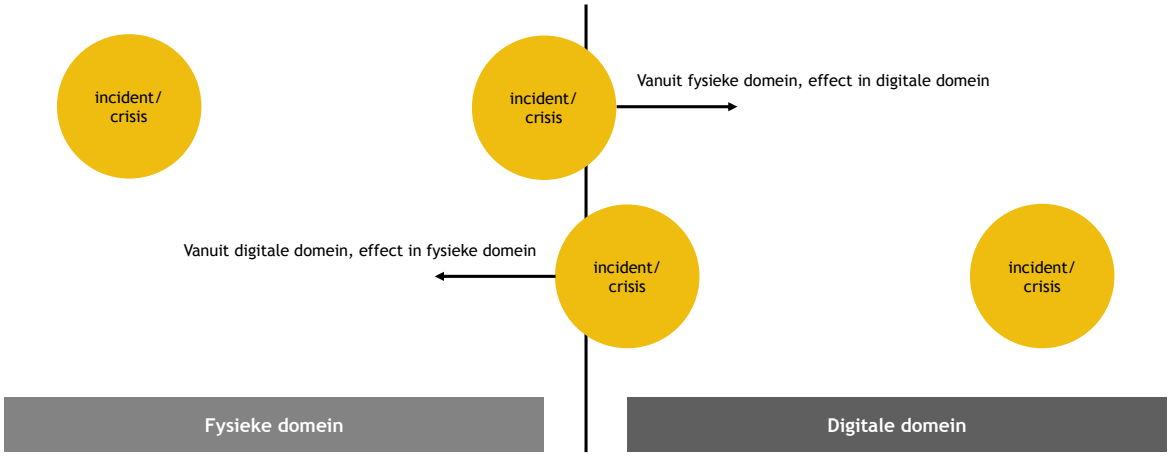
De inhoud van dit document is opgesteld op basis van aangereikte beleidsdocumenten en -initiatieven die in bijlage B zijn opgesomd. Ook zijn er stakeholdergesprekken gevoerd met bij dit onderwerp betrokken organisaties, voornamelijk in het publieke domein. Zie daarvoor bijlage A.

FYSIEK
VERSUS DIGITAAL

De eerste systeemuitdaging betreft 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. Om dit te kunnen doen is het van belang om te begrijpen hoe het fysieke en digitale domein zich tot elkaar verhouden.

Onder het fysieke domein verstaan we in dit rapport het totaal van alle objecten, structuren, systemen en organisatievormen met een tastbare belichaming in de fysieke leefomgeving. Het digitale domein definiëren we als het totaal van alle digitale genetwerkte technologie voor het creëren, opslaan, uitwisselen, bewerken, verwerken en verwijderen van data en informatie. In feite is dat dus heel cyberspace, dat groter is dan alleen het Internet.

Incidenten en crises kunnen binnen één van deze domeinen plaatsvinden, maar lopen vaak in elkaar over zoals in onderstaande figuur wordt geschetst.



Figuur 4 - Incidenten en crises in het fysieke en het digitale domein

Wanneer je kijkt naar het verloop van incidenten en crises in het fysieke en digitale domein dan zijn er kenmerkende verschillen aan te wijzen die impact hebben op de wijze waarop een incident of crisis zou moeten worden bestuurd. In dit hoofdstuk beschrijven we deze verschillen[9] en leggen we vervolgens uit hoe deze verschillen impact hebben op de besturing van de afhandeling van incidenten en crises.

KENMERKEN VAN INCIDENTEN EN CRISES

Als we verschillende beleidsdocumenten, maar ook rapporten en onderzoeken over incidenten en crises bestuderen valt op dat incidenten en crises in het digitale domein op vijf kenmerken afwijken van incidenten en crises in het fysieke domein:

6. Verspreiding: de wijze waarop incidenten en crises opschalen.
7. Verbinding: de mate van verbinding naar andere ketens en netwerken.
8. Schaal: de mate van voorspelbaarheid van de potentiële schaal.
9. Tijd: de wijze van verloop in de tijd.
10. Lokaliteit: de mate van helderheid over de locatie van betrokken assets.

De verschillen worden in onderstaande tabel in detail nader toegelicht.

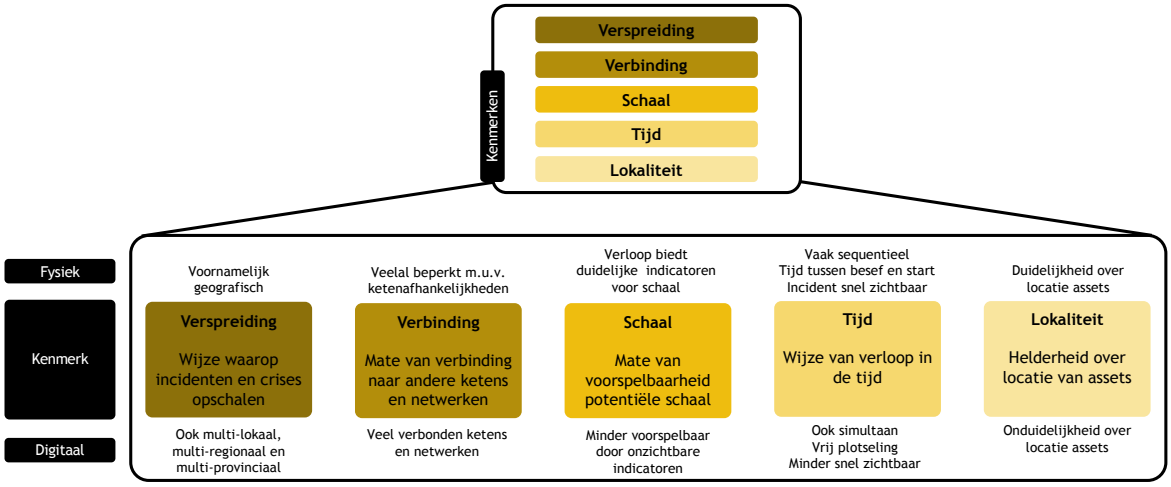
Kenmerk	Fysieke domein	Digitale domein
Verspreiding	Incidenten schalen meestal geografisch op: lokaal, regionaal, provinciaal, nationaal, internationaal.	Incidenten schalen vaak grillig op. Dit kan net als in het fysieke domein geografisch zijn, maar ook op meerdere plekken tegelijkertijd: multi-lokaal, multi-regionaal en multi-provinciaal.
Verbinding	In de fysieke werkelijkheid is de mate van verbinding veelal beperkt en daardoor blijven incidenten vaker beperkt in termen van locatie en tijdsduur, tenzij er ketenafhankelijkheden zijn die zorgen voor verbinding naar andere regio's.	In het digitale domein is de mate van verbinding groot. Er is sprake van veel verbonden ketens en netwerken. Daardoor kunnen incidenten in potentie groot worden in termen van geografische spreiding en tijdsduur.
Schaal	Vaak biedt het verloop van een incident indicatoren waarmee de uiteindelijke schaal goed voorspeld kan worden.	Digitale incidenten kenmerken zich door een grote mate van onvoorspelbaarheid, bijvoorbeeld doordat indicatoren die wijzen op een incident vaker onzichtbaar zijn voor potentiële slachtoffers.
Tijd	In het fysieke domein verlopen incidenten en crises nagenoeg altijd volgens een sequentieel proces.	Naast sequentieel, kunnen incidenten in potentie op veel plekken simultaan optreden.
	Er is bij bepaalde typen incidenten sprake van een tijdsbestek tussen het besef dat er een incident aankomt en de daadwerkelijke start ervan.	Incidenten overvallen het slachtoffer vaker plotseling, omdat indicatoren die kunnen wijzen op een incident vaker onzichtbaar zijn.

[9]Mede op basis van: Berg, B. van den en Kuipers, S.L., 2022, Vulnerabilities and cyberspace: a new kind of crisis. Oxford Research Encyclopedia of Politics.

	Bij incidenten en crises in het fysieke domein is vaak evident dat er een incident of crisis gaande is (voor zowel voor het slachtoffer van het incident als voor de partijen die erop moeten acteren).	Bij incidenten en crises in het digitale domein is niet altijd meteen evident dat er een incident of crisis gaande is (niet voor het slachtoffer van het incident en ook niet voor de partijen die erop moeten acteren, zoals een CSIRT, of een betrokken cybersecurity-dienstverlener). Het kan even duren voordat duidelijk is dat systemen niet meer (goed) werken als gevolg van een cyberincident.
Lokaliteit	Het is voor een organisatie of overheid vaak duidelijk waar de fysieke assets zich bevinden die betrokken zijn bij een incident (concreet).	Het kan onduidelijk zijn waar de assets zich bevinden en het is voor een organisatie of overheid vaak minder duidelijk waar de verantwoordelijkheid voor de beveiliging van data, netwerken en systemen begint en eindigt als assets bij verschillende organisaties zijn ondergebracht (abstract).

Tabel 2 - Kenmerken van incidenten en crises in het fysieke en digitale domein

Deze verschillen zijn samengevat in onderstaande figuur.



Figuur 5 - Verschil in kenmerken van incidenten en crises in het fysieke en digitale domein

Hieronder schetsen we enkele voorbeelden van casuïstiek waarin de verschillen tussen incidenten in het fysieke en digitale domein op deze kenmerken nader worden geïllustreerd.

Kenmerk	Casus
Verspreiding	Cybersecurity incident bij Maersk (https://archief.nipv.nl/wp-content/uploads/sites/2/2022/03/2018-IFV-H6-Cyberaanval-op-Maersk.pdf) Op 27 juni 2017 werden bij verschillende bedrijven en overheden in Oekraïne computersystemen vergrendeld. Dit leidde tot verstoringen

	door heel Oekraïne zoals bij ziekenhuizen, elektriciteitscentrales, telecomproviders, metrolijnen en vliegvelden. Daarna verspreidde de cyberaanval zich naar andere landen waaronder Denemarken, Frankrijk, het Verenigd Koninkrijk, de Verenigde Staten en Nederland. Via het interne netwerk van Maersk werden de systemen van APM Terminals in de Rotterdamse Haven gecompromitteerd door de malware NotPetya. Het gevolg was dat de kranen van APM Terminals tot stilstand kwamen. Deze casus laat zien dat cybersecurityincidenten zich grillig (kunnen) opschalen en zich niet laten tegenhouden door geografische grenzen.
Verbinding	Kwetsbaarheid in software Citrix (https://onderzoeksraad.nl/wp-content/uploads/2023/11/kwetsbaar_door_software_lessen_naar_aanleiding_van_beveiligingslekken_door_sof.pdf) Op 17 december 2019 deed de softwarefabrikant Citrix een openbare mededeling dat diverse van hun softwareproducten een kwetsbaarheid bevatten waardoor kwaadwillenden ongewenst konden binnentreden in de systemen van de gebruikers. Dit had gevolgen voor veel organisaties in binnen- en buitenland, omdat Citrix een veelgebruikte tool is om een werkomgeving mee te beheren. Deze casus illustreert dat een kwetsbaarheid bij één product van een softwarefabrikant kan leiden tot een in potentie groot cybersecurityincident voor wat betreft spreiding en tijdsduur om dat er sprake is van verbinding met veel verschillende organisaties.
Schaal	Storing Crowdstrike (https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf) Op 19 juli 2024 vond het CrowdStrike incident plaats dat werd veroorzaakt door een foutieve patch op Microsoft Windows van de beveiligingssoftware van CrowdStrike. Patches worden routinematig en automatisch via CrowdStrike gedistribueerd om cybersecuritydreigingen af te wenden. De foutieve patch zorgde ervoor dat systemen vastliepen en er over de hele wereld storingen optraden waaronder in de luchtvaartsector. Deze casus laat zien dat cybersecurityincidenten zich (kunnen) kenmerken door een grote mate van onvoorspelbaarheid ten aanzien van de opschaling. Niemand had voorzien dat de impact van een foutieve automatische update van deze beveiligingssoftware zo grote en zichtbare gevolgen zou hebben.
Tijd	KPN storing 112 (https://archief.nipv.nl/wp-content/uploads/sites/2/2022/04/H6-20201104-IFV-Lessen-uit-crises-en-mini-crises-2019.pdf) Op 24 juni 2019 was het nationale noodnummer 112 onbereikbaar door een storing in het landelijke telefonienetwerk van KPN. Deze storing trof ook verschillende gemeenten en bedrijven. Naast de storing in het telefonienetwerk trad er een storing op in het onderdeel dat de distributie van NL-Alert berichten via het netwerk van KPN verzorgt. De storing van het telefonienetwerk werd veroorzaakt door het falen van het routeringsplatform dat de route naar de bestemming van een telefoongesprek vaststelt. Dit kwam door een onvolkomenheid in de softwareconfiguratie in combinatie met een groot aantal foutmeldingen in het routeringssysteem.

	Dergelijke storingen zijn niet volledig te voorkomen aangezien niet iedere situatie op voorhand denkbaar is. Deze casus illustreert dat een cybersecurityincident zich op verschillende plaatsen simulaan kan voordoen, dat slachtoffers hierdoor (kunnen) worden overvallen (omdat indicatoren onzichtbaar zijn) en dat veelal niet direct evident is dat er een incident gaande is.
Lokaliteit	Gijzelsoftware Veiligheidsregio Noord- en Oost-Gelderland (https://nipv.nl/wp-content/uploads/2022/02/20210518-IFV-Evaluatie-gijzelsoftware-VNOG.pdf) Op 12 september 2020 werd de Veiligheidsregio Noord- en Oost-Gelderland (VNOG) geconfronteerd met gijzelsoftware die leidde tot verstoring van interne computersystemen waardoor het interne bedrijfsnetwerk, verschillende applicaties en de email niet meer functioneerden. De VNOG liet zich vanwege de aard van de processen (die voor de VNOG anders zijn dan bij een reguliere crisis) ondersteunen bij het afhandelen van het incident door experts van de ICT-leverancier, het NCSC en van een cybersecurity consultancybureau. Deze casus illustreert dat het voor een organisatie vaak onvoldoende duidelijk is waar de verantwoordelijkheid voor de beveiliging van data, netwerken en systemen begint en eindigt en waar de infrastructuur zich precies bevindt, omdat het vaak onduidelijk is waar specifieke assets zich bevinden. In deze casus was behoefte aan diepgaande (externe) specialistische kennis met betrekking tot de ICT-infrastructuur om tot een oplossing van het incident te komen.

Tabel 3 - Voorbeelden van casuïstiek die de verschillen tussen incidenten in het fysieke en het digitale domein illustreren

IMPACT OP BESTURING VAN INCIDENTEN EN CRISES

Uit de stakeholdergesprekken, maar ook uit de bestudeerde documentatie (zie bijlagen A en B) is duidelijk geworden dat er belangrijke verschillen zijn in de besturing van incidenten en crises die voortvloeien uit de in de vorige paragraaf beschreven verschillen tussen het verloop ervan in het fysieke en digitale domein.

In onderstaande tabel wordt vanuit het gezichtspunt van een *incident in het digitale domein* aangegeven welk effect de verschillen ten opzichte van het fysieke domein hebben op besturingsuitdagingen. Met andere woorden: op welke gebieden ontstaan besturingsuitdagingen die rechtstreeks een gevolg zijn van de verschillen op gebied van verspreiding, verbinding, schaal, tijd en lokaliteit.

Kenmerk	Additionele uitdagingen besturing
Verspreiding	• Door de grillige verspreiding kunnen er snel meerdere plekken zijn waar een incident optreedt. Om goed grip te houden op het verloop van dit soort incidenten is helderheid over **taken en verantwoordelijkheden**, maar ook over **regie** en **mandaat** van belang. • Bij grilligere verspreiding zijn de traditionele **structuren voor opschaling** mogelijk niet toereikend en is extra duidelijkheid nodig over opschaling bij incidenten in het digitale domein.
Verbinding	• Doordat er sneller keteneffecten zijn is helderheid over **taken en verantwoordelijkheden** nodig (want wie zijn er

	betrokken), maar ook over **regie** en **mandaat** van belang (wie acteert wanneer en waarop). • Door potentieel bredere betrokkenheid van een keten, zijn de traditionele **structuren voor opschaling** mogelijk niet toereikend en is extra duidelijkheid nodig over opschaling bij incidenten in het digitale domein.
Schaal	• Bij minder zichtbare indicatoren kan het verloop incidenten en crises minder voorspelbaar zijn, waardoor **urgentie** minder snel duidelijk kan zijn. • Meer **inzicht en overzicht** over indicatoren die zicht geven op hoe incidenten en crises opschalen is ondersteunend in de keuzes voor besturing.
Tijd	• Vanwege minder zichtbare indicatoren kan de **urgentie** pas laat worden ervaren, terwijl deze idealiter eerder duidelijk zou zijn. • Meer **inzicht en overzicht** over indicatoren die zicht geven op hoe incidenten en crises verlopen in de tijd is ondersteunend in de keuzes voor besturing.
Lokaliteit	• Vanwege ketenafhankelijkheden (denk aan assets die bij meerder providers zijn ondergebracht) is helderheid over **taken en verantwoordelijkheden** nodig (want wie zijn er betrokken), maar ook over **regie** en **mandaat** van belang (wie acteert wanneer en waarop). • Het is van belang **inzicht en overzicht** te hebben over waar deze assets zich bevinden.
Alle	• Er is nog weinig consensus over goede basismaatregelen en **standaarden** zijn nog in ontwikkeling. • Er is gebrek aan **expertise en capaciteit** over het verloop van incidenten in het digitale domein.

Tabel 4 - Besturingsuitdagingen van het digitale domein ten opzichte van het fysieke domein

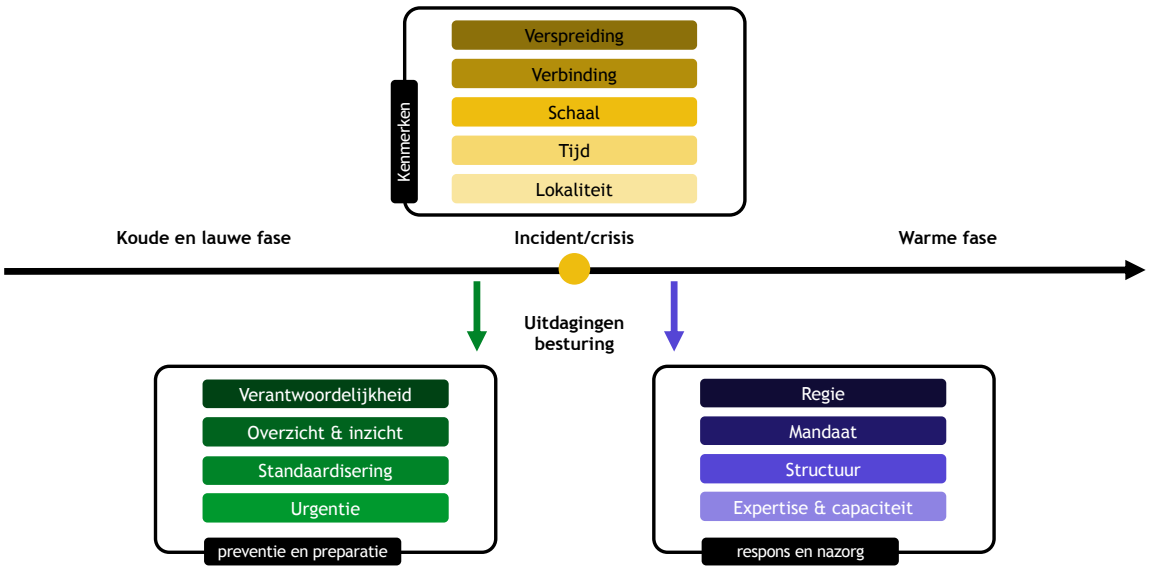
Bovenstaande tabel laat zien dat er uitdagingen zijn op acht gebieden, waarvan er vier gaan over de koude en lauwe fase van incidenten en crises:

1. Verantwoordelijkheid
2. Overzicht en inzicht
3. Standaardisering
4. Urgentie

Nog eens vier gaan over de warme fase van incidenten en crises:

5. Regie
6. Mandaat
7. Structuren
8. Expertise en capaciteit.

Onderstaande figuur geeft de relatie tussen de verschillende kenmerken en de impact op de besturing van incidenten en crises visueel weer.



Figuur 6 - Relatie tussen kenmerken van incidenten en crises en de uitdaging voor besturing

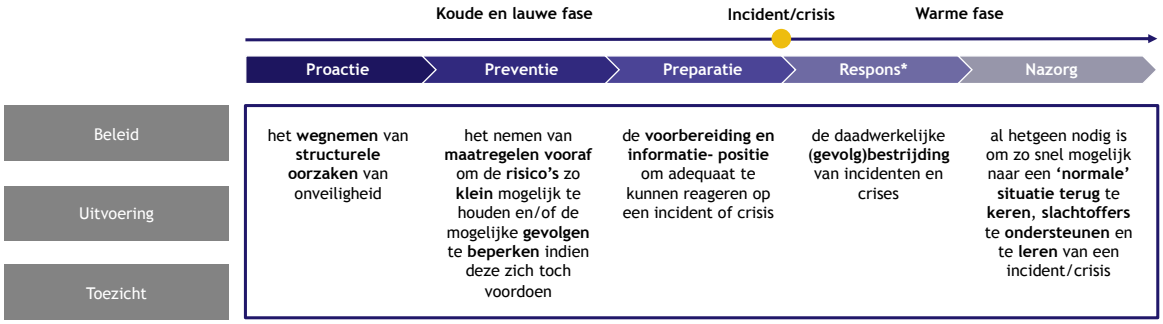
OVERZICHT LANDSCHAP DIGITALE VEILIGHEID

Om zicht te krijgen op de uitdagingen die er liggen op het terrein van digitale veiligheid voor gemeenten is het van belang om allereerst het huidige landschap op dit gebied in kaart te brengen voor wat betreft het beleid (1), de uitvoering: de huidige taken, verantwoordelijkheden en bevoegdheden (2) en het toezicht op gemeenten (3). Dit hebben we gedaan langs de dimensies van de incidentcategorieën die we in de inleiding hebben geschetst (zie Tabel 1):

A. Uitval en verstoring van dienstverlening en gemeenteprocessen wegens het niet op orde zijn van de interne digitale veiligheid van gemeenten.
B. Ontwrichting binnen gemeentegrenzen als gevolg van een cyberincident.
C. Cybercrime en gedigitaliseerde criminaliteit die zich binnen gemeentegrenzen manifesteert.
D. Online aangejaagde openbare-ordeverstoringen binnen gemeentegrenzen.

Om het landschap goed in kaart te brengen, maken we gebruik van de stappen uit de veiligheidsketen[10], een model dat in het fysieke veiligheidsdomein door gemeenten en veiligheidsregio's al veel wordt ingezet en daardoor vanuit lokaal perspectief herkenbaar is (zie onderstaande figuur). De vierde fase in de veiligheidsketen heet 'repressie'. Wij hebben in dit document voor de term 'respons' gekozen omdat deze term beter aansluit op de thematiek in dit rapport en het digitale domein. In het digitale domein valt voor wat betreft de uitwerking in dit rapport herstelvermogen om de processen en systemen te herstellen onder de noemer respons. Ook kan het zijn dat bij respons van incidenten in het digitale domein, respons zich ook kan richten op maatregelen in het fysieke domein. Denk bijvoorbeeld aan een fysiek gebiedsverbod of een stopgesprek. Onder nazorg valt onder andere evalueren, maar bijvoorbeeld ook slachtofferhulp.

[10] Bron: Stol, W., Tielenburg, C., Rodenhuis, W., Pleysier, S., & Timmer, J., 2011, Basisboek integrale veiligheid, Den Haag: Boom Lemma uitgevers.



Figuur 7 - De veiligheidsketen om te gebruiken voor het beschrijven van het landschap

We hebben voor alle vier incidentcategorieën in kaart gebracht welk beleid voorhanden is, wat de taken, verantwoordelijkheden en bevoegdheden zijn van gemeenten, maar ook van belangrijke (voornamelijk publieke) stakeholders die een rol vervullen rondom de afhandeling van incidenten en crises en hoe het toezicht is ingericht. In dit hoofdstuk vatten we de conclusies op hoofdlijnen samen. In de hierop volgende hoofdstukken doen we dat in verder detail.

BELEID

Voor dit onderzoek hebben we in kaart gebracht welke relevante handreikingen, beleidsdocumenten en initiatieven er al voorhanden zijn en waaraan wordt gewerkt. Zie hiervoor bijlage B. We hebben dit beleid gemapt op de fasen van de veiligheidsketen en komen dan tot onderstaand overzicht.

	Koude en lauwe fase			Warme fase	
Categorieën	Proactie	Preventie	Preparatie	Respons	Nazorg
A Interne digitale veiligheid gemeenten	9, 24, 28, 29, 32, 30, 33, 34, 35, 44, 58, 59, 63, 70, 82	19, 20, 21, 22, 23, 51, 59, 64	10, 11, 25, 38, 39, 59, 65, 78, 83	59, 83	18, 53, 54, 55, 59
B Ontwrichting binnen de gemeentegrenzen door een cyberincident	9, 30, 52, 58, 63, 67, 68, 69, 70	19, 20, 21, 22, 64	10, 11, 25, 38, 39, 62, 65, 78, 79, 80, 84	62, 81	53, 54, 55
C Cybercrime en gedigitaliseerde criminaliteit die zich binnen de gemeentegrenzen manifesteert	9, 30, 58, 70, 87, 88	12, 13, 19, 20, 21, 22, 26, 27, 43, 71, 72, 86	72, 75	72, 76	72
D Online aangejaagde ordeverstoringen binnen de gemeentegrenzen	4, 9, 30, 37, 58, 70	12, 13, 72, 73, 74	72, 77	72	72

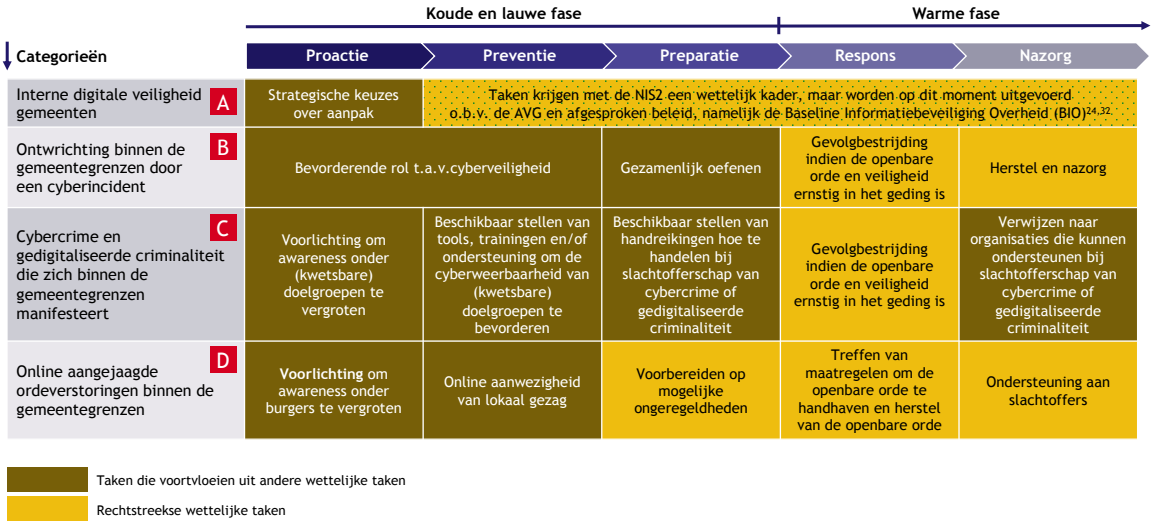
Figuur 8 - Overzicht van beschikbaar beleid (voor de verwijzing van de nummers, zie bijlage B)

Zonder hierbij naar de inhoud van deze documenten en initiatieven te kijken (dat doen we in de hiernavolgende hoofdstukken) laat dit overzicht zien dat er veel beleid is ontwikkeld voor de koude en lauwe fase en minder beleid voorhanden is voor de warme fase. Dat is opvallend te noemen, temeer daar gemeenten vooral een rol hebben in de warme fase (zie hiervoor de volgende sectie: uitvoering). Hoewel het logisch is dat beleid zich (ook) richt op proactie, preventie en preparatie zou het goed zijn om bestaand beleid op gebied van respons en nazorg nog eens tegen het licht te houden door deze bril om te beoordelen of dat voldoende voorhanden is.

UITVOERING

Naast beleid hebben we onderzocht wat de huidige taken, verantwoordelijkheden en bevoegdheden zijn van gemeenten, maar ook van andere betrokken (met name publieke) stakeholders voor de vier incidentcategorieën. Dat levert voor de gemeenten het beeld op uit onderstaande figuur. De gele vakjes in deze figuur refereren aan rechtstreekse wettelijke taken. De bruine vakjes gaan over taken die indirect volgen uit meer algemene wettelijke taken van gemeenten. Kort samengevat levert dat het volgende beeld op:

A. Gemeenten hebben bij de beveiliging van eigen processen en systemen de verantwoordelijkheid en intrinsieke plicht om in de fasen van preventie tot en met nazorg incidenten en crises af te handelen. Op dit moment is de verplichting tot het beveiligen van eigen processen en systemen nog niet rechtstreeks wettelijk maar wel bestuurlijk vastgelegd. Ze volgen voornamelijk uit de Baseline Informatiebeveiliging Overheid. De BIO is een voorbeeld van zelfregulering door overheden. Het rijk, de provincies, gemeenten en waterschappen hebben zichzelf de verplichting opgelegd om aan deze norm te voldoen. Ook volgen vereisten tot informatiebeveiliging van gemeenten uit bestaande wetgeving zoals de AVG, Wet Suwi, BRP, etc... In de nabije toekomst zullen vereisten voor informatiebeveiliging van gemeenten wettelijk verankerd worden in de Cyberbeveiligingswet (Cbw) omdat gemeenten zijn aangemerkt als essentiële entiteiten onder de Cbw.
B. Bij ontwrichting binnen gemeentegrenzen liggen de wettelijke taken, verantwoordelijkheden en bevoegdheden van gemeenten vooral in de fasen van respons en nazorg. Het gaat dan om incidentgevolgbestrijding als de openbare orde en veiligheid in het geding is.
C. Ook voor wat betreft cybercrime en digitale criminaliteit liggen de wettelijke taken, verantwoordelijkheden en bevoegdheden vooral op gebied van respons. Uit de stakeholdergesprekken met gemeenten, OM en politie ontstaat het beeld dat gemeenten een grotere taak zouden kunnen hebben voor wat betreft slachtoffer- en daderpreventie, bijvoorbeeld als het gaat om voorlichting. Wel zijn daarvoor dan middelen nodig. Deze taak ligt nu met name bij de politie, de Platforms Veilig Ondernemen (PVO's) en cyberweerbaarheidscentra. De ministeries van BZK en J&V hebben preventieactiviteiten voor verschillende doelgroepen gestimuleerd, onder andere via het City Deal-programma.
D. Bij online aangejaagde openbare-ordeverstoringen heeft de gemeente in alle fasen wettelijke taken, verantwoordelijkheden en bevoegdheden. Die zijn ook hier met name gericht op effecten in het fysieke domein. De vraagstelling die hier met name speelt is hoe eerder zicht kan worden verkregen op situaties die online spelen voordat ze plotseling door een ordeverstoring zichtbaar worden in het fysieke domein. Dat ziet toe op de informatiebehoefte van gemeenten.



Figuur 9 - Taken en verantwoordelijkheden van gemeenten bij cyberincidenten

Hoe de taken, verantwoordelijkheden en bevoegdheden van gemeenten in de verschillende incidentcategorieën zich verhouden tot die van andere (met name publieke) stakeholders wordt in de volgende hoofdstukken per incidentcategorie nader toegelicht.

TOEZICHT

Er zijn diverse organisaties die betrokken zijn bij controle van en toezicht op elementen van digitale veiligheid van gemeenten in alle vier incidentcategorieën. De gemeenteraad heeft een kader stellende en controlerende taak richting het college van burgemeester en wethouders. Het college legt als eerste verantwoording af aan de gemeenteraad. Dit wordt ook wel horizontale controle genoemd.

Daarnaast zijn er diverse toezichthouders betrokken. Zo zijn er stelselhouders die toetsen of gemeenten aan hun (aansluit)voorwaarden voldoen. Daarnaast zijn er inspecties voor specifieke stelsels, zoals bijvoorbeeld de Autoriteit Persoonsgegevens in het kader van de Algemene Verordening Gegevensbescherming (AVG). Binnenkort wordt er aan dit totaal aan toezicht nog een nieuwe toezichthouder toegevoegd vanwege de Cyberbeveiligingswet: de Rijksinspectie voor Digitale Infrastructuur (RDI). De werkzaamheden van toezichthouders worden verticaal toezicht genoemd.

Toezicht wordt in de navolgende hoofdstukken per incidentcategorie in verder detail uitgewerkt.

Belangrijk instrument bij het afleggen van verantwoording door gemeenten in het kader van toezicht is ENSIA[11] - Eenduidige Normatiek Single Information Audit. Het doel van ENSIA is om tot een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid te komen, gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). In de toekomst zal ENSIA gebruikt worden in het kader van verantwoording ten aanzien van de Cyberbeveiligingswet (Cbw). ENSIA

[11] https://vng.nl/projecten/ensia

structureert verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI) richting de rijksoverheid en gemeenteraad.

Alle Nederlandse gemeentebesturen leggen in het kader van ENSIA jaarlijks op hetzelfde moment en via dezelfde methode, verantwoording af over hun informatieveiligheid, datakwaliteit en data-integriteit. Het self-assessment strekt zich ook uit tot uitbestede diensten. Gemeentebesturen gebruiken de informatie uit de ENSIA-audit voor de verantwoording aan de gemeenteraad én aan toezichthouders binnen de rijksoverheid (daar waar het gaat om het gebruik van de genoemde landelijke voorzieningen). De ENSIA-methode geeft gemeenten inzicht in de risico's op het vlak van informatiebeveiliging en helpt gemeenten om de juiste maatregelen te nemen.

Het toezichtstelsel op de Cbw en de Wwke zal meer wetten en regelingen kennen dan de zeven stelsels die nu in ENSIA zijn opgenomen. Het effect hiervan op de scope van ENSIA wordt op dit moment onderzocht.

	Koude en lauwe fase			Warme fase	
↓ Toezichthouders	Proactie	Preventie	Preparatie	Respons	Nazorg
Gemeenteraad	• ENSIA[5,6] structureert verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI) richting de rijksoverheid en gemeenteraad • Toezicht op Gemeenschappelijke Regelingen door bestuurders (dagelijks bestuur en algemeen bestuur) • Toezicht op inzet bevoegdheden				
Toezichthouders Rijksoverheid	• ENSIA[5,6] structureert verantwoording over de Basisregistratie Personen (BRP) en Reisdocumenten, Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT), Basisregistratie Ondergrond (BRO) en de Structuur uitvoeringsorganisatie Werk en Inkomen (SUWI) richting de rijksoverheid en gemeenteraad				
Rijksinspectie voor de Digitale Infrastructuur (RDI) (op systeemniveau, feitelijk de gemeenteraad)	• Samenhangend Inspectiebeeld cybersecurity vitale processen[66] • Significante incidenten i.k.v. de nieuwe Cbw moeten worden gemeld aan de toezichthouder • De toezichthouder i.k.v. de CBW kan informatie opvragen om te onderzoeken hoe incidenten worden opgevolgd om daar lering uit te trekken				

Figuur 10 - Overzicht van toezichthouders[12] gemeenten in relatie tot cyberincidenten

[12] De gemeenteraad is formeel gezien geen toezichthouder, maar controleert het college van B&W

UITDAGINGEN
DIGITALE VEILIGHEID

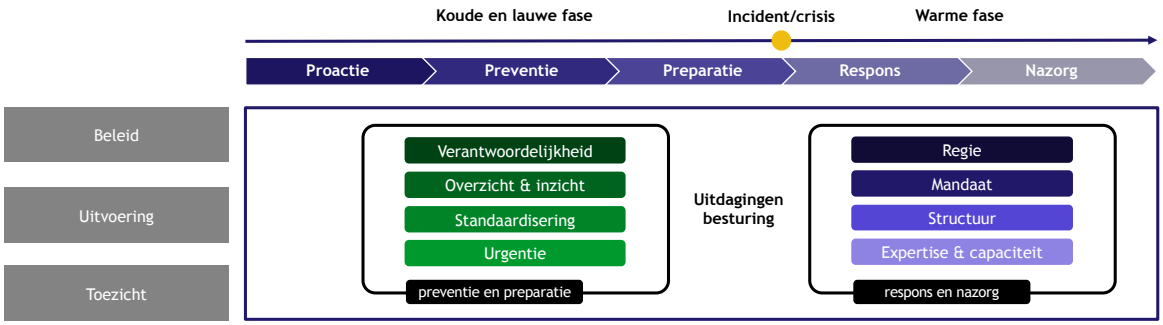
Er wordt binnen gemeenten al veel gedaan aan digitale veiligheid op de vier incidentcategorieën (A) eigen digitale veiligheid, (B) ontwrichting door een incident bij een organisatie binnen gemeentegrenzen, (C) cybercrime en gedigitaliseerde criminaliteit en (D) online aangejaagde openbare-ordeverstoringen. Daarbij moet overigens worden opgemerkt dat gemeenten deze onderwerpen vaak belegd hebben bij verschillende afdelingen. Zo werken er vaak CISO-teams aan de eigen digitale veiligheid terwijl collega's uit het openbare orde en veiligheidsteam (OOV) werken aan één of meer van de andere thema's. Nog niet altijd wordt er tussen deze afdelingen samengewerkt.

Naast inzicht in wat er nu al gebeurt op de vier incidentcategorieën (zoals op hoofdlijnen omschreven in het voorgaande hoofdstuk), is er tijdens de gesprekken met stakeholders, maar ook in de analyse van de verschillende beleidsdocumenten in kaart gebracht welke behoeften er liggen voor de toekomst voor wat betreft de verdere ontwikkeling van digitale veiligheid op de vier gebieden en welke informatiebehoefte er is bij gemeenten die hen in staat stelt hun taken op deze terreinen goed uit te voeren.

Dit heeft geleid tot de formulering van enkele tientallen behoeften die verderop in dit hoofdstuk en de rest van dit document worden beschreven. Wat echter lastig is, is om voor deze gevallen op waarde te schatten of de gestelde behoefte breed wordt herkend en erkend, of deze haalbaar is, realistisch is en wie eventueel aan zet is om aan deze behoefte invulling te geven. In dit document volstaan we voor nu met het omschrijven van de behoefte en het geven van een specifiekere onderbouwing waar mogelijk (met een toelichting van stakeholders die als respondent fungeerden, bestudeerde publicaties en/of onderzochte casuïstiek). Bij de verdere uitwerking van het bestuurlijk convenant zal een nadere uitwerking nodig zijn, waarbij in kaart wordt gebracht welke concrete casuïstiek ten grondslag ligt aan de gestelde behoeften zodat de achterliggende vraag concreet kan worden gemaakt. Bovendien moet in een

nadere uitwerking worden vastgesteld hoe breed die behoefte leeft en hoe realistisch ze is. Ook moeten er prioriteiten worden gesteld voor wat betreft de invulling van de behoeften en moeten er eventueel actiehouders aan worden toegekend. Dit punt nemen we mee in de aanbevelingen in het laatste hoofdstuk van dit document.

Uit onze eerdere analyse van de verschillen tussen het fysieke en digitale veiligheidsstelsel is gebleken dat de voornaamste uitdagingen voor besturing van incidenten en crises liggen op acht terreinen, waarvan vier in de koude en lauwe fase (verantwoordelijkheid, overzicht en inzicht, standaardisering, urgentie) en vier in de warme fase (regie, mandaat, structuur, expertise en capaciteit), zie onderstaande figuur.



Figuur 11 - Aandachtspunten bij de besturing van cyberincidenten

De uitkomsten van de analyse van de beleidsdocumenten en stakeholdergesprekken hebben we beschreven aan de hand van deze acht terreinen. In onderstaande sectie zijn de belangrijkste uitdagingen per incidentcategorie beschreven. Deze zijn tot stand gekomen op basis van een analyse van de geïnventariseerde uitdagingen per incidentcategorie die in detail beschreven zijn in de hierop volgende hoofdstukken.

BELANGRIJKSTE UITDAGINGEN PER INCIDENTCATEGORIE

Voor de eerste incidentcategorie uitval dienstverlening en gemeenteprocessen wegens niet op de orde hebben van de *interne digitale veiligheid* zien we uitdagingen op alle acht besturingsuitdagingen. De voornaamste uitdagingen die uit de analyse van de documenten en gesprekken volgen zijn:

1. Er is een gebrek aan duidelijkheid over de verantwoordelijkheden die verschillende stakeholders hebben vanwege de complexiteit van systemen (IT, OT, gemeenschappelijke regelingen, etc.). Dit maakt het diffuus wie wanneer waarvoor aan zet is voor digitale veiligheid.
2. Er is onvoldoende duidelijkheid over keteneffecten van incidenten. Steeds vaker zijn processen en netwerk- en informatiesystemen van verschillende organisaties (waaronder toeleveranciers) aan elkaar verbonden waardoor keteneffecten (kunnen) ontstaan als er incidenten plaatsvinden.
3. Toeleveranciers vormen mogelijk een kwetsbare schakel, vooral leveranciers die door veel gemeenten voor diverse doeleinden in verschillende domeinen worden ingezet. Overzicht van veel gebruikte systemen en leveranciers ontbreekt op dit

moment. Ook kan er beter worden samengewerkt als het gaat om het toezien op de digitale veiligheid van gezamenlijke systemen en leveranciers.
4. Er zijn veel handreikingen voor digitale veiligheid ontwikkeld, onder andere vanuit de Vereniging Nederlandse Gemeenten (VNG), maar gebruik door gemeenten in de praktijk moet verder vormkrijgen onder andere door voorlichting en/of begeleiding over de toepassing.
5. ENSIA is zinvol, maar behoeft vereenvoudiging, aansluiting op de nieuwe wetgeving en harmonisering van normenkaders.
6. Voor respons moeten benodigde structuren en netwerken nog verder worden ingericht.
7. Om kleinere gemeenten te ondersteunen kunnen grotere gemeenten een steviger rol spelen (groot helpt klein).

Bij de tweede incidentcategorie *ontwrichting* zien we de voornaamste uitdagingen op verantwoordelijkheid, overzicht & inzicht en alle vier thema's rondom respons en nazorg:

1. De rol van gemeenten (en de burgemeester) bij incidenten met ontwrichting kan nog duidelijker worden gedefinieerd, evenals de rol van veiligheidsregio's: wie is wanneer waarvoor verantwoordelijk en heeft welke taken en bevoegdheden?
2. Er is behoefte aan meer inzicht in het bredere netwerk (publiek en privaat) dat een rol speelt bij dit incidenttype evenals inzicht in welke typen incidenten relatief vaker (kunnen) voorkomen in een bepaalde regio.
3. Er is behoefte aan meer helderheid in de rolverdeling voor wat betreft regie en mandaat en ondersteunende structuren voor opschaling en informatiedeling.
    a. Er is behoefte aan met GRIP vergelijkbare helderheid over opschaling.
    b. Er is behoefte aan tijdige informatie bij gemeenten over mogelijke ernstige verstoring van openbare orde en veiligheid, niet zozeer *incident*informatie, maar *gevolg*informatie.

Op gebied van de derde categorie *cybercrime en gedigitaliseerde criminaliteit* liggen uitdagingen op de thema's verantwoordelijkheid, overzicht & inzicht, mandaat en expertise & capaciteit:

1. Belangrijk vraagstuk is hoe dader- en slachtofferpreventie beter kan worden aangepakt en door wie. Zoals eerder opgemerkt kunnen, mits daar middelen voor zijn, gemeenten een rol spelen.
2. Vraag is eveneens hoe met (bestaande) bevoegdheden meer zicht kan worden verkregen op de modus operandi van criminelen in het digitale domein en effectiever interventies kunnen worden gedaan.
3. Er is behoefte aan een meer globaal overzicht in de problematiek van cybercrime en gedigitaliseerde criminaliteit (aard, omvang, verschijningsvormen, kwetsbaarheden, mogelijke gevolgen, dader- en slachtofferprofielen) danwel is het nodig dat al beschikbare overzichten een breder publiek bereiken. Deze informatie is van belang om preventie goed in te kunnen richten.

4. Er is behoefte aan een overzicht over en inzicht in de effectiviteit van de aanpak danwel is het nodig dat al beschikbare overzichten een breder publiek bereiken (best practices & lessons learned).
5. Nadere afstemming over activiteiten op met name preventie is gewenst, omdat het aanbod van verschillende partijen elkaar lijkt te raken en soms ook overlapt, terwijl er elders mogelijk lacunes in het aanbod zijn, dan wel (kunnen) ontstaan.
6. Er is zorg over de aanwezigheid van voldoende kennis, capaciteit en prioriteit.

Bij de vierde incidentcategorie *online aangejaagde openbare-ordeverstoringen* liggen de voornaamste uitdagingen op overzicht & inzicht en mandaat:

1. Er is behoefte aan meer zicht op wat er speelt op dit thema binnen het digitale domein, dus: hoe krijg je beter zicht op (dreigende) onrust die kan leiden tot ernstige verstoring van openbare orde en veiligheid) en welke bevoegdheden hiervoor wanneer kunnen worden ingezet, ook voor preventie en nazorg.
2. Voor het fysieke domein is er voldoende houvast in termen van regie, mandaat en structuur, maar die ontbreekt nog voor het digitale domein.
3. Er is behoefte aan handelingsperspectief bij een (dreigend) incident waarbij de bron zich buiten de gemeentegrenzen ophoudt en de gevolgen zich binnen de gemeentegrenzen (kunnen) manifesteren.

OVERKOEPELENDE UITDAGINGEN

Ook is er een aantal uitdagingen te benoemen die overkoepelend zijn en daarmee op alle incidentcategorieën van toepassing. Het gaat om de volgende zaken:

1. Het overzicht van het landschap dat in dit rapport wordt gegeven voegt waarde toe voor verschillende stakeholders omdat dit overzicht nog niet eerder voorhanden was. Uitdaging is om dit ook in de toekomst actueel te houden.
2. Een (periodieke) meting over de mate van digitale weerbaarheid van gemeenten op de vier incidentcategorieën (de wegen uit de Lokale Cyberwegenkaart) is van toegevoegde waarde om een goed beeld te verkrijgen waar gemeenten nu staan (vergelijkbaar met wat het samenwerkingsverband NH Veilig recent heeft onderzocht en ook het CCV heeft in 2024 iets beknopter een landelijke thermometer uitgevoerd). Zo'n meting biedt gemeenten zelf inzicht, maar is (geanonimiseerd) ook van waarde om regionaal en nationaal prioriteiten te stellen.
3. Ondanks dat er al veel bestuurlijke gesprekken zijn gevoerd is er nog steeds een beperkt gevoel van urgentie bij bestuurders (en raadsleden) op gemeentelijk niveau. Daarbij is er gebrek aan expertise, ook bij ambtenaren om over de gehele breedte van de uitdagingen in het digitale domein de juiste keuzes te (kunnen) maken. Er ontstaat een beeld dat de basis nog niet overal op orde is. Ook is er veel vrijblijvendheid in keuzes van wat wel en niet te doen op basis van een zorgvuldige afwegingen.
4. Er wordt op veel verschillende plekken ingezet op gezamenlijk oefenen, maar daardoor is er wel een wildgroei ontstaan van dit soort initiatieven. Als dit beter

wordt gestroomlijnd, komt er wellicht capaciteit vrij om te werken aan het verbeteren van benodigde structuren voor incidentafhandeling en crisisbeheersing.

INTERNE DIGITALE VEILIGHEID GEMEENTEN

In dit hoofdstuk wordt het huidige landschap alsook de uitdagingen en informatiebehoefte beschreven vanuit het perspectief van de eigen digitale veiligheid van gemeenten.

BELEID

Er is veel beleid voorhanden gericht op de beveiliging van de eigen processen en systemen van gemeenten. Deze worden in onderstaande tabel opgesomd en ingedeeld in de fasen van de veiligheidsketen[13]. De nummers verwijzen naar bijlage B. Opvallend is dat dit beleid zich vooral richt op de fasen proactie, preventie en preparatie en minder op respons en nazorg. Beleid in die fasen kan gemeenten nog verder ondersteunen in de wijze waarop zij respons en nazorg inrichten.

Proactie	Preventie	Preparatie	Respons	Nazorg

• Focusblad Digitale Veiligheid, gekoppeld aan het Kernbeleid Veiligheid[70]
• Doorontwikkeling BIO[24, 32]
• Inkoopeisen Cybersecurity Overheid voor aanbieders van de overheid[28,29,63]
• Methoden voor diepgaande risicoanalyse en impactanalyse bedrijfsprocessen gemeenten i.k.v. BIO en
	• VNG factsheets rondom continuïteit, zoals Model Continuïteitsstrategie en Bepalen kritische bedrijfsprocessen[59]
	• Dreigingsbeeld IB Nederlandse gemeenten[51]
	• Cyberaanvallen door statelijke actoren[64]
	• Ontwikkelingen rondom herkenbare overheid[19, 20, 21, 22]
		• VNG factsheets over voorbereiding op incidenten en digitaal forensisch onderzoek[59]
		• Scenario-ontwikkeling[65]
		• Oefenen via
		  ○ Interactieve cyberoefeningen[10]
		  ○ Overheidsbreed Cyberprogramma (bijv. red teaming, webinars, …)[11,25]
		  ○ Isidoor[38,39,78]
			• VNG factsheet over hoe verder na een hack[59]
			• Cyber- en IT-crisisplannen, bijvoorbeeld: Den Haag[83]
				• Risicobeheerfonds Cyber bij schade[18]
				• VNG factsheet strategie en handreiking back-up en recovery[59]
				• Best practices en lessons learned[53,54,55]

[13] Dit overzicht is gecreëerd op basis van input uit de gesprekken, mogelijk ontbreken er nog enkele zaken die in een later stadium kunnen worden aangevuld

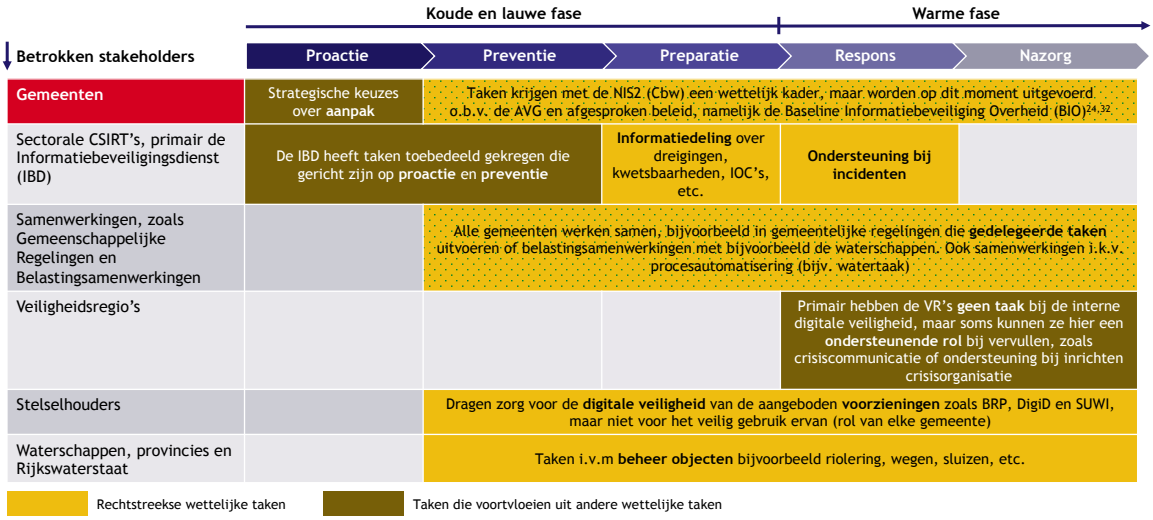
verder inzicht[34,44,59] • Gesprekken met lokale bestuurders[9,35] en digitale sessies voor o.a. CISO's[58] over digitale veiligheid[33] • Digitale Agenda Gemeenten (DAG) 2024[82] • Informatiebe-hoefte G4[30]	• Meting informatie-veiligheidsstand aarden[23]			

Tabel 5 - Overzicht beleid interne digitale veiligheid gemeenten

UITVOERING

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. In de praktijk is dit complexer dan dat het wellicht op het eerste oog lijkt. Dat komt onder andere doordat gemeenten met elkaar samenwerken in allerlei samenwerkingsvormen, zoals gemeenschappelijke regelingen en belastingsamenwerkingen, die soms gedelegeerde taken vanuit gemeenten uitvoeren en daarmee impact hebben op de digitale veiligheid van gemeenten. Gemeenten werken vaak samen met één of meerdere sectorale CSIRT's, bijvoorbeeld de Informatiebeveiligingsdienst (IBD), maar soms ook met anders CSIRT's, zoals Z-CERT of het NCSC. Zij ontvangen informatie en kunnen een beroep doen op ondersteuning ten tijde van een incident. Gemeenten hebben verder te maken met stelselhouders die verantwoordelijk zijn voor de digitale veiligheid van voorzieningen die gemeenten gebruiken, zoals bijvoorbeeld SUWI en DigiD. Ook zijn er relaties met waterschappen, provincies en Rijkswaterstaat die taken hebben rondom het beheer van bepaalde objecten die zich in of vlak bij een gemeente bevinden, zoals riolering, wegen en sluizen. Veiligheidsregio's hebben geen wettelijke taak in dit domein wanneer het enkel de digitale veiligheid van de gemeentelijke organisatie zelf betreft, maar hebben soms toch een ondersteunende rol rondom incidenten, bijvoorbeeld door het bieden van ondersteuning bij crisiscommunicatie.

Deze rolverdeling is grafisch weergegeven in onderstaande figuur. De gele blokken verwijzen naar rechtstreekse wettelijke taken en de bruine blokken naar taken die voortvloeien uit meer algemene wettelijke taken.



Figuur 12 - Rollen en taken interne digitale veiligheid gemeenten

De bevoegdheden die de verschillende stakeholders hebben rondom de interne digitale veiligheid van gemeenten komen voort uit meerdere wetten, waaronder in de loop van 2025 ook de Cyberbeveiligingswet. Onderstaande tabel somt deze op waarbij de nummers verwijzen naar bijlage B.

Organisatie	Wettelijk kader
Gemeenten	• Nu en straks: Algemene Verordening Gegevensbescherming (AVG) • Straks: Cyberbeveiligingswet[14] • Burgers en bedrijven kunnen veilig en betrouwbaar inloggen met elektronische identificatiemiddelen (eID) met een hoge mate van betrouwbaarheid (Wet digitale overheid)[B.24]
Sectorale CSIRT's, primair de Informatie Beveiligingsdienst (IBD)	• Straks: Cyberbeveiligingswet[14]
Gemeenschappelijke regelingen	• Wet Gemeenschappelijke Regelingen (WGR) • Nu en straks: Algemene Verordening Gegevensbescherming (AVG) • Straks: Cyberbeveiligingswet[14]. Een gemeenschappelijke regeling valt onder de NIS2, mits het voldoet aan de criteria van een overheidsentiteit van de Cyberbeveiligingswet. Samenwerkingen op het gebied van bedrijfsvoering en ICT hebben er indirect mee te maken omdat de deelnemende gemeenten zich moeten verantwoorden over de digitale veiligheid bij deze regelingen.
Veiligheidsregio's	• Nu en straks: Algemene Verordening Gegevensbescherming (AVG) • Oefenen ter voorbereiding op openbare orde verstoringen (Artikel 10 Wet Veiligheidsregio's)[B.25] • Nazorg na een (dreigend) incident Wet Veiligheidsregio's (Artikel 2.1.3. Wet Veiligheidsregio's)[B.25]
Stelselhouders	• Paspoortuitvoeringsregeling (PUN)[B.26], Paspoortwet[B.27], Wet basisadministraties persoonsgegevens BES[B.28]

	• Basisregistratie Personen (BRP)[B.29], Algemene verordening gegevensbescherming (AVG)[B.30] • Digitale persoonsidentificatie (DigiD)[B.31], Besluit digitale overheid[B.24] en de Regeling voorzieningen Wdo[B.24] • Basisregistratie Adressen en Gebouwen (BAG)[B.32], Wet basisregistratie adressen en gebouwen[B.33] en Organisatiewet Kadaster[B.34] • Basisregistratie Grootschalige Topografie (BGT) [B.35], Wet basisregistratie grootschalige topografie[B.35] en Organisatiewet Kadaster[B.34] • Basisregistratie Ondergrond (BRO) [B.36] en Handelsregisterwet[B.37] • Wet Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet) [B.38], Werkloosheidswet [B.39], Wet inkomensvoorziening oudere werklozen[B.40], Ziektewet[B.41], Wet op de arbeidsongeschiktheidsverzekering[B.42], Wet werk en inkomen naar arbeidsvermogen[B.43], Toeslagenwet[B.44], Algemene Ouderdomswet[B.45], Algemene nabestaandenwet[B.46], Algemene Kinderbijslagwet[B.47], Wet arbeidsongeschiktheidsverzekering zelfstandigen[B.48], Wet arbeidsongeschiktheidsvoorziening jonggehandicapten[B.49], Participatiewet[B.50], Wet Maatschappelijke ondersteuning (Wmo)[B.51] en Jeugdwet[B.52]

Tabel 6 - Wettelijke kaders interne digitale veiligheid gemeenten

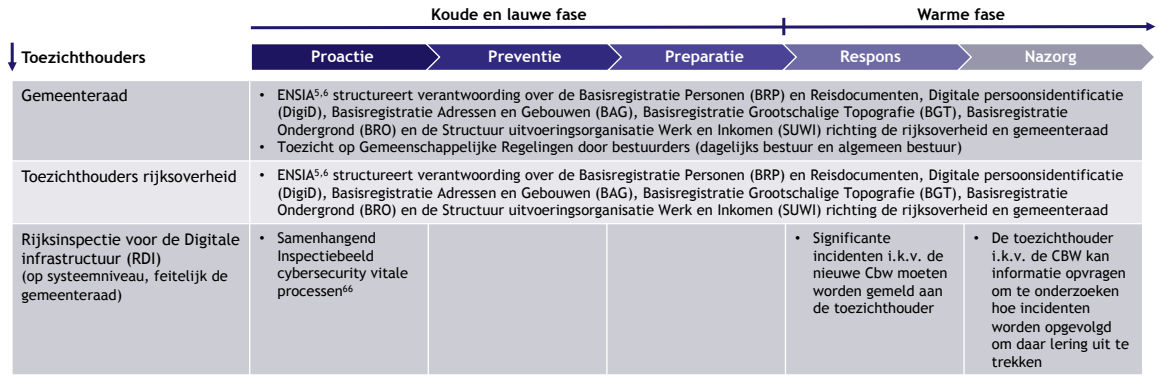
TOEZICHT

Allereerst heeft de gemeenteraad een kader stellende en controlerende rol richting het college van burgemeester en wethouders. Het college legt als eerste verantwoording af aan de gemeenteraad in wat ook wel horizontale controle wordt genoemd.

Daarnaast zijn er diverse toezichthouders betrokken vanuit wat verticaal toezicht wordt genoemd. Zo zijn er stelselhouders die toetsen of gemeenten aan hun (aansluit)voorwaarden voldoen, bijvoorbeeld voor de basisregistratie persoonsgegevens (BRP) en DigiD. Daarnaast zijn er inspecties voor specifieke stelsels, zoals bijvoorbeeld de Autoriteit Persoonsgegevens in het kader van de Algemene Verordening Gegevensbescherming (AVG). Binnenkort wordt er aan dit totaal aan toezicht nog een nieuwe toezichthouder toegevoegd vanwege de Cyberbeveiligingswet: de Rijksinspectie voor Digitale Infrastructuur (RDI).

ENSIA (Eenduidige Normatiek Single Information Audit) speelt hierbij een belangrijke rol en blijft dat naar verwachting in de toekomst ook doen. Insteek van ENSIA is via één keer uitvragen, meermaals te verantwoorden. Gemeenten moeten in het kader van ENSIA een jaarlijks self-assessment uitvoeren waarin zij vaststellen in hoeverre zij aan de eisen voldoen en welk volwassenheidsniveau van informatieveiligheid op dat moment voor hen geldt. Het self-assessment strekt zich ook uit tot uitbestede diensten.

Onderstaande figuur geeft een overzicht van het toezicht op de interne digitale veiligheid van gemeenten.



Figuur 13 - Toezichthouders[14] interne digitale veiligheid gemeenten

UITDAGINGEN BESTURING

Tijdens consultatiegesprekken (zie bijlage A), maar ook uit de bestudeerde documentatie (zie de sectie over beleid) zijn de uitdagingen rondom de interne digitale veiligheid van gemeenten in kaart gebracht. Deze hebben wij gekoppeld aan de acht uitdagingen op gebied van besturing van digitale veiligheid (zie pagina 20). Bij sommige uitdagingen is er een voor de hand liggende eenvoudige oplossingsrichting. Als dat het geval is, wordt die in deze paragraaf beschreven en in bijlage C opgenomen in een lijst met suggesties voor oplossingen.

We merken hierbij op, zoals ook eerder in dit document aangegeven, dat de uitdagingen gebaseerd zijn op behoeften waarvan lastig in te schatten is in hoeverre deze breed wordt herkend en erkend, of deze haalbaar is, realistisch is en wie eventueel aan zet is om aan deze behoefte invulling te geven. In dit document volstaan we voor nu met het omschrijven van de behoefte en het geven van een specifiekere onderbouwing waar mogelijk (met een toelichting van stakeholders die als respondent fungeerden, bestudeerde publicaties en/of onderzochte casuïstiek). Bij de verdere uitwerking van het bestuurlijk convenant zal een nadere uitwerking nodig zijn, waarbij in kaart wordt gebracht welke concrete casuïstiek ten grondslag ligt aan de gestelde behoeften zodat de achterliggende vraag concreet kan worden gemaakt. Bovendien moet in een nadere uitwerking worden vastgesteld hoe breed die behoefte leeft en hoe realistisch ze is. Ook moeten er prioriteiten worden gesteld voor wat betreft de invulling van de behoeften en moeten er eventueel actiehouders aan worden toegekend. Dit punt nemen we mee in de aanbevelingen in het laatste hoofdstuk van dit document.

[14] De gemeenteraad is formeel gezien geen toezichthouder, maar controleert het college van B&W

Uitdagingen in de koude en lauwe fase

De belangrijkste uitdagingen in deze fase liggen op vier thema's:

1. Verantwoordelijkheid
    a. Er bestaat onvoldoende duidelijkheid over de verantwoordelijkheid van digitale processen en systemen van een gemeente vanwege de complexiteit ervan, mede door de betrokkenheid van meerdere partijen. Het gaat om (on)duidelijkheid doordat gemeentelijke IT-systemen en OT-systemen binnen de gemeentegrenzen bij veel verschillende organisaties kunnen zijn ondergebracht. Bijvoorbeeld systemen die zijn ondergebracht in gemeenschappelijke regelingen, applicaties die beheerd worden door stelselhouders (BRP, DigiD, Suwi, etc.), systemen van lokale overheidsorganisaties die bij de gemeente in beheer zijn, zoals GGD-en of de systemen van buurgemeenten die soms onder beheer zijn van een grotere gemeente. De vraag is of voldoende duidelijk is voor relevante betrokkenen wie voor welk deel verantwoordelijk is en wie voor het totale landschap.
    b. Er is onduidelijkheid over de verantwoordelijkheden als er risico's in een keten ontstaan. Sommige objecten vormen een relatief groter risico doordat zij een cruciale impact (kunnen) hebben bij ketenverstoring. Keteneffecten overstijgen bovendien snel de grenzen van een gemeente richting andere gemeenten, waterschappen, provincies, etc..
    c. De gemeentelijke organisatie legt met ENSIA ieder jaar verantwoording af aan de gemeenteraad inzake digitale veiligheid. Op basis hiervan kan de gemeenteraad controleren of de digitale veiligheid van de gemeentelijke organisatie op orde is en waar eventueel (extra) aandacht vereist is. De verhouding tussen aandacht voor het primaire proces van gemeenten en toezicht wordt niet als optimaal ervaren en het is bovendien niet duidelijk in hoeverre de gemeenteraad voldoende kennis heeft om controle op dit onderwerp goed uit te voeren, bijvoorbeeld als het gaat om de continuïteit van de (digitale) dienstverlening van de gemeente of de privacy van burgers.
2. Overzicht & inzicht
    a. Gemeenten maken veel gebruik van toeleveranciers van digitale systemen. Deze kunnen een relatief kwetsbare schakel vormen als er leveranciers zijn die diensten leveren aan veel gemeenten. Uit de stakeholdergesprekken komt naar voren dat het overzicht hierover ontbreekt. Er is bijvoorbeeld beperkt overzicht over welke data van gemeenten bij welke partijen is belegd. Welke leveranciers beschikken over data van veel verschillende gemeenten en lopen daarmee extra risico? Is daar bijvoorbeeld extra toezicht op (nodig)? Moeten alle gemeenten ieder afzonderlijk hier de veiligheid testen bij deze leveranciers? Etc. Ook is er geen centraal inzicht in hoe kwetsbaarheden bij veel gebruikte leveranciers verholpen worden. Mogelijk kan de IBD hierbij een rol spelen. Tot slot is onduidelijk of gezamenlijke inkoop van meerdere gemeenten bij dezelfde leveranciers schaalvoordelen kan opleveren die kunnen leiden tot kostenbesparingen.

b. Er bestaan zorgen of de verantwoording over de BIO via ENSIA een goed inzicht geeft in de daadwerkelijke beveiliging van gemeenten. Daarnaast is er een noodzaak tot harmonisering van normenkaders van de andere wetten waar overheidsorganisaties aan moeten voldoen en waarin eisen aan informatieveiligheid zijn opgenomen. Dit biedt ook meteen gelegenheid voor vereenvoudiging.
c. Er wordt voor allerlei doelen data verzameld door gemeenten en er is onvoldoende overzicht over de impact hiervan in relatie tot cyberveiligheid. Is die data bijvoorbeeld voldoende beveiligd? En wie mag er wanneer waarvoor onder welke voorwaarden toegang toe hebben? Mag data verzameld voor het ene doel ook worden ingezet voor een ander doel? Hoe zit het met bewaartermijnen, etc.

3. Standaardisering
   a. ENSIA standaardiseert als het ware het toezicht (1x onderzoeken, meerdere keren verantwoorden). Het is goed om in het oog te houden dat de wijze van verantwoorden in ENSIA de druk van toezicht moeten blijven verminderen. Dat wordt namelijk niet altijd als zodanig ervaren. Hierin moet recente wetgeving, zoals de Cbw blijvend worden meegenomen.
   b. De governancestructuren m.b.t. gemeentelijke besturing werken remmend op het kiezen van gezamenlijke beveiligingsstandaarden. Immers, elke gemeente staat het vrij eigen keuzes te maken voor in te zetten processen en systemen. Vanuit veiligheidsoptiek zijn gemeenten erbij gebaat om processen en systemen juist te standaardiseren en te werken met breed geaccepteerde kaders en standaarden waarin randvoorwaarden ten aanzien van cyberveiligheid zo goed mogelijk (kunnen) worden geborgd.
   c. Agenda Digitale Veiligheid (ADV) en IBD van de VNG hebben de afgelopen jaren veel methodieken en best practices ontwikkeld en beschikbaar gesteld. Veel gemeenten zijn echter nog steeds zoekend naar een goede aanpak en werkwijze en hebben ondersteuning nodig om deze methodieken en best practices in de praktijk te (kunnen) brengen. Capaciteit bij ADV en IBD van de VNG om hierin te ondersteunen is echter beperkt. Meer guidance voor met name kleinere gemeenten met een lage volwassenheid op het gebied van cybersecurity is gewenst.
   d. Er worden best practices op het gebied van digitale veiligheid aangeboden aan gemeenten vanuit het Centrum voor Informatiebeveiliging en Privacy (CIP) en vanuit Agenda Digitale Veiligheid (ADV) van de Vereniging Nederlandse Gemeenten (VNG). Er is behoefte aan consolidatie op dit gebied en één centrale plek waar dit soort best practices ter beschikking worden gesteld aan de afnemers/gebruikers.
   e. De IBD richt zich formeel op *informatie*beveiliging, terwijl de vraag verschuift naar het bredere thema digitale veiligheid. Dat is breder dan alleen informatie en gaat dus ook over uitval van systemen. Het is van belang dat het expliciet duidelijk wordt hoe de IBD zicht tot dit bredere domein verhoudt.

4. Urgentie
    a. Bestuurlijke aandacht en urgentie is nog steeds een punt van zorg. Het koppelen van de uitdagingen rondom digitale veiligheid aan de impact op het primaire proces kan helpen bestuurlijke aandacht te vergroten.
    b. Het onderwerp digitale veiligheid staat door gebrek aan middelen onder druk. Er is al een veelomvattend en complex en kostenintensief takenpakket bij gemeenten en daarmee moet digitale veiligheid concurreren.
    c. Stelselhouders lopen soms achter met beveiligingsmaatregelen. Er is bovendien geen wederkerigheid. Gemeenten verantwoorden zich over de stelsels (DigiD, BRP, SUWI, etc.) maar krijgen geen zicht op de status van de beveiliging van de landelijke voorzieningen terwijl transparantie hierover wel zinvol is om een goede inschatting te kunnen maken van risico's die gemeenten (kunnen) lopen.

Uitdagingen in de warme fase

De belangrijkste uitdagingen in deze fase liggen op vier thema's:

1. Regie
    a. Veiligheidsregio's hebben bij dit onderwerp een minder prominente rol dan in het fysieke domein omdat traditionele partners zoals brandweer en politie minder vaak nodig zijn bij incidentafhandeling. Er zijn (ook) andere partners nodig bij incident- en crisisafhandeling zoals de CISO van een gemeente, sectorale en nationale CSIRT(s), cybersecuritydienstverleners, etc.
    b. Het is onvoldoende duidelijk wie waarvoor in de lead is bij een incident of crisis. Uit de verschillen tussen het fysieke en digitale domein blijkt dat er andere stakeholders betrokken zijn bij de afhandeling bij digitale incidenten. Uit de stakeholdergesprekken ontstaat het beeld dat niet alle gemeenten helder hebben wie zij bij incidenten en crises in het digitale domein moeten betrekken. Er zijn gemeenten die netwerkkaarten hebben gemaakt waarin duidelijk is welke organisatie in welke fase van een incident of crisis welke rol heeft. Dat zijn positieve voorbeelden die ook elders toegepast kunnen worden.
2. Mandaat
    a. Gemeenten hebben in bepaalde situaties onvoldoende mandaat om (vroegtijdig) te interveniëren bij een (dreigend) incident in cyberspace dat zich ook in het fysieke domein kan (gaan) manifesteren. Andere stakeholders hebben soms wel mandaat, maar bijvoorbeeld geen capaciteit of geven er geen of onvoldoende prioriteit aan.
    b. Gemeenten hebben niet dezelfde rol als een sectoraal CSIRT en daarom niet dezelfde informatie nodig, maar hebben soms wel een taak om de bevolking te informeren, als een incident de openbare orde en veiligheid raakt. Ze hebben hiervoor tijdig informatie nodig over de (mogelijke) impact van incidenten op de openbare orde en veiligheid en niet zozeer technische informatie over het incident zelf.

3. Structuur
    a. Er is behoefte aan fallbackscenario's die kunnen worden ingezet bij een cyberincident of -crisis in deze categorie. Denk bijvoorbeeld aan tijdelijke analoge oplossingen, of oplossingen waarbij een deel van de systemen wel blijft functioneren als andere delen (kunnen) uitvallen.
    b. Er is behoefte aan structureel ingerichte netwerken die in geval van incidenten snel verbindingen kunnen maken, bijvoorbeeld een CISO-netwerk met CISO's van gemeenten en andere lokale publieke organisaties binnen een bepaalde regio, of netwerken waarin medewerkers in het OOV en CISO-domein snel met elkaar kunnen schakelen als een incident ook de openbare orde en veiligheid raakt.
    c. Veiligheidsregio's hebben geen formele rol bij dit type incident (wel bij maatschappelijk ontwrichting, zie categorie B). Ze kunnen echter wel ad hoc hulp bieden in de warme fase, bijvoorbeeld bij het informeren van burgers of ondersteuning bieden bij crisiscoördinatie. Deze inzet hangt samen met de volwassenheid en expertise van de betreffende gemeente met het incident.
4. Expertise & Capaciteit
    a. Het Landelijk Crisisplan Digitaal (LCP-D) beschrijft landelijke crisisopschaling. Het is geen vervanging voor lokale planvorming. Wat nodig is, is om ook op lokaal niveau een incident- en crisisplan te maken. Het gaat hierbij om interne crisisplannen voor gemeenten. Uit de stakeholdergesprekken is het beeld ontstaan dat deze op veel plaatsen nog niet aanwezig zijn. Er bestaat wel een handreiking voor vanuit de VNG. Beleidsmatig kan het helpen om duidelijk te maken welke plannen welk doel dienen en hoe ze zich tot elkaar verhouden.

INFORMATIEBEHOEFTE

Tot slot is de belangrijkste informatiebehoefte van gemeenten op een rij gezet voor iedere fase van de veiligheidsketen. Deze liggen voor de interne digitale veiligheid van gemeenten op gebied van proactie, preventie, preparatie, respons en nazorg.

Over het algemeen valt op dat de informatiebehoefte van gemeenten samenhangt met de eigen capaciteiten, maar ook met de complexiteit van het partner- en leveranciersnetwerk van een gemeente.

Proactie:

1. Gemeenten zouden graag meer zicht krijgen op de afhankelijkheden die (kunnen) ontstaan doordat infrastructuur van gemeenten via netwerken gekoppeld is aan infrastructuur van partners en leveranciers.
2. Er is behoefte aan meer zicht op hoe vanuit gemeenten regie kan worden gevoerd op het delen van dreigingsinformatie met leveranciers en partners. Ook zoeken gemeenten naar kaders over hoe om te gaan met wat wanneer wel en wat niet met partners en leveranciers kan worden gedeeld.

Preventie:

1. Er is behoefte aan geanalyseerde informatie om een zorgvuldig afgewogen inschatting van risico's te kunnen maken en keuzes voor te nemen maatregelen mee te onderbouwen. Denk aan incidentanalyses, fenomeenanalyses, dreigingsbeelden, handelingsperspectieven, etc.

Preparatie:

1. Er is behoefte aan ruwe gegevens om mogelijke incidenten mee te kunnen detecteren in zowel het IT- als het OT-domein (bijv. kwetsbaarheden, IOC's, etc.) voor gemeenten die zelf aan detectie doen (d.m.v. een Security Operations Center). Mogelijk kan threat intelligence voor de hoger volwassen gemeenten die dit kunnen verwerken gezamenlijk worden ingekocht. Hier kan een rol zijn weggelegd voor de IBD.

Respons:

1. Er is behoefte aan best practices voor gemeenten die nog moeten starten met het inrichten van security monitoring en incident respons. Hierbij is duidelijkheid over de rolverdeling tussen gemeenten en de IBD belangrijk.

Nazorg:

1. Er is behoefte aan best practices voor gemeenten ten aanzien van business continuity management en hoe bedrijfsvoering ten aanzien van essentiële producten en diensten voor burgers en ondernemers weer kan worden opgestart nadat deze al dan niet tijdelijk is gestaakt na een incident.

ONTWRICHTING DOOR EEN DIGITAAL INCIDENT

In dit hoofdstuk wordt het huidige landschap alsook de uitdagingen en informatiebehoefte beschreven vanuit het perspectief van ontwrichting als gevolg van een digitaal incident bij een organisatie binnen de gemeentegrenzen.

BELEID

Voor ontwrichting is er voornamelijk beleid (inclusief handreikingen en best practices) ontwikkeld voor de koude en lauwe fase. Deze worden in onderstaande tabel opgesomd ingedeeld in de fasen van de veiligheidsketen[15]. De nummers verwijzen naar bijlage B.

Proactie	Preventie	Preparatie	Respons	Nazorg
• Focusblad Digitale Veiligheid, gekoppeld aan het Kernbeleid Veiligheid[70] • De Cbw[89] en BIO2[90] • Digitale sessies voor o.a. ambtenaren OOV over digitale veiligheid[9,58] • Toolbox Veilig Inkopen[63] • Bestuurlijke bevoegdheden cyber (NIPV)[52] • Advies over basis:	• Cyberaanvallen door statelijke actoren[64] • Ontwikkelingen rondom herkenbare overheid[19, 20, 21, 22]	• Landelijk Crisisplan Digitaal (LCP-D)[62] • Handreiking (voorbereiding) op digitale ontwrichting voor gemeenten[79] • Scenario-ontwikkeling[65] • Oefenen via ○ Interactieve cyberoefe-ningen[10] ○ Overheids-breed Cyberpro-gramma (bijv. red teaming,	• Handreiking cybergevolg-bestrijding G4 (Berenschot, 2020)[81]	• Best practices en lessons learned[53,54,55]

[15] Dit overzicht is gecreëerd op basis van input uit de gesprekken, mogelijk ontbreken er nog enkele zaken die in een later stadium kunnen worden aangevuld

○ Documentatie van DTC en NCSC over te nemen (basis)maat-regelen ○ Basismaat-regelen voor cybersecurity van IACS (BIACS)[67] ○ Basisbeveili-gingsmaat-regelen Slimme Apparaten (IoT)[68] ○ Security Check Procesauto-matisering[69] ○ Informatie-behoefte G4[30]		webinars, …)[11,25] ○ Isidoor[38,39,78] ○ Cyberoefen-driehoek[80] ○ Cyberscena-rio's voor veiligheids-regio's[84]		

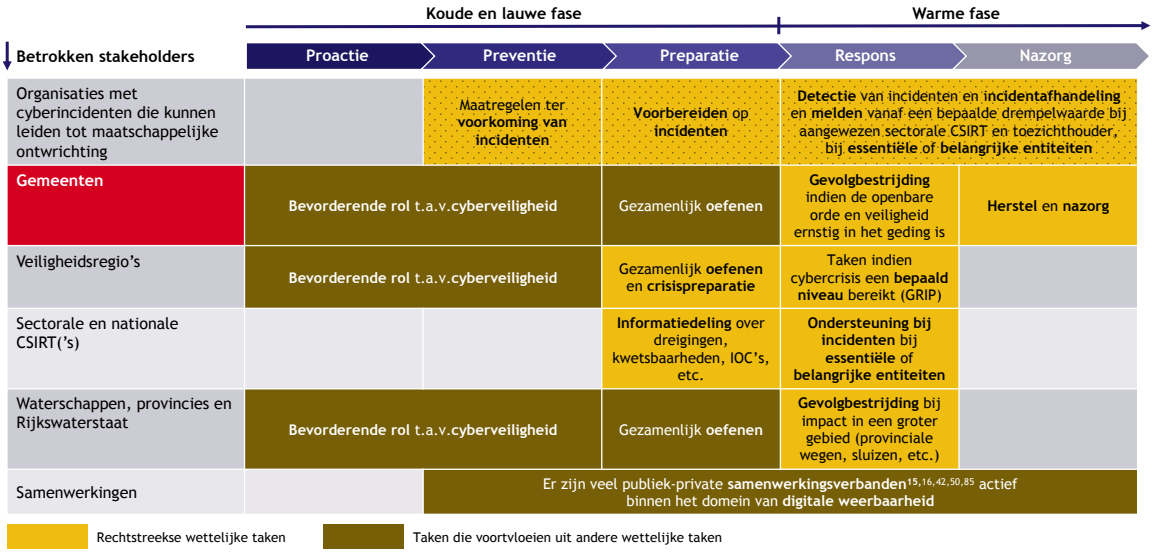
Tabel 7 - Overzicht beleid ontwrichting door een digitaal incident

UITVOERING

Bij een digitaal incident bij een organisatie binnen gemeentegrenzen die gevolgen kan hebben in de fysieke ruimte en kan leiden tot ontwrichting, is de organisatie waar het incident plaatsvindt zelf aan zet van proactie tot en met nazorg. In veel gevallen zijn dit bij (mogelijke) ontwrichting organisaties die in het kader van de Cyberbeveiligingswet als essentieel of belangrijk zijn aangemerkt. Het kan echter ook om andere organisaties gaan met veel maatschappelijke impact op de samenleving, zoals bijvoorbeeld nonprofit-organisaties.

Hoewel gemeenten in de koude en lauwe fase taken uitvoeren, liggen de wettelijke taken die expliciet zijn gedefinieerd juist in de warme fase en zijn deze gericht op incident- en crisisgevolgbestrijding en nazorg als de openbare orde en veiligheid in het geding is. Opvallend genoeg is voor deze fase nog weinig beleid voorhanden (zie vorige sectie en bovenstaande tabel). Naast gemeenten spelen ook veiligheidsregio's bij dit soort incidenten een rol, enerzijds om gezamenlijk te oefenen, maar ook als er een crisis ontstaat met een bepaald opschalingsniveau (GRIP). Sectorale CSIRT's en het nationale CSIRT spelen bij deze categorie eveneens een rol, zowel in de informatievoorziening, als in de ondersteuning van belangrijke en essentiële incidenten ten tijde van een cyberincident. Ook kunnen waterschappen, provincies en Rijkswaterstaat betrokken zijn als gevolgbestrijding in een groter gebied plaats moet vinden die onder hun verantwoordelijkheid valt. Tot slot zijn er op het gebied van ontwrichting veel verschillende samenwerkingen, publiek-privaat, die bijdragen aan het verhogen van de cyberweerbaarheid.

Deze rolverdeling is grafisch weergegeven in onderstaande figuur. De gele blokken verwijzen naar rechtstreekse wettelijke taken en de bruine blokken naar taken die voortvloeien uit meer algemene wettelijke taken.



Figuur 14 - Rollen en taken ontwrichting door een digitaal incident

De bevoegdheden die de verschillende stakeholders hebben rondom ontwrichting komen voort uit meerdere wetten, waaronder in de loop van 2025 ook de Cyberbeveiligingswet. Onderstaande tabel somt deze op waarbij de nummers verwijzen naar bijlage B.

Organisatie	Wettelijk kader
Organisaties met cyberincidenten die kunnen leiden tot maatschappelijke ontwrichting	• Cyberbeveiligingswet o.b.v. NIS2[14] voor essentiële en belangrijke entiteiten (voorlopig nog Wbni o.b.v. NIS voor vitale aanbieders en digitale dienstverleners)
Gemeenten	• Toezicht op evenementen (Art. 174 Gemeentewet)[B.1] • Informatieplicht (Art. 7 Wet Veiligheidsregio's) [B.25] i.v.m. bevolking informeren over (dreigende) gevaren en incidenten en over de maatregelen die de overheid heeft getroffen ter voorkoming en bestrijding of beheersing ervan en over de daarbij te volgen gedragslijn[B2] • Noodbevel (Art. 175 Gemeentewet)[B3] of noodverordening (Art. 176 Gemeentewet)[B4] bij dreigende ontwrichting van de samenleving • Nazorg na een (dreigend) incident (Art. 2.1.3. Wet Veiligheidsregio's)[B.25]
Veiligheidsregio's	• Informatieplicht[B.25] (Art. 7 Wet Veiligheidsregio's) i.v.m. bevolking informeren over (dreigende) gevaren en incidenten[B2] • Noodbevel (Art. 175 Gemeentewet)[B3] of noodverordening (Art. 176 Gemeentewet)[B4] bij dreigende ontwrichting van de samenleving • Bedrijven inspecteren die onder het Besluit risico's zware ongevallen (BRZO) vallen[B.25] (Wet Veiligheidsregio's Art. 31) • Voorbereiden op crisisbeheersing (Art. 10 Wvr)
Sectorale en nationale CSIRT('s)	• Cyberbeveiligingswet o.b.v. NIS2[14] voor essentiële en belangrijke entiteiten

Provincies	• Aanwijzingen geven inzake de crisisbeheersing bij een (Dreigende) ramp of crisis van bovenregionale betekenis[B.25] (Wet Veiligheidsregio's Art. 42)

Tabel 8 - Wettelijke kaders ontwrichting door een digitaal incident

TOEZICHT

Een organisatie die een cyberincident heeft kan te maken krijgen met een toezichthouder in het kader van de Cyberbeveiligingswet, als het een essentiële of belangrijke entiteit betreft. Voor veel organisaties is dit de Rijksinspectie voor de Digitale Infrastructuur (RDI), maar afhankelijk van de sector kan dit ook een sectorspecifieke toezichthouder zijn. De gemeente heeft voor toezicht in deze categorie te maken met de gemeenteraad. Zie hiervoor ook onderstaande figuur. Ook de Autoriteit Persoonsgegevens speelt bij deze typen incidenten mogelijk een rol, namelijk als er sprake is van een datalek veroorzaakt door een cyberincident.

	Koude en lauwe fase			Warme fase	
Toezichthouders	Proactie	Preventie	Preparatie	Respons	Nazorg
Gemeenteraad				• Toezicht op inzet bevoegdheden	
Rijksinspectie voor de Digitale infrastructuur (RDI)	• Samenhangend Inspectiebeeld cybersecurity vitale processen[66]			• Significante incidenten van essentiële en belangrijke entiteiten i.k.v. de nieuwe Cbw moeten worden gemeld aan de betreffende toezichthouder	• De toezichthouder i.k.v. de CBW kan informatie opvragen om te onderzoeken hoe incidenten worden opgevolgd om daar lering uit te trekken
Autoriteit Persoonsgegevens (AP)				• Datalekken veroorzaakt door een cyberincident moeten worden gemeld aan de AP	

Figuur 15 - Toezichthouders[16] bij ontwrichting

UITDAGINGEN BESTURING

Tijdens consultatiegesprekken (zie bijlage A), maar ook uit de bestudeerde documentatie (zie de sectie over beleid) zijn de uitdagingen rondom ontwrichting door een digitaal incident in kaart gebracht. Deze hebben wij gekoppeld aan de acht uitdagingen op gebied van besturing van digitale veiligheid (zie pagina 20). Bij sommige uitdagingen is er een voor de hand liggende eenvoudige oplossingsrichting. Als dat het geval is, wordt die in deze paragraaf beschreven en in bijlage C opgenomen in een lijst met suggesties voor oplossingen.

We merken hierbij op, zoals ook eerder in dit document aangegeven, dat de uitdagingen gebaseerd zijn op behoeften waarvan lastig in te schatten is in hoeverre deze breed wordt herkend en erkend, of deze haalbaar is, realistisch is en wie eventueel aan zet is om aan deze behoefte invulling te geven. In dit document volstaan we voor nu met het omschrijven van de behoefte en het geven van een specifiekere onderbouwing waar mogelijk (met een toelichting van stakeholders die als respondent fungeerden, bestudeerde publicaties en/of onderzochte casuïstiek). Bij de verdere uitwerking van het bestuurlijk convenant zal een nadere uitwerking nodig

[16] De gemeenteraad is formeel gezien geen toezichthouder, maar controleert het college van B&W

zijn, waarbij in kaart wordt gebracht welke concrete casuïstiek ten grondslag ligt aan de gestelde behoeften zodat de achterliggende vraag concreet kan worden gemaakt. Bovendien moet in een nadere uitwerking worden vastgesteld hoe breed die behoefte leeft en hoe realistisch ze is. Ook moeten er prioriteiten worden gesteld voor wat betreft de invulling van de behoeften en moeten er eventueel actiehouders aan worden toegekend. Dit punt nemen we mee in de aanbevelingen in het laatste hoofdstuk van dit document.

Uitdagingen in de koude en lauwe fase

De belangrijkste uitdagingen in deze fase liggen op drie thema's:

1. Verantwoordelijkheid.
    a. Gemeenten verrichten relatief veel activiteiten op gebied van proactie, preventie en preparatie terwijl de wettelijke taken liggen op incidentgevolgbestrijding. Deze focus is met name zinvol als er zich veel organisaties met een hoog risicoprofiel binnen een gemeente bevinden. Gemeenten vragen zichzelf af of ze ook een rol hebben in het weerbaar maken van het MKB voor organisaties die niet onder de Cbw vallen, maar wel lokaal van belang zijn voor het functioneren van een stad of in situaties waarin er meerdere kleine incidenten zijn waarbij er hierdoor veel organisaties en burgers worden geraakt. Een voorbeeld hiervan is de gemeente Haagse Hogeschool die met het initiatief Platform Lokaal Cyberweerbaar Den Haag een cyberweerbaarheidsmeting aanbiedt aan onder meer het MKB om zicht te krijgen op hun mogelijke kwetsbaarheden en hier desgewenst handvatten voor beschikbaar te stellen om de cyberweerbaarheid te bevorderen.
    b. Er bestaan veel verschillende beelden over de rol van veiligheidsregio's bij incidenten in het digitale domein. De veiligheidsregio's zien zichzelf niet als digitale brandweer, terwijl andere ketenpartners daar wel een (mogelijke) rol zien, met name bij (kleinere) gemeenten met relatief weinig capaciteit, kennis en/of expertise in het cyberdomein. Ook kan worden nagedacht over situaties waarin duidelijke triggers tot opschaling ontbreken, maar waarin het wel nodig is om vast na te denken over mogelijk scenario's die om opschaling (kunnen) gaan vragen waarin de veiligheidsregio een rol zou (kunnen) hebben.
    c. Er kan worden onderzocht in hoeverre gemeentelijke bevoegdheden (bijvoorbeeld rondom verstrekking van vergunningen) kunnen helpen bij het voorkomen van incidenten.
2. Overzicht & inzicht.
    a. Inzicht in welke incidenten bij organisaties binnen een gemeente (kunnen) optreden is er op dit moment beperkt, maar helpt bij het bepalen van een regionaal en gemeentelijk risicoprofiel en een goede voorbereiding op incidentgevolgbestrijding. (Beperkte) toegang tot het register met incidenten die gemeld worden i.k.v. de Cyberbeveiligingswet is hierin ondersteunend en

daarom wenselijk. In het register zou bij melding een inschatting moeten worden meegenomen in hoeverre een incident impact kan hebben op de openbare orde en veiligheid zodat gemeenten vroegtijdig voorbereidingen kunnen treffen.

b. Er is behoefte aan meer inzicht in mogelijke lokale cascade- en neveneffecten van aanvallen in het digitale domein.
c. Het is belangrijk om inzicht te bieden in hoe het verloop van incidenten en crises in het fysieke domein anders zijn dan in (de mix met) het digitale domein. Denk bijvoorbeeld aan het breder uitwerken van goede oefenscenario's voor dit soort situaties waarin aan deze aspecten expliciet aandacht wordt besteed.
d. Het helpt als gemeenten en veiligheidsregio's een netwerkanalyse en criteria ontwikkelen ten aanzien van welke partners in welke fase op welke manier betrokken moeten worden bij een digitaal incident. Ook is het goed als zij nadenken over andere aspecten zoals aandachtspunten bij dit soort incidenten, definities die worden gehanteerd, uitleg over welk instanties betrokken moeten worden en welke rol zij dan hebben.

3. Urgentie.
   a. Er bestaan zorgen over hoe de noodzaak voor dit onderwerp beter onder het voetlicht te brengen bij de burgemeester.

Uitdagingen in de warme fase

De belangrijkste uitdagingen in deze fase liggen op vier thema's:

1. Regie
   a. De afbakening met gemeenten, politie en veiligheidsregio's is uitdagend voor wat betreft crisisbeheersing. Het LCP-D geeft deze rollen al deels aan, maar is niet volledig en er wordt niet overal op deze manier in de praktijk invulling aan gegeven.
   b. Voor de beheersing van incidenten en crisis moet in het digitale domein een breed netwerk aan stakeholders betrokken worden en het is in elke regio belangrijk om deze goed in kaart te brengen zodat duidelijk is wie in welke fase betrokken op welke manier moet worden.
2. Mandaat
   a. Het mandaat van verschillende stakeholders is onduidelijk bij incidenten die zich eerst langere tijd in het digitale domein manifesteren voordat ze zichtbaar worden in het fysieke domein: wie heeft wanneer welke rol en bevoegdheden?
   b. Gemeenten hebben niet dezelfde rol als een sectoraal CSIRT en daarom niet dezelfde informatie nodig, maar hebben mogelijk wel een taak om de bevolking te informeren en hebben daarvoor tijdig informatie nodig over de (mogelijke) impact van incidenten op de openbare orde en veiligheid (en niet zozeer technische informatie over het incident zelf).
3. Structuur

a. Bij (dreigende) incidenten en crises met een multi-lokale/multi-regionale/multi-provinciale aard is bredere samenwerking nodig tussen onder andere gemeenten, veiligheidsregio's en politie. Deze behoeft meer structuur zodat er snel geschakeld kan worden tijdens een (dreigend) incident of crisis, denk bijvoorbeeld aan het uitwerken van een netwerkkaart waarin duidelijk is welke partijen betrokken moeten worden of afspraken met deze partijen over hoe deze betrokkenheid kan worden vormgegeven.
b. Belangrijk is om de rol van verschillende stakeholders (gemeenten, politie en veiligheidsregio's) eenduidiger te bepalen zodat dit kan worden meegenomen in de nieuwe versie van het LCP-D die in 2025 wordt herzien.
c. In het fysieke domein is GRIP in gebruik. In de mix met het digitale domein is opschaling complexer en zijn vaak meer partijen betrokken. Het is goed om meer duidelijkheid te bieden voor wat betreft de opschalingsstructuur bij cyberincidenten (bijvoorbeeld in het LCP-D).
d. Incidenten en crises worden primair in de functionele kolom afgehandeld. Voor diverse publieke organisaties (gemeenten, veiligheidsregio's) in de algemene kolom ontstaat er een rol als er impact is op openbare orde en veiligheid. Belangrijk is om inzichtelijk te maken hoe en op welke momenten deze kolommen op elkaar aansluiten, bijvoorbeeld voor wat betreft tijdige informatievoorziening op het overgangsvlak van de functionele naar de algemene kolom (welke informatie is dan nodig, op welk moment en wie kan deze leveren?).

4. Expertise & Capaciteit
   a. Er is behoefte aan meer basiskennis voor burgemeesters over hoe om te gaan met dit type incidenten, maar ook aan meer basiskennis bij crisisteams die veelal nog gericht zijn op incidenten in het fysieke domein.
   b. Naast landelijk en lokaal oefenen zou (multi-)regionaal oefenen kunnen helpen om beter in te spelen op de aard van incidenten in het digitale domein. Dit kan bijvoorbeeld via regionale samenwerkingsverbanden.

INFORMATIEBEHOEFTE

Tot slot is de belangrijkste informatiebehoefte op een rij gezet voor iedere fase van de veiligheidsketen. Deze ligt voor ontwrichting door een digitaal incident op het gebied van preparatie.

In het kader van openbare orde en veiligheid is van belang dat er in de lauwe fase informatievoorziening op gang komt over (mogelijke) impactvolle cyberincidenten.

Preparatie:

1. Er is behoefte aan tijdig inzicht in actuele cyberincidenten binnen gemeentegrenzen met mogelijke impact op de openbare orde en veiligheid (niet zozeer technische informatie over het incident zelf, maar vooral impactinformatie).

2. Er is behoefte aan structurele informatievoorziening op gebied van digitale veiligheid in de lauwe fase (dreigingen, incidenten, etc. zoals bijvoorbeeld VIC Utrecht[17])

[17] https://vru.nl/wij-zijn-de-vru/wat-we-doen/veilige-en-gezonde-leefomgeving/veiligheidsinformatiecentrum/#:~:text=Veiligheidsregio%20Utrecht%20heeft%20sinds%202013,trends%20kunnen%20we%20daarin%20zien%3F

CYBERCRIME & GEDIGITALISEERDE CRIMINALITEIT

In dit hoofdstuk wordt het huidige landschap alsook de uitdagingen en informatiebehoefte beschreven vanuit het perspectief van gedigitaliseerde criminaliteit en cybercrime binnen gemeentegrenzen. Hierbij moet worden opgemerkt dat binnen dit domein de strafrechtketen normaal gesproken wordt gehanteerd om structuur aan te brengen. In dit rapport hebben we ervoor gekozen om de modellering met de veiligheidsketen en eerder geïntroduceerde modellen te hanteren, zodat de incidentcategorieën beter tot elkaar te relateren zijn.

Voor cybercrime hanteren we in dit rapport als definitie criminaliteit waarbij digitale technologie het doelwit is van de criminaliteit, maar ook het middel dat wordt gebruikt om de criminele handelingen mee te verrichten. Voorbeelden zijn ransomware- en DDoS-aanvallen. Onder gedigitaliseerde criminaliteit verstaan we traditionele criminaliteit waarbij digitale technologie wordt ingezet voor de criminele handelingen. Een voorbeeld is vriend-in-nood-fraude of bankhelpdeskfraude.

BELEID

Voor cybercrime en gedigitaliseerde criminaliteit is er voornamelijk beleid (inclusief handreikingen en best practices) ontwikkeld op gebied van proactie en preventie. Deze worden in onderstaande tabel opgesomd ingedeeld in de fasen van de veiligheidsketen[18]. De nummers verwijzen naar bijlage B.

Proactie	Preventie	Preparatie	Respons	Nazorg
• Focusblad Digitale Veiligheid, gekoppeld aan	• Regionale samenwerking (delen van expertise,	• Tools en informatie van het Digital Trust Center (zoals	• Meldknop.nl[76]	• Hulp bij verwerking via helpwanted.nl of

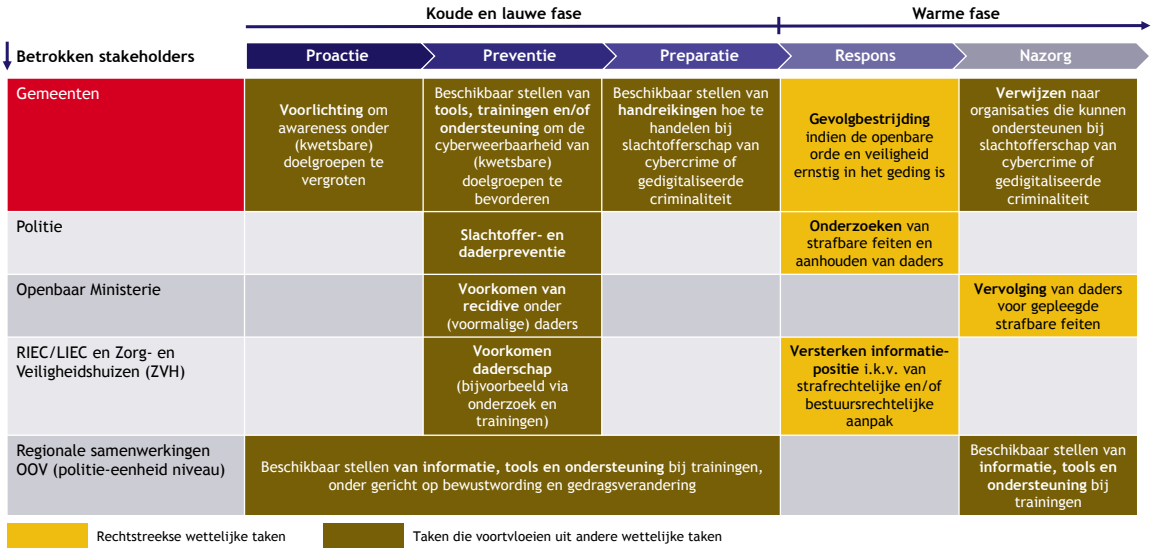
[18] Dit overzicht is gecreëerd op basis van input uit de gesprekken, mogelijk ontbreken er nog enkele zaken die in een later stadium kunnen worden aangevuld

het Kernbeleid Veiligheid[70] • Digitale sessies voor o.a. ambtenaren OOV over digitale veiligheid[9,58] • Veiligheids-agenda 2023-2026[87] • Informatie-behoefte G4[30] • Cybercrime-beeld 2024[88]	trainingen, tools, voorlichting) in Regionaal Expertteam Digitale Veiligheid onder andere i.k.v. City Deal Cybercrime[12,13,43] en in Platforms Veilig Ondernemen[86] • Geldezel en Cyberslachtoffer tools voor inzicht[71,72] • Monitor Online Veiligheid en Criminaliteit[92] • Voorlichtings-campagnes publiek[26,27] • Ontwikkelingen rondom herkenbare overheid[19, 20, 21, 22]	phishing en fraude quiz)[75]		Slachtofferhulp Nederland

Tabel 9 - Overzicht beleid cybercrime en gedigitaliseerde criminaliteit

UITVOERING

Bij cybercrime en gedigitaliseerde criminaliteit zijn als eerste politie en het Openbaar Ministerie aan zet voor hun wettelijke taken ten aanzien van het onderzoeken van strafbare feiten, het aanhouden en vervolgen van de daders. De Regionale Informatie- en Expertisecentra (RIEC's) ondersteund door het Landelijk Informatie- en Expertisecentrum (LIEC) en ook de Zorg- en Veiligheidshuizen (ZVH's) vervullen hier een rol als het gaat om het versterken van de informatiepositie in het kader van een strafrechtelijke én bestuursrechtelijke aanpak van dit soort problematiek. Gemeenten hebben een wettelijke taak bij gevolgbestrijding als de openbare orde en veiligheid in het geding is in de respons-fase. In de overige fasen zien we gemeenten ook actief bij voorlichting, het beschikbaar stellen van tools, trainingen en informatie en het doorverwijzen van slachtoffers naar hulpverlenende instanties.



Figuur 16 - Rollen en taken cybercrime en gedigitaliseerde criminaliteit

Deze rolverdeling is grafisch weergegeven in bovenstaande figuur. De gele blokken verwijzen naar rechtstreekse wettelijke taken en de bruine blokken naar taken die voortvloeien uit meer algemene wettelijke taken.

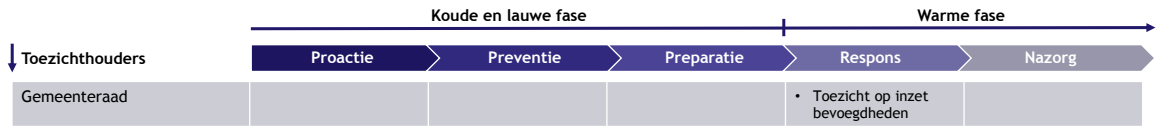
De bevoegdheden die de verschillende stakeholders hebben rondom cybercrime en gedigitaliseerde criminaliteit komen voort uit meerdere wetten. Onderstaande tabel somt deze op waarbij de nummers verwijzen naar bijlage B.

Organisatie	Wettelijk kader
Gemeente	• De gemeente kan voor een wettelijke regeling aansluiting zoeken bij de Gemeentewet (artikel 172). De Gemeentewet schrijft voor dat de burgemeester belast is met de handhaving van de openbare orde. De handhaving van de openbare orde is nader gespecificeerd in de Algemene Plaatselijke Verordening (APV) van de gemeente. [B.22]
Politie	• Wet computercriminaliteit III[B.22] • Wetboek van Strafvordering (WvSv)[B.55]
Openbaar Ministerie	• Wet computercriminaliteit III[B.22] • Wetboek van Strafvordering (WvSv)[B.55]
RIEC/LIEC en Zorg- en Veiligheidshuizen (ZVH)	• Wet gegevensverwerking door samenwerkingsverbanden[B.54] (Paragraaf 2.3 WGS Regionale Informatie- en Expertise Centra en Paragraaf 2.4 WGS Zorg- en Veiligheidshuizen)

Tabel 10 - Wettelijke kaders cybercrime en gedigitaliseerde criminaliteit

TOEZICHT

Voor wat betreft de wettelijke taken van de gemeente in het kader van cybercrime en gedigitaliseerde criminaliteit, namelijk gevolgbestrijding vindt toezicht plaats vanuit de gemeenteraad. Zie onderstaande figuur.



Figuur 17 - Toezichthouders[19] cybercrime en gedigitaliseerde criminaliteit

UITDAGINGEN BESTURING

Tijdens consultatiegesprekken (zie bijlage A), maar ook uit de bestudeerde documentatie (zie de sectie over beleid) zijn de uitdagingen rondom cybercrime en gedigitaliseerde criminaliteit in kaart gebracht. Deze hebben wij gekoppeld aan de acht uitdagingen op gebied van besturing van digitale veiligheid (zie pagina 20). Bij sommige uitdagingen is er een voor de hand liggende eenvoudige oplossingsrichting. Als dat het geval is, wordt die in deze paragraaf beschreven en in bijlage C opgenomen in een lijst met suggesties voor oplossingen.

We merken hierbij op, zoals ook eerder in dit document aangegeven, dat de uitdagingen gebaseerd zijn op behoeften waarvan lastig in te schatten is in hoeverre deze breed wordt herkend en erkend, of deze haalbaar is, realistisch is en wie eventueel aan zet is om aan deze behoefte invulling te geven. In dit document volstaan we voor nu met het omschrijven van de behoefte en het geven van een specifiekere onderbouwing waar mogelijk (met een toelichting van stakeholders die als respondent fungeerden, bestudeerde publicaties en/of onderzochte casuïstiek). Bij de verdere uitwerking van het bestuurlijk convenant zal een nadere uitwerking nodig zijn, waarbij in kaart wordt gebracht welke concrete casuïstiek ten grondslag ligt aan de gestelde behoeften zodat de achterliggende vraag concreet kan worden gemaakt. Bovendien moet in een nadere uitwerking worden vastgesteld hoe breed die behoefte leeft en hoe realistisch ze is. Ook moeten er prioriteiten worden gesteld voor wat betreft de invulling van de behoeften en moeten er eventueel actiehouders aan worden toegekend. Dit punt nemen we mee in de aanbevelingen in het laatste hoofdstuk van dit document.

Uitdagingen in de koude en lauwe fase

De belangrijkste uitdagingen in deze fase liggen op vier thema's:

1. Verantwoordelijkheid
    a. Gemeenten kunnen met preventie (samen met lokale, regionale partners waaronder het Platform Veilig Ondernemen - PVO) en sectorale partners waaronder cyberweerbaarheidscentra (zoals Cyberweerbaarheidscentrum Brainport – CWB, Cyberweerbaarheidscentrum Greenport – CWG, Cyberweerbaarheidscentrum Maakindustrie Zuid-Holland - CWM en FERM) een rol spelen om de kans op en/of impact van cybercrime en gedigitaliseerde criminaliteit te reduceren. Hiermee kan zowel (herhaald) slachtoffer- als daderschap worden voorkomen. Rechtstreekse wettelijke

[19] De gemeenteraad is formeel gezien geen toezichthouder, maar controleert het college van B&W

taken op dit terrein liggen bij de politie en het openbaar ministerie, maar de politie komt in de praktijk relatief vaak niet toe aan deze taak. Gemeenten en politie kunnen elkaar op dit onderwerp ook juist versterken, omdat zij ieder een andere informatiepositie hebben. De Citydeal zet juist in op deze samenwerking. Gemeenten zetten al actief in op preventie, bijvoorbeeld op gebied van jeugdcybercrime, samen met lokale partners.

b. Nazorg is een taak die primair bij gemeenten ligt en nader kan worden ingevuld. Er zijn al voorbeelden van projecten tussen gemeenten, politie en OM, waarbij ook Slachtofferhulp Nederland is betrokken. Aandachtspunt is dat, net als bij traditionele criminaliteit, slachtoffers bij een aangifte moeten aangeven of er behoefte is aan slachtofferhulp en de aangiftebereidheid bij digitale criminaliteit is op dit moment laag is.
c. Gemeenten zouden dit thema integraal moeten oppakken (OOV bijvoorbeeld regisseren, maar samen met andere beleidsthema's uitvoeren, bijvoorbeeld economische zaken (EZ) voor ondernemers, maatschappelijke ontwikkeling (MO) voor kwetsbare burgers, het onderwijs en het sociaal domein voor preventieactiviteiten richting kinderen en jongeren, etc.). Hiervoor is recent in samenwerking met het CCV een praatplaat voor gemeenten ontwikkeld, waarin onderwijs, sociaal domein, jeugd, ondermijning, economische zaken aan bod komen[20].
d. Provincies kiezen soms ook voor een rol op preventie (bijvoorbeeld vanuit digitale economiebevordering). Er ontstaat zo een versnipperd landschap, terwijl er schaarse capaciteit is. Consolidatie is hier voor de hand liggend.
e. Belangrijk vraagstuk (net als bij online aangejaagde openbare-ordeverstoringen) is het online onderzoeken van activiteiten in het digitale domein. De politie heeft hier bevoegdheden, maar dan moet er al snel worden opgeschaald. Hierbij geldt ook dat de politie pas kan/mag opschalen naar een gemeente als er sprake is van een strafbaar feit. Om eerder een situatie te kunnen ombuigen of de-escaleren, is het nodig om gemeenten daarvoor in positie te brengen. De vraag is daarbij hoe op een andere manier (dus zonder structureel monitoren) signalen kunnen worden opgepikt die duiden op gedigitaliseerde criminaliteit of cybercrime. Mogelijkheden hiervoor zijn vaak niet duidelijk en worden daarmee onvoldoende benut[21]. Dit past bij de nationale insteek om geen nieuwe bevoegdheden te ontwikkelen, maar beter gebruik te maken van het bestaande instrumentarium. Gemeenten hebben hier soms onvoldoende kennis over, maar er is evenmin een eenduidig beeld of de burgemeester dit soort activiteiten tot zijn taken ziet. Wel zien we voorbeelden waarbij lokale partners soms geanonimiseerde informatie delen over trends en er zijn voorbeelden waarbij online

[20] https://hetccv.nl/ccv-cyberpraatplaat-voor-integrale-aanpak-gemeenten/
[21] Zie voor mogelijkheden bijvoorbeeld het rapport 'Burgemeesters in cyberspace' uit 2018 van W. Bantema et al. https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2018/burgemeesters-in-cyberspace-313/

jongerenwerkers signalen oppikken waarmee verder aan de slag kan worden gegaan.

f. Een openstaande vraag is hoe verschillende stakeholders in dit landschap zich tot elkaar verhouden. Denk daarbij ook aan bijvoorbeeld het ministerie van Justitie en Veiligheid, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Slachtofferhulp Nederland, de Fraudehelpdesk, CCV, maar ook privaat, zoals banken en verzekeraars. Het zou interessant zijn om een bredere stakeholderkaart te maken waarin de onderlinge verbinding van deze stakeholders met elkaar en met gemeenten duidelijker wordt ook in relatie tot de verschillende doelgroepen (zoals MKB, jeugd, etc.). Vanuit het Actieprogramma Veilig Ondernemen wordt al gewerkt aan een kaart met stakeholders. Wel leert de ervaring dat zo'n kaart snel complex kan worden en gedateerd kan raken. Toch is er behoefte aan meer duidelijkheid over wie wat doet.

2. Overzicht & inzicht
   a. Uit de gesprekken kwam naar boven dat er behoefte is aan meer algemeen overzicht in de problematiek. Tegelijkertijd bereikt ons het signaal dat er ook al allerlei analyses beschikbaar zijn (zoals de Cybercrime Pathways Onderzoeksagenda, de Veiligheidsagenda, de monitor Online Veiligheid en Criminaliteit, het Cybercrimebeeld Nederland, etc. Het behoeft nader onderzoek of er inderdaad gebrek is aan overzicht en inzicht of dat de inzichten en overzichten de doelgroep onvoldoende bereiken. Uit de gesprekken kwam de volgende behoeftestelling naar voren:
      - Een duidelijke definitie van de problematiek om te voorkomen dat alle vormen van criminaliteit onder dit thema worden geschoven.
      - Meer inzicht in digitale delicten (waar, door wie, gevolgen) om daarmee te onderzoeken wat mogelijke passende interventies zijn.
      - Inzicht in 'massaal slachtofferschap': als dezelfde daders veel verschillende slachtoffers maken. Dit heeft onder andere te maken met meldingsbereidheid dan slachtoffers die soms beperkt is, maar ook met prioritering van onderzoek. Als er meer zicht komt op de aard en omvang is ook preventie beter mogelijk.
      - Meer fenomeenanalyses, bijvoorbeeld vanuit de RIEC's. Hierbij moet worden opgemerkt dat de kerntaak van RIEC's op dit moment ondermijnende criminaliteit is en dat dit een uitbreiding van taken zou betreffen waarover zou moeten worden besloten.
      - Overzicht van lokaal en regionaal ontwikkelde best practices die breder (bijvoorbeeld landelijk) kunnen worden overgenomen.
      - De RIEC's en de ZVH's kunnen nog beter worden benut voor het draaien van casuïstiek en specifiek de RIEC's voor het maken van criminaliteitsbeelden voor gemeenten waarin cybercrime en gedigitaliseerde criminaliteit in georganiseerd verband worden meegenomen.
   b. Er is behoefte aan overzicht over en inzicht in de effectiviteit van de aanpak:

- Een rijksbreed overzicht van welke stakeholders waaraan werken in relatie tot dit type incidenten zodat relevante stakeholders elkaar en beschikbare informatie beter weten te vinden.
- Een wetenschappelijke onderbouwing van de huidige aanpak van cybercrime en gedigitaliseerde criminaliteit.
- Een overzicht van beproefde interventies. Vanuit de City Deal Lokale Weerbaarheid Cybercrime[22] wordt al gewerkt aan het borgen van succesvolle interventies, bijvoorbeeld bij landelijke partners.

c. Overzicht van wat er speelt binnen een gemeente zou vaker integraal moeten worden besproken (gemeente, politie, OM, RIEC, etc.). Evaluatie van bij gemeenten uitgeprobeerde integrale aanpakken kan helpen om breder tot een effectieve aanpak te komen. Daarbij kunnen ook andere beleidsterreinen worden betrokken om verbanden te vinden (zoals bijvoorbeeld schuldsanering in relatie tot geldezels of katvangers).

d. Er zijn kansen om dit onderwerp te verbinden aan de aanpak voor ondermijnende criminaliteit (bijvoorbeeld aan het programma Preventie met Gezag). Gemeenten investeren in projecten om jonge aanwas (bijvoorbeeld criminele uitbuiting) te voorkomen. Deze projecten richten zich veelal op het voorkomen dat jongeren in de drugscriminaliteit komen en/of hier niet meer uit kunnen komen. Er is hierbij nog onvoldoende aandacht voor jongeren die zich inlaten met cybercrime en/of gedigitaliseerde criminaliteit[23].

3. Standaardisering
   a. Inzicht in volwassenheid ten aanzien van de aanpak van dit thema. Er wordt binnen de VNG gewerkt aan de totstandkoming van een visitatiecommissie die gemeenten bevraagt en kwalificeert op basis van hun volwassenheidsniveau ten aanzien van onder meer de aanpak van cybercrime en gedigitaliseerde criminaliteit.
4. Urgentie
   a. Gemeenten hebben moeite om lokaal te kiezen voor inzet op cyberproblematiek omdat de impact van online slachtofferschap onvoldoende helder is (beperkte beleving van schade). Er is echter onderzoek gedaan waaruit blijkt dat impact van online slachtofferschap groot kan zijn. Nazorg is hierin ook van belang: slachtoffers ondersteunen bij mogelijke identiteitsfraude en hen helpen zich beter te beschermen om de kans op herhaald slachtofferschap te reduceren.
   b. In de driehoek zouden vaker gesprekken moeten plaatsvinden over prioriteiten bij vervolgen waarbij expliciete keuzes worden gemaakt voor prioriteiten. Nu is er soms door nieuwe ontwikkelingen sneller aandacht voor zaken die urgent lijken, bijvoorbeeld het betrappen op heterdaad als gevolg

[22] N.B. CityDeal en de bijbehorende middelen stopt na 2026
[23] Het CCV heeft een inventarisatie verricht naar interventies op het gebied van jeugd en cybercrime - https://hetccv.nl/app/uploads/2023/12/Interventies-op-het-gebied-van-Jeugd-en-Cybercrime-DEF-20231212.pdf

van introductie van zelfscankassa's, maar kan dit ten koste gaan aandacht voor gedigitaliseerde criminaliteit.

Uitdagingen in de warme fase

De belangrijkste uitdagingen in deze fase liggen op drie thema's:

1. Mandaat
    a. Er is binnen gemeenten behoefte aan meer inzicht over bevoegdheden die in dit domein kunnen worden ingezet (bijvoorbeeld om datacentra aan te pakken, wat lastig is omdat onduidelijk is wie eigenaar is van bepaalde servers, of bijvoorbeeld als in een bedrijfspand een callcenter is ingericht voor helpdeskfraude en waarbij een inval wapens en drugs worden gevonden). Kan bijvoorbeeld ondermijningswetgeving hierin helpen? Wat kan er eventueel bestuursrechtelijk?
2. Structuur
    a. Digitale meldkamers zorgen ervoor dat slachtoffers van online criminaliteit sneller politiefunctionarissen op bezoek krijgen om een aangifte af te nemen en/of om sporen veilig te stellen. Het doel van de politie is om relevante informatie voor verder onderzoek te vergaren en daarmee de kans te vergroten om daders van online criminaliteit op te sporen. Voorheen moesten slachtoffers van online criminaliteit veelal online aangifte doen of voor een afspraak naar het politiebureau komen. Mogelijk kan de inzet van meer digitale meldkamers helpend zijn. Dit is al getest in Midden- en Oost-Nederland en wordt landelijk geïmplementeerd[24].
3. Expertise & Capaciteit.
    a. Het kan helpen om in een ambtelijke en/of bestuurlijke subdriehoek specifiek deze problematiek te bespreken zodat gezamenlijk gewerkt kan worden aan goede interventies.
    b. Capaciteitsgebrek is een grote uitdaging op dit dossier. Een suggestie is om digitaal veiligheidsbeleid te verweven in bestaande taken van organisaties/organisatieonderdelen die zich op gebied van traditionele criminaliteit er al mee bezig houden.
    c. Er is behoefte om een netwerkdag voor ketenpartners te organiseren op dit thema om van elkaar te leren en de community bij elkaar te brengen. Ieder doet dit nu voor zichzelf voor een deel van de keten. Zo wordt ook beter duidelijk hoe het totale speelveld in elkaar zit.
    d. Er is zorg of er voldoende kennis is bij gemeenteambtenaren over dit thema (bevoegdheden, mogelijke interventies, etc.). Het CCV heeft bijvoorbeeld een webdossier ingericht waar medewerkers van onder meer gemeenten

[24] https://www.politie.nl/nieuws/2024/februari/2/02-oost-nederland-slachtoffers-sneller-geholpen-bij-digitale-criminaliteit.html en https://www.politie.nl/nieuws/2025/mei/19/politie-komt-ook-langs-bij-digitale-criminaliteit.html

informatie kunnen vinden over best practices & lessons learned ten aanzien van (de aanpak van) cybercrime en gedigitaliseerde criminaliteit[25].

INFORMATIEBEHOEFTE

Tot slot is de belangrijkste informatiebehoefte op een rij gezet voor iedere fase van de veiligheidsketen. Deze ligt voor cybercrime en digitaliseerde criminaliteit op het gebied van proactie en preventie.

Proactie:

1. Er is behoefte aan inzicht in (herhaald) slachtofferschap om daarmee te komen tot betere interventies. Om meer zicht te verkrijgen op de aard, omvang, verschijningsvormen, modus operandi van daders en slachtofferkenmerken moet de aangiftebereidheid worden bevorderd. Er is al een verkenning uitgevoerd naar een mogelijk op te richten schadefonds voor online slachtofferschap. Deze zou als mogelijk bijeffect kunnen leiden tot een grotere aangiftebereidheid.

Preventie:

1. Er is behoefte aan meer gestructureerde data (aangiften) en aan meer analyses van slachtofferkenmerken, generieke daderkenmerken en modus operandi. Er zijn op dit gebied al diverse lopende initiatieven voor informatievoorziening, zoals de monitor Zicht op Ondermijning (www.zichtopondermijning.nl), de Veiligheidsmonitor (www.veiligheidsmonitor.nl), het dashboard Waar staat je gemeente (www.waarstaatjegemeente.nl), de monitor Jeugdcriminaliteit (www.wodc.nl/onderwerpen/monitor-jeugdcriminaliteit) en het dashboard Criminaliteit en Recht (www.criminaliteit-en-recht.nl) waar informatie (per gemeente) is te vinden over daders en/of slachtoffers van cybercrime en gedigitaliseerde criminaliteit. Echter zijn deze initiatieven (nog) onvoldoende bekend bij gemeenten en/of is ondersteuning verreist hoe deze te gebruiken in de praktijk. Er wordt door het CCV momenteel gewerkt aan een handreiking voor gemeenten hoe zij deze (en andere) monitors kunnen gebruiken bij informatie gestuurd werken bij de aanpak van criminaliteit (waaronder cybercrime en gedigitaliseerde criminaliteit).

[25] https://hetccv.nl/themas/cyberveiligheid/cybercrime/#:~:text=Cybercrime%20verdient%20een%20integrale%20aanpak,van%20haar%20inwoners%20en%20bedrijven .

ONLINE AANGEJAAGDE OPENBARE-ORDEVERSTORINGEN

In dit hoofdstuk wordt het huidige landschap alsook de uitdagingen en informatiebehoefte beschreven vanuit het perspectief van online aangejaagde openbare-ordeverstoringen die impact hebben binnen gemeentegrenzen.

BELEID

Voor online aangejaagde openbare-ordeverstoringen is er voornamelijk beleid (inclusief handreikingen en best practices) ontwikkeld voor de koude en lauwe fase. Deze worden in onderstaande tabel opgesomd ingedeeld in de fasen van de veiligheidsketen[26]. De nummers verwijzen naar bijlage B.

Proactie	Preventie	Preparatie	Respons	Nazorg
• Handreiking voor gemeenten voor online onderzoek bij het handhaven van de openbare orde[37] • Focusblad Digitale Veiligheid, gekoppeld aan het Kernbeleid Veiligheid[70] • Digitale sessies voor o.a. ambtenaren OOV over digitale veiligheid[9,58] • Analyse wetgeving en	• Fenomenen-kaart[74] • Digitale barrièremodel voor online aangejaagde openbare-ordeversto-ringen[72] • Regionale samenwerking (delen van expertise) in Regionaal Expertteam Digitale Veiligheid i.k.v. City Deal Cybercrime[12,13] • Handelings-perspectief bij	• Digitale barrièremodel voor online aangejaagde openbare-ordeversto-ringen[72] • Interventiekaart aanpak online aangejaagde openbare-ordeversto-ringen[77] • Protocol online onderzoek[91] • Analyse wetgeving en jurisprudentie online aangejaagde openbare	• Digitale barrièremodel voor online aangejaagde openbare-ordeversto-ringen[72] • Analyse wetgeving en jurisprudentie online aangejaagde openbare ordeversto-ringen[4]	• Digitale barrièremodel voor online aangejaagde openbare-ordeversto-ringen[72]

[26] Dit overzicht is gecreëerd op basis van input uit de gesprekken, mogelijk ontbreken er nog enkele zaken die in een later stadium kunnen worden aangevuld

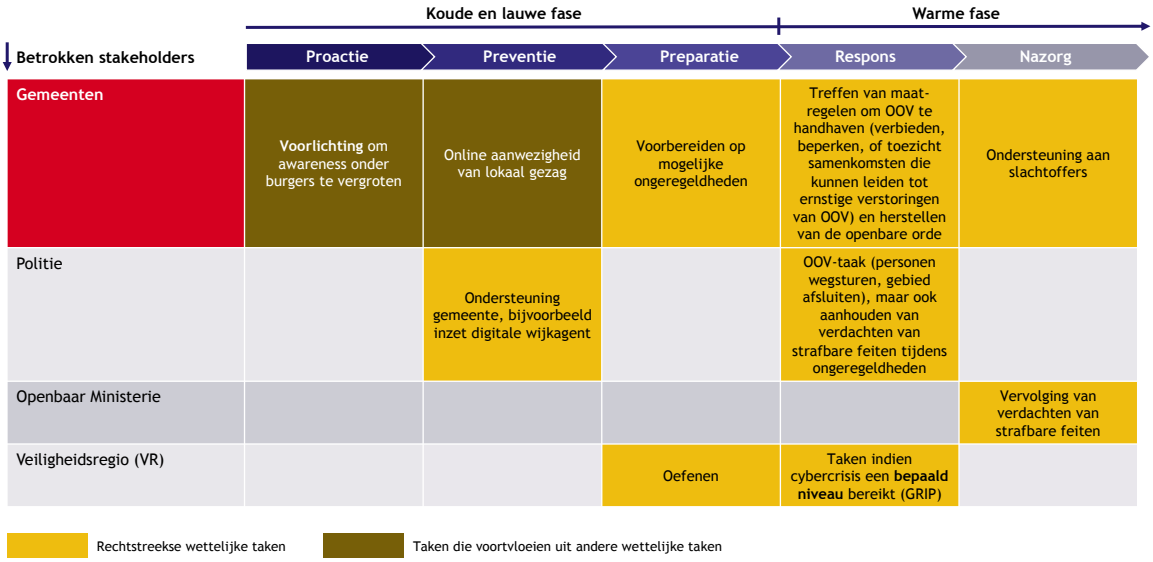
jurisprudentie online aangejaagde openbare ordeversto-ringen[4] • Informatie-behoefte G4[30]	online aangejaagde openbare-ordeversto-ringen[73] • Analyse wetgeving en jurisprudentie online aangejaagde openbare ordeversto-ringen[4]	ordeversto-ringen[4]		

Tabel 11 - Overzicht beleid online aangejaagde openbare-ordeverstoringen

UITVOERING

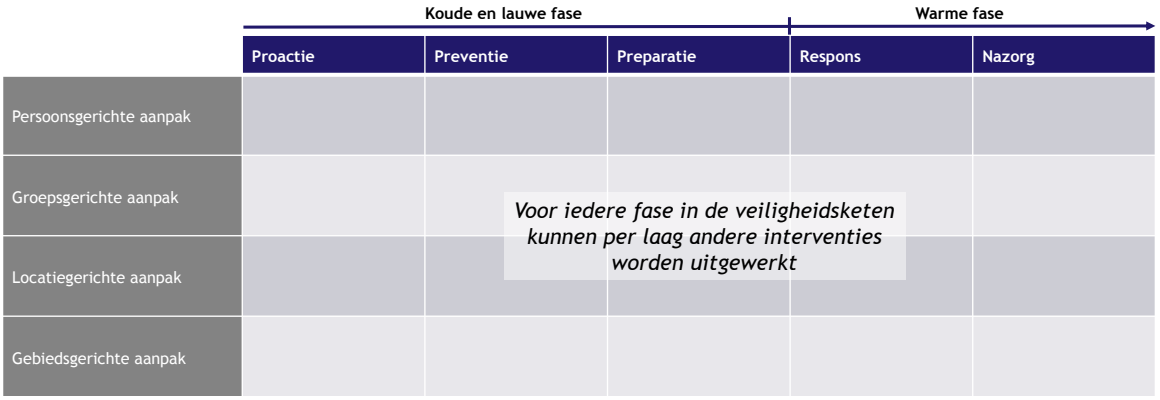
Bij online aangejaagde openbare-ordeverstoringen is er inmiddels een goed beeld van de mogelijke inzet van bevoegdheden voor gemeenten, politie, Openbaar Ministerie en veiligheidsregio's. Wel valt op dat de bevoegdheden van gemeenten zich concentreren rondom de periode dat een incident zich manifesteert in het fysieke domein. Er zijn echter voor gemeenten weinig mogelijkheden tot het onderzoeken van wat er in het online domein gebeurt waardoor gemeenten kunnen worden verrast door een incident (wanneer het zich plotseling fysiek manifesteert).

De politie kan de gemeente hierbij ondersteunen. Bijvoorbeeld door de inzet van de digitale wijkagent. Deze functionaris volgt wat burgers bezighoudt op social media, in de lokale en regionale online media en op fora. Op deze manier kan de digitale wijkagent monitoren op signalen van een (mogelijke) online aangejaagde openbare-ordeverstoring. De rolverdeling is grafisch weergegeven in onderstaande figuur. De gele blokken verwijzen naar rechtstreekse wettelijke taken en de bruine blokken naar taken die voortvloeien uit meer algemene wettelijke taken.



Figuur 18 - Rollen en taken online aangejaagde openbare-ordeverstoringen

Gemeenten kunnen bij online aangejaagde openbare-ordeverstoringen gelaagd werken door zich specifiek te richten op een persoon, groep, locatie en/of gebied. Onderstaande figuur geeft dit weer.



Figuur 19 - Gelaagd werken bij online aangejaagde openbare-ordeverstoringen

De bevoegdheden die de verschillende stakeholders hebben rondom online aangejaagde openbare-ordeverstoringen komen voort uit meerdere wetten. Onderstaande tabel somt deze op waarbij de nummers verwijzen naar bijlage B.

Organisatie	Wettelijk kader
Gemeente	• Algemene bevoegdheid ter handhaving openbare orde (Artikel 172 Gemeentewet)[B.5] • Openbare ordebevoegdheden (Artikel 172 Gemeentewet)[B.6] • Bestrijding voetbalvandalisme en ernstige overlast (meldplicht, groepsverbod, gebiedsverbod) (Artikel 172a Gemeentewet)[B.7] • Bestuurlijke ophouding (Artikel 154 Gemeentewet en Artikel 176 Gemeentewet)[B.8] • Cameratoezicht om de openbare orde te handhaven (Gemeentewet 151)[B.10] • Informatie uitwisseling voor de handhaving van de openbare orde (Wet Politiegegevens en Wet justitiële en strafvorderlijke gegevens)[B.11] • Noodbevoegdheden ter handhaving van de openbare orde of ter beperking van gevaar (Artikel 175 Gemeentewet en Artikel 176 Gemeentewet)[B.12] • Beperkende bevoegdheden en verplichtingen bij een samenkomst op een openbare plaats (Wet Openbare manifestaties)[B.13] • Preventief fouilleren voor de handhaving van de openbare orde (Artikel 151 Gemeentewet)[B.14] • Toezicht op openbare samenkomsten (Artikel 174 Gemeentewet)[B.15] • Preventieve last onder dwangsom (Artikel 125 Gemeentewet)[B.16] • Last onder dwangsom (Artikel 125 Gemeentewet)[B.17] • Algemene Plaatselijke Verordening (APV)[B.22] om personen ervan te weerhouden online uitingen te doen die een gevaar vormen voor de openbare orde.

	• Verbod op onrechtmatige uitingen gericht op openbare-ordeverstoring (art. 6:162 BW)[B.23]
Openbaar Ministerie	• Bevel tot ontoegankelijk maken van gegevens (Art. 125p Sv)[B.56] • Vervolging en veroordeling wegens opruiing (Art. 131 Sr)[B.57] • Vervolging en veroordeling wegens verspreiding van opruiend materiaal (Art. 132 Sr)[B.58] • Vervolging en veroordeling wegens voorbereiding van openlijke geweldpleging (Art. 141a Sr)[B.59] • Vervolging en veroordeling wegens Smaad (Art. 261 Sr)[B.60] • Vervolging en veroordeling wegens Laster (Art. 262 Sr)[B.61] • Gedragsaanwijzing aan verdachte die de openbare orde ernstig heeft verstoord en waarbij grote vrees voor herhaling bestaat (art. 509hh lid 1 Sv)[B.62] • Gedragsaanwijzing (Artikel 509 Wetboek van Strafvordering)[B.21]
Veiligheidsregio (VR)	• Oefenen ter voorbereiding op openbare orde verstoringen[B.25] (Artikel 10 Wet Veiligheidsregio's) • Nazorg na een (dreigend) incident Wet Veiligheidsregio's[B.25] (Artikel 2.1.3. Wet Veiligheidsregio's)

Tabel 12 - Wettelijke kaders online aangejaagde openbare-ordeverstoringen

TOEZICHT

Bij online aangejaagde openbare-ordeverstoringen zien de gemeenteraad en de rechtspraak toe op de inzet van bevoegdheden. Zie onderstaande figuur.

Figuur 20 – Toezichthouders[27] online aangejaagde openbare-ordeverstoringen

UITDAGINGEN BESTURING

Tijdens consultatiegesprekken (zie bijlage A), maar ook uit de bestudeerde documentatie (zie de sectie over beleid) zijn de uitdagingen rondom online aangejaagde openbare-ordeverstoringen in kaart gebracht. Deze hebben wij gekoppeld aan de acht uitdagingen op gebied van besturing van digitale veiligheid (zie pagina 20). Bij sommige uitdagingen is er een voor de hand liggende eenvoudige oplossingsrichting. Als dat het geval is, wordt die in deze paragraaf beschreven en in bijlage C opgenomen in een lijst met suggesties voor oplossingen.

We merken hierbij op, zoals ook eerder in dit document aangegeven, dat de uitdagingen gebaseerd zijn op behoeften waarvan lastig in te schatten is in hoeverre

[27] De gemeenteraad is formeel gezien geen toezichthouder, maar controleert het college van B&W

deze breed wordt herkend en erkend, of deze haalbaar is, realistisch is en wie eventueel aan zet is om aan deze behoefte invulling te geven. In dit document volstaan we voor nu met het omschrijven van de behoefte en het geven van een specifiekere onderbouwing waar mogelijk (met een toelichting van stakeholders die als respondent fungeerden, bestudeerde publicaties en/of onderzochte casuïstiek). Bij de verdere uitwerking van het bestuurlijk convenant zal een nadere uitwerking nodig zijn, waarbij in kaart wordt gebracht welke concrete casuïstiek ten grondslag ligt aan de gestelde behoeften zodat de achterliggende vraag concreet kan worden gemaakt. Bovendien moet in een nadere uitwerking worden vastgesteld hoe breed die behoefte leeft en hoe realistisch ze is. Ook moeten er prioriteiten worden gesteld voor wat betreft de invulling van de behoeften en moeten er eventueel actiehouders aan worden toegekend. Dit punt nemen we mee in de aanbevelingen in het laatste hoofdstuk van dit document.

Uitdagingen in de koude en lauwe fase

De belangrijkste uitdagingen in deze fase liggen op twee thema's:

2. Overzicht & inzicht.

a. Er is behoefte aan inzicht in wat binnen bestaande bevoegdheden (on)mogelijkheden zijn om meer zicht te krijgen op problematiek die zich online manifesteert en ook wat er preventief mogelijk is (bijvoorbeeld jongerenwerk online). Het Bureau Regionale Veiligheidsstrategie (RVS) Midden-Nederland werkt samen met het Veiligheidsnetwerk Oost-Nederland aan een project waarin gemeenten worden ondersteund bij rechtmatig en doelmatig online openbare-bronnenonderzoek met als doel om de openbare orde en veiligheid te waarborgen. Het zwaartepunt in de ondersteuning ligt bij het juridisch kader, de toepassing van online onderzoekstools en de samenwerking met politie en openbaar ministerie.
b. Er is behoefte aan meer inzicht in welke type van nazorg nodig is als gevolg van informatie die online aanwezig blijft en kan doorwoekeren, onder andere de vraag hoe en of schadelijke online content kan worden verwijderd.
c. Het ontbreekt deels nog aan jurisprudentie die gemeenten van kaders voorziet waarmee het handelingsperspectief duidelijker wordt (bijvoorbeeld voor wat betreft inzet bestuurlijk instrumentarium).
d. Er is behoefte aan inzicht in hoe er balans kan worden gevonden in online onderzoek versus ingrijpen. Een te harde aanpak aan het begin kan bijvoorbeeld juist (onbedoeld) escalatie in de hand werken.
e. Het digitale barrièremodel van het CCV is een goed hulpmiddel bij het verkrijgen van inzicht in deze problematiek en mogelijke interventies[28].
f. Er zijn ook voorbeelden van incidenten waarbij er sprake is van incidenten in het online domein, die fysiek of online worden aangejaagd. Dit is een complex onderwerp omdat het dan in feite gaat om zoiets als online openbare orde. Het is goed om meer inzicht te verkrijgen in de mate waarin

[28] https://hetccv.nl/nieuw-barrieremodel-tegen-online-aangejaagde-ordeverstoringen-geintroduceerd/

deze problematiek speelt en in hoeverre de aanpak van de online aangejaagde openbare-ordeverstoringen hiernaartoe vertaald kan worden.

g. Er is al veel informatie over dit onderwerp voorhanden. Vraag is dus ook of er nieuwe inzichten nodig zijn, of dat bestaande informatie beter bekend moet worden gemaakt onder gemeenten.

Uitdagingen in de warme fase

De belangrijkste uitdagingen in deze fase liggen op vier thema's:

1. Regie.
   a. Een duidelijke afbakening van wie in de online fase wat wanneer doet en hoe en op welke manier informatieoverdracht plaatsvindt (bijvoorbeeld door politie vanuit online onderzoek naar gemeente) behoeft aandacht.
   b. Zodra er incidenten zijn die multi-lokaal/-regionaal/-provinciaal optreden is er nadere afstemming nodig die goed moet worden ingeregeld.
2. Mandaat.
   a. Er is bij gemeenten behoefte aan meer duidelijkheid over wat er met huidige bevoegdheden wel en niet mag, hoe bepaalde bevoegdheden uit het fysieke domein eventueel ook online in te zetten zijn, hoe moreel wenselijk dat is en welke problematiek hiermee mogelijk buiten de boot valt. Wat zijn daarbij de grenzen aan wat mag en wenselijk is op gebied van online onderzoek? Denk bijvoorbeeld aan zaken die nu nog niet bestaan, maar nader kunnen worden onderzocht, zoals een online gebiedsverbod en online BOA's, maar bijvoorbeeld ook aan het verplaatsen van activiteiten naar andere locaties, snel kunnen inzetten van beveiliging, etc.
   b. De vervolgvraag is wie welke bevoegdheden zou moeten hebben in het digitale domein: dus hoe kan er beter zicht worden verkregen op wat er binnen het digitale domein gebeurt, voordat dit zich in het fysieke domein als ordeverstoring manifesteert. Wie beschikt over welke gereedschapskist.
3. Structuur.
   a. Grote uitdaging is dat de ingerichte structuren beter moeten gaan aansluiten op de snelheid waarmee problematiek als deze zich manifesteert.
   b. Er is behoefte aan een onderzoek naar de wenselijkheid van een meldvoorziening voor online aangejaagde openbare-ordeverstoringen.
4. Expertise & Capaciteit.
   a. Er is bij gemeenten handelingsverlegenheid ten aanzien van online onderzoek en analyse: dit is geen taak van gemeenten, maar wat mag er dan wel en hoe samen te werken met de politie? Hoe kunnen ambtenaren beter worden opgeleid op dit onderwerp? De VNG heeft bijvoorbeeld hiervoor de handreiking online onderzoek voor handhaving openbare orde[29] mee opgesteld als vervolg op een handreiking van de ministeries van BZK en J&V[37], maar uit de gesprekken met respondenten blijkt dat hier nog opvolging aan moet worden gegeven. Ook is expertise nodig om de

[29] https://vng.nl/nieuws/handreiking-online-onderzoek-voor-handhaving-openbare-orde

informatie die uit onderzoek naar boven komt juist te interpreteren en daarin de context waarin een incident plaatsvindt mee te nemen.

b. Sommige gemeenten hebben geen ervaring met het fenomeen van online aangejaagde openbare-ordeverstoringen en (dus) ook geen kennis, anderen juist relatief veel (bijvoorbeeld omdat ze met dergelijke incidenten al te maken hebben gehad). Hoe kan deze ervaring beter worden benut als minder ervaren gemeenten te maken krijgen met deze problematiek? Moeten alle gemeenten hier expertise op hebben? Het CCV heeft bijvoorbeeld een webdossier ingericht waar medewerkers van onder meer gemeenten informatie kunnen vinden over best practices & lessons learned ten aanzien van (de aanpak van) online aangejaagde openbare-ordeverstoringen[30].

INFORMATIEBEHOEFTE

Tot slot is de belangrijkste informatiebehoefte op een rij gezet voor iedere fase van de veiligheidsketen. Deze ligt voor online aangejaagde openbare-ordeverstoringen op gebied van preparatie.

Preparatie:

2. Er is behoefte aan tijdig inzicht in wat er online speelt met mogelijke impact op verstoringen van de openbare orde en veiligheid (mogelijke aanvallers, doelwitten en slachtoffers).

[30] https://hetccv.nl/themas/cyberveiligheid/online-aangejaagde-ordeverstoringen/

CONCLUSIES EN AANBEVELINGEN

In dit rapport is een eerste uitwerking gemaakt van twee van de drie systeemuitdagingen uit het Bestuurlijk Convenant Digitale Veiligheid Gemeenten. Specifiek gaat het om de volgende systeemuitdagingen uit het convenant:

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.

Uit deze uitwerking kunnen enkele generieke conclusies worden getrokken. Ook zijn er specifieke conclusies ten aanzien van de twee genoemde systeemuitdagingen te trekken. Deze worden in dit hoofdstuk beschreven evenals enkele aanbevelingen voor een verdere uitwerking van het convenant.

GENERIEKE CONCLUSIES EN AANBEVELINGEN

Op dit moment is er sprake van een complex landschap voor wat betreft de uitdagingen die gemeenten hebben ten aanzien van digitale veiligheid. In dit rapport is een eerste overzicht geschetst van dit landschap, geordend naar de vier incidentcategorieën die we in de inleiding hebben geschetst (zie Tabel 1): (A) interne digitale veiligheid, (B) ontwrichting naar aanleiding van een cyberincident, (C) cybercrime en gedigitaliseerde criminaliteit en tot slot (D) online aangejaagde openbare-ordeverstoringen.

Een belangrijke opbrengst van dit onderzoek is het overzicht dat is gecreëerd van het lokale cybersecuritylandschap op gebied van beleid, uitvoering en toezicht voor deze vier incidentcategorieën. Deze analyse is voor een breed stakeholderveld van

toegevoegde waarde, zo bleek onder andere uit de gesprekken die in het kader van dit onderzoek zijn uitgevoerd.

Ook heeft het onderzoek zicht gegeven op behoeften die er leven om het landschap verder te ontwikkelen. Hoewel dit nog slechts een startpunt biedt voor verdere uitwerking, laat de inventarisatie zien dat er op veel terreinen verdere ontwikkeling mogelijk en soms ook nodig is.

Conclusie van dit onderzoek is dat het op een gestructureerde manier in kaart brengen van het landschap, zowel voor wat betreft beleid, uitvoering en toezicht als voor wat betreft uitdagingen die er spelen van belang is voor de bij dit onderwerp betrokken stakeholders.

Aanbeveling is om het overzicht van het landschap regelmatig (bijvoorbeeld tweejaarlijks) te actualiseren, omdat het voortdurend aan verandering onderhevig is, sommige uitdagingen dan zijn opgelost en er nieuwe uitdagingen (kunnen) ontstaan. Uitdagingen zullen in de loop der tijd ook veranderen als het volwassenheidsniveau van gemeenten inzake digitale veiligheid hoger wordt of wanneer belemmeringen in wet- en regelgeving en nationaal beleid zijn opgelost.

De behoeften die in kaart zijn gebracht zijn weliswaar bij een diverse groep geïnventariseerd (zie bijlage A), maar niet bij veel verschillende organisaties van dezelfde soort. Het geeft een globaal beeld wat er bij sommige organisaties in de keten speelt, maar niet bij een representatief aantal van die organisaties. Wat nodig is voor het vervolg is om op waarde te schatten of de opgehaalde behoeften breed worden herkend en erkend, of deze haalbaar zijn, realistisch zijn en wie eventueel aan zet is om aan deze behoeften invulling te geven.

Conclusie is dat een nadere uitwerking nodig is van de uitdagingen op gebied van de besturing van digitale veiligheid van gemeenten waarbij een grotere en representatieve groep van de verschillende stakeholders om input wordt gevraagd[31].

Aanbeveling is om in kaart te brengen welke concrete casuïstiek ten grondslag ligt aan de in kaart gebrachte behoeften zodat de achterliggende vraag concreet kan worden gemaakt. Bovendien moet in een nadere uitwerking worden vastgesteld hoe breed de geïnventariseerde behoeften leven, wat er nodig is en hoe realistisch ze zijn. Ook moeten er prioriteiten worden gesteld voor wat betreft de eventuele invulling van de behoeften en moeten er dan actiehouders aan worden toegekend.

CONCLUSIES EN AANBEVELINGEN VERTALING FYSIEKE NAAR DIGITALE VEILIGHEIDSSTELSEL

Voor wat betreft de eerste systeemuitdaging heeft dit onderzoek allereerst in kaart gebracht hoe op dit moment het fysieke en digitale domein zich tot elkaar verhouden

[31] Hierbij kunnen onder andere de commissies Bestuur en Veiligheid en Informatiesamenleving van de VNG worden betrokken.

in termen van incidenten en crises. Er zijn vijf aspecten naar voren gekomen die kenmerkend zijn voor de verschillen, namelijk:

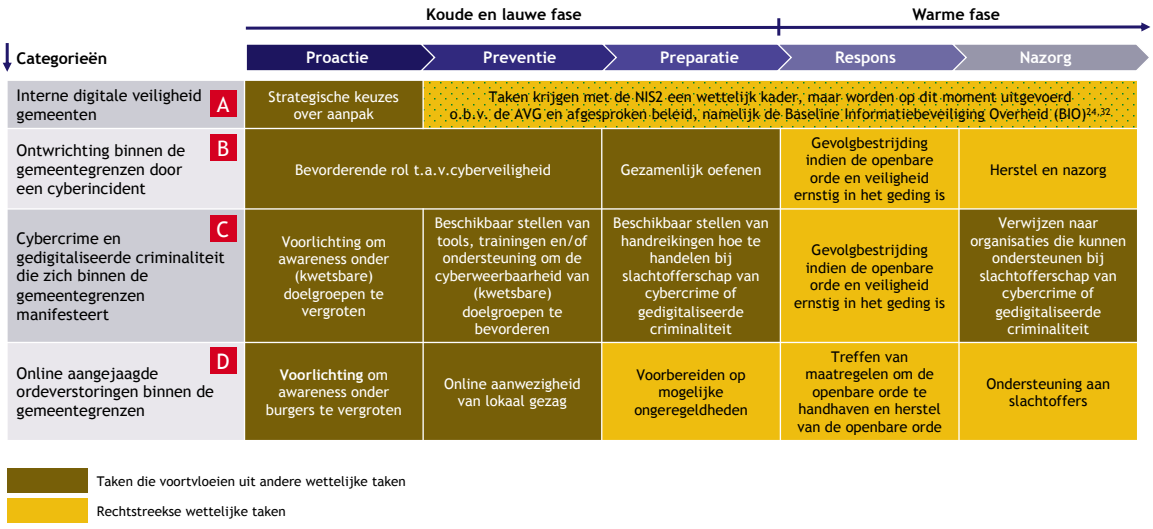
1. Verspreiding: de wijze waarop incidenten en crises opschalen
2. Verbinding: de mate van verbinding naar andere ketens en netwerken
3. Schaal: de mate van voorspelbaarheid van de potentiële schaal van een incident
4. Tijd: de wijze van verloop van incidenten in de tijd
5. Lokaliteit: helderheid over de locatie van assets

Het onderzoek heeft deze kenmerken vervolgens vertaald naar uitdagingen voor de besturing van incidenten en crises.

Conclusie is dat de analyse van de verschillen tussen het fysieke en digitale domein van toegevoegde waarde is voor het begrip van de problematiek en wat er nodig is voor een betere besturing van incidenten en crises.

Aanbeveling is om deze analyse voortaan als ijkpunt te gebruiken bij beleidsvormende initiatieven op dit gebied én om deze regelmatig (bijvoorbeeld tweejaarlijks) te actualiseren.

Voor ieder van de vier incidentcategorieën is vervolgens in kaart gebracht wat op dit moment de verantwoordelijkheden, rollen, taken en bevoegdheden van gemeenten zijn. Dit is in het hoofdstuk *Overzicht landschap digitale veiligheid* schematisch weergeven in Figuur 9, hieronder nogmaals afgebeeld in Figuur 21.



Figuur 21 - Taken en verantwoordelijkheden van gemeenten bij cyberincidenten

Conclusie is dat bij de incidentcategorieën B, C en D de expliciete wettelijke taken en verantwoordelijkheden voornamelijk liggen in de warme fase van incidenten en crises. Deze gaan vooral over incidentgevolgbestrijding op het moment dat de openbare orde en veiligheid in het geding is en over (ondersteuning bij) herstel en nazorg. In incidentcategorie A hebben gemeenten vanzelfsprekend vanaf preventie tot en met nazorg wettelijke taken bij het afhandelen van incidenten die betrekking hebben op de interne digitale veiligheid van gemeentelijke processen en systemen.

Opvallend aspect in de analyse van het aanwezige beleid is dat dit beleid voor incidentcategorieën B, C en D voornamelijk aanwezig is voor de koude en lauwe fase en minder voor de warme fase.

Aanbeveling is om te onderzoeken in hoeverre het beleid dat voor de warme fase is geformuleerd afdoende is voor wat er nodig is voor gemeenten of dat er aanvullend beleid (bijvoorbeeld handreikingen) nodig zijn, met het oog op de verschillen in het verloop van incidenten in het fysieke en digitale domein.

De inventarisatie van uitdagingen laat onder andere zien dat er bij verschillende incidentcategorieën tussen de verschillende stakeholders nog best wat discussie bestaat over wie in de keten welke taken en verantwoordelijkheden zou moeten hebben. Ook is er soms onduidelijkheid over regie, mandaat en opschalingsstructuren.

Het verdient de aanbeveling om bij de verdere uitwerking van de uitdagingen (zie aanbeveling in de sectie over generieke conclusies en aanbevelingen) extra aandacht te besteden aan taken en verantwoordelijkheden en regie en mandaat. Soms zal een bijstelling nodig zijn, maar soms kan worden volstaan bij herbevestiging en heldere communicatie.

Vanuit het perspectief van het Bestuurlijk Convenant Digitale Veiligheid Gemeenten is het uitdagend om uit de brede set van behoeften en uitdagingen er enkele te kiezen om mee aan de slag te gaan. Het publiek maken van dit rapport stimuleert verschillende organisaties binnen dit domein mogelijk om zelf de lopende activiteiten te evalueren en prioriteren.

Tegelijkertijd kan het centraal oppakken van enkele grote thema's vanuit het Bestuurlijk Convenant een impuls geven aan de ontwikkeling van de digitale veiligheid in het lokale domein.

Daarom doen wij in onderstaand overzicht enkele suggesties voor thema's die zich hiervoor lenen, en die uit de gesprekken en beleidsdocumenten als overkoepelende onderwerpen naar boven zijn gekomen. Op sommige van deze thema's lopen al initiatieven. In dat geval is het goed om aan deze initiatieven de uitkomsten van dit onderzoek mee te geven en de voortgang op afstand te monitoren. Andere thema's lenen zich voor een apart vervolg, mogelijk op te pakken vanuit het Bestuurlijk Convenant Digitale Veiligheid Gemeenten.

Categorie	Mogelijk onderwerp meerjarenagenda	Mogelijk aansluiten bij
A - interne digitale veiligheid	Keteneffecten: management van (gezamenlijke) toeleveranciers, de koppeling van IT en OT en de impact daarvan op digitale veiligheid	***Oppakken als vervolgstap bestuurlijk convenant in nauwe relatie met de implementatie van de Cbw***
B - Ontwrichting	Eenduidige en transparante structuren voor opschaling bij incidenten en crises, met	• Update Landelijk Crisisplan Digitaal

	aandacht voor de minder traditioneel betrokken partners, helderheid over regie en mandaat en aandacht voor informatiedeling	• Ontwikkeling van stedelijke en regionale crisisplannen • Verdere uitrol Veiligheidsinformatiecentra Veiligheidsregio's (zoals VIC VR Utrecht)
C - Cybercrime & gedigitaliseerde criminaliteit	Hoe met bestaande bevoegdheden meer bereiken: inzicht nodig in de kern van problematiek, de effectiviteit van diverse aanpakken en de afstemming van taken en rollen	• Gebruikmaken van handreiking CCV over gebruik bestaande monitors • ***Verder oppakken als vervolgstap bestuurlijk convenant***
D - Online aangejaagde openbare-ordeverstoringen	Op welke wijze kan meer zicht worden gekregen op online dreiging die kan leiden tot online en fysieke ordeverstoringen en wie heeft daarbij welke rol	• Er loopt een wetgevingstraject voor de uitbreiding van politiebevoegdheden online i.k.v. openbare orde[32] • Er is een initiatief wet ingediend voor extra bevoegdheden voor burgemeesters[33] • Aanhaken bij lopend project door Veiligheidscoalitie Midden-Nederland naar online aangejaagde openbare-ordeverstoringen
Overkoepelend	Een periodieke meting uitvoeren dan wel het aanreiken aan gemeenten van een meetinstrument over de mate van digitale weerbaarheid van gemeenten op de vier incidentcategorieën (de wegen uit de Lokale Cyberwegenkaart)	***Oppakken als vervolgstap bestuurlijk convenant***
	Blijvend aandacht voor urgentie en rolverdeling verschillende organisaties	Opvolging VNG-project bestuurlijke gesprekken digitale veiligheid indien dit project een vervolg krijgt

Figuur 22 - Suggesties voor opvolging uitkomsten onderzoek

Hoe deze vervolgstappen worden vormgegeven zal nog verder moeten worden uitgewerkt. Voor wat betreft de periodieke meting (overkoepelend onderwerp) doen we hieronder nog enkele aanvullende suggesties.

Landelijke meting cyberweerbaarheid gemeenten

Dit onderzoek heeft vooral het landschap in kaart gebracht en meer kwalitatief zicht gegeven op de belangrijkste uitdagingen op gebied van digitale veiligheid vanuit gemeentelijk perspectief. Om meer grip te krijgen op digitale veiligheid binnen de vier

[32] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2024Z21161&did=2024D49874
[33] https://www.internetconsultatie.nl/oaoov/b1

incidentcategorieën is een goede vervolgstap om op deze categorieën verder in te zoomen per gemeente, voor:

1. Grote gemeenten met meer dan 100.000 inwoners (G40) – ca. 48
2. Middelgrote gemeenten met ca. 30.000 – 80.000 inwoners (M50) - ca. 162
3. Kleine gemeenten met minder dan 25.000 inwoners (K80) – ca. 114

Een aanpak hiervoor kan zijn om een landelijke meting op zetten op de vier incidentcategorieën, die in feite de vier routes zijn van de lokale cyberwegenkaart van het CCV.

Belangrijke aspecten bij zo'n meting zijn:

- Het vaststellen van een methodiek voor het meten op basis van best practices, zoals bijvoorbeeld aan de hand van de ervaring van Noord Holland Veilig die al een vergelijkbare meting heeft uitgevoerd.
- Het is niet de bedoeling een nieuw verantwoordingsinstrument te introduceren, maar een instrument dat inzicht biedt aan de gemeente zelf en geaggregeerd helpt bij het prioriteren van weerbaarheidsinitiatieven. Het biedt dus toegevoegde waarde naast de verantwoording via ENSIA.
- Draagvlak onder gemeenten is noodzakelijk voor het uitvoeren van zo'n meting.

De uitkomsten van een dergelijke meting vormen belangrijke input voor het creëren van een nationaal beeld van de mate van cyberweerbaarheid op de vier incidentcategorieën. Die is enerzijds lokaal bruikbaar voor gemeenten bij het maken van eigen keuzes. Anderzijds is het (geanonimiseerd) input voor de prioritering op regio's en ook een nationale keuze voor het investeren in weerbaarheidsinitiatieven. Daarmee biedt het ook waardevolle input voor de meerjarenagenda in het kader van het Bestuurlijk Convenant.

Als richtlijn wordt meegegeven om een periodieke meting in te stellen waarvoor in 2025 de methodiek kan worden vastgesteld en wellicht getest in een beperkte setting, waarna de meting nationaal wordt uitgerold.

Mocht een brede meting niet (direct) haalbaar zijn, dan kan gestart worden met het aanreiken van een meetinstrument aan gemeenten waarmee zo'n meting kan worden uitgevoerd. Bij succesvolle toepassing binnen meerdere gemeenten ontstaat dan wellicht draagvlak voor een meting bij alle gemeenten.

CONCLUSIES EN AANBEVELINGEN INFORMATIEPOSITIE VAN GEMEENTEN

In aansluiting op de uitdagingen voor wat betreft digitale veiligheid is in het onderzoek ook gekeken naar de informatiepositie die gemeenten nodig hebben op de vier incidentcategorieën en de informatiebehoefte die zij op dit moment ervaren. Deze behoefte staat in nauw verband met de verantwoordelijkheden, rollen, taken en bevoegdheden van gemeenten.

Net als bij de geïnventariseerde uitdagingen is bij informatiebehoefte de vraag in hoeverre deze behoeften breder erkend en herkend worden, of zij haalbaar zijn en realistisch en wat dan eventueel de prioriteiten zijn en wie aan zet is om de behoeften daadwerkelijk invulling te geven.

Aanbeveling is om met gemeenten in gesprek te gaan om de informatiebehoeften verder uit te werken, rekening houdend met het risicoprofiel en omvang van gemeenten. Daarbij wordt geadviseerd om de informatiebehoefte uit te werken aan de hand van concrete casuïstiek waarin knelpunten eerder zichtbaar zijn geworden en vanuit daar kan worden gekeken wat mogelijk, wenselijk, nodig, maar ook haalbaar en realistisch is om te bewerkstelligen.

Wat verder opvalt in de gesprekken over informatiebehoefte is dat de term 'informatie' in de gesprekken diffuus blijft en niet nader gespecificeerd.

Aanbeveling is om bij een verdere uitwerking van de informatiebehoefte van gemeenten het informatiemodel uit het Programma Cyclotron[15] te gebruiken om de behoefte zo concreet mogelijk te maken.

In de paragrafen hieronder worden de belangrijkste behoeften voor wat betreft de informatiebehoefte per incidentcategorie opgesomd.

Interne digitale veiligheid gemeenten

Gemeenten met monitoring capaciteiten ten aanzien van digitale veiligheid hebben behoefte aan meer dreigingsinformatie om daarmee eerder (dreigende) cyberincidenten te kunnen onderkennen. De IBD vult deze behoefte deels al in met het monitoren van het externe aanvalsoppervlak van gemeenten waarmee zij in maart 2024 zijn gestart[34]. Ook hebben gemeenten behoefte aan analyses over het dreigingslandschap ten behoeve van risico inschattingen op gemeentelijk niveau, maar ook om deze te vertalen in concrete beveiligingsmaatregelen binnen de eigen context.

Er is breder binnen gemeenten meer zicht nodig op de afhankelijkheden die er zijn met partners en leveranciers. Cyberincidenten bij deze partners en leveranciers kunnen namelijk ook impact hebben op de werking van gemeentelijke processen en systemen. De IBD heeft hier in het verleden al eerder op proberen in te zetten, maar is hierin nog niet geslaagd. Ten aanzien van de partners en leveranciers is er behoefte aan duidelijkheid over wie er regie heeft op informatievoorziening in de keten, wat de rol is van de gemeente hierbij en in hoeverre dreigingsinformatie die de gemeente bereikt gedeeld mag worden met partners en leveranciers. Ook is het van belang dat gemeenten op tijd geïnformeerd worden als er relevante systemen van partners en leveranciers uitvallen (waaronder bijvoorbeeld ook de BRP en DigiD).

[34] https://www.informatiebeveiligingsdienst.nl/nieuws/start-monitoring-external-attack-surface-gemeenten/

Ontwrichting door een cyberincident bij een organisatie binnen gemeentegrenzen

In de responsfase valt op dat gemeenten soms pas relatief laat op de hoogte zijn van een (dreigend) cyberincident binnen gemeentegrenzen die verstoring van de openbare orde en veiligheid tot gevolg kan hebben. Alleen als dat het geval is hebben gemeenten een expliciet omschreven wettelijke taak. Er is daarom behoefte aan tijdige informatie over (dreigende) cyberincidenten die (kunnen) plaatsvinden bij organisaties binnen gemeentegrenzen. Het gaat dan niet zozeer om technische informatie over zo'n incident, maar vooral om informatie die gaat over de impact en gevolgen ervan, zodat de gemeente haar wettelijke taken in relatie tot de openbare orde en veiligheid goed kan uitvoeren en ook het bredere publiek adequaat kan informeren.

Organisaties binnen de gemeentegrenzen hebben geen wettelijke plicht om dit soort informatie te delen met de gemeente, maar doen er verstandig aan om een risico-inschatting te maken van de impact op de openbare orde en veiligheid en in voorkomende gevallen de gemeente daarover tijdig te informeren. Het zou goed zijn om te onderzoeken hoe dit proces kan worden verbeterd. Overigens zijn er op dit aspect wel zorgen over de haalbaarheid van het realiseren van deze behoefte. Soms ontdekken organisaties zelf pas laat dat zij een incident hebben en realiseren zich vaak niet dat hun gemeente informeren nodig kan zijn. Gemeenten kunnen vanuit de rol van burgervader inzetten op het opbouwen van netwerken met relevante organisaties binnen gemeentegrenzen. Dit zal ook het melden van incidenten helpen bevorderen.

Ook de Rijksoverheid beschikt mogelijk over dit soort informatie. Het is goed om verder te verkennen welke (impact)informatie vanuit de Rijksoverheid beschikbaar is én noodzakelijk is voor gemeenten om hun taken goed te kunnen uitvoeren.

Ook hebben gemeenten behoefte aan een structurele informatievoorziening binnen dit domein in de lauwe fase. Het gaat dan juist om bredere analyses van dreigingen, incidenten, etc. die zicht geven op de dreiging in een bepaalde regio. Juist de gemeentelijke context is hierbij relevant, dus een vertaalslag van wat diverse dreigingen daadwerkelijk kunnen betekenen voor gemeentelijke processen en systemen.

Cybercrime en gedigitaliseerde criminaliteit

Binnen het domein van cybercrime en gedigitaliseerde criminaliteit is er behoefte aan meer inzicht in (herhaald) slachtofferschap. Ook is er behoefte aan meer gestructureerde data over incidenten, op basis van aangiften, en aan meer analyses van slachtofferkenmerken, generieke daderkenmerken en modus operandi. Deze inzichten zijn van toegevoegde waarde om passende interventies te ontwikkelen ten aanzien van dit onderwerp.

Online aangejaagde openbare-ordeverstoringen

Voor wat betreft online aangejaagde openbare-ordeverstoringen valt op dat betrokken organisaties worstelen met de vraag hoe er meer inzicht kan worden verkregen in online sentimenten in relatie tot mogelijke ordeverstoringen, met zo min mogelijk impact op de privacy van burgers. Er zijn veel mogelijkheden om deze problematiek in de fysieke fase te bestrijden, maar dit geldt in mindere mate voor de online fase.

BIJLAGEN

A. GERAADPLEEGDE ORGANISATIES

Er zijn tijdens de uitwerking van het bestuurlijk convenant gesprekken gevoerd met en input gevraagd aan de volgende organisaties:

- Ministerie BZK
- Ministerie J&V
- VNG (ADV, IBD en ENSIA)
- Gemeente Amsterdam
- Gemeente Den Haag
- Gemeente Leeuwarden
- Gemeente Rotterdam
- Gemeente Utrecht
- Provincie Flevoland
- Provincie Gelderland
- Unie van Waterschappen
- Openbaar Ministerie
- Politie
- Veiligheidsregio Noord Holland Noord

6. Veiligheidsregio Utrecht
7. NIPV
8. CCV
9. LIEC
10. RIEC Limburg
11. RIEC Midden Nederland
12. RIEC Noord Holland
13. RIEC Noord Nederland
14. Bureau Regionale Veiligheid Strategie
15. Platform Veilig Ondernemen Den Haag
16. Veiligheidsnetwerk Oost-Nederland
17. Veiligheidsalliantie regio Rotterdam

18. Noord Holland Samen Veilig
- Zorg en Veiligheidshuizen

Ook zijn de uitkomsten gebruikt uit de bestuurlijke gesprekken die de VNG heeft gevoerd met 252 bestuurders van gemeenten die als volgt zijn verdeeld:
- Grote gemeenten (+100.000 inwoners) = 24x gesproken.
- Middelgrote gemeenten (30.000-80.000 inwoners) = 93x gesproken.
- Kleine gemeenten (-25.000 inwoners) = 61x gesproken.

B. OVERZICHT VAN BELEIDSINITIATIEVEN EN BELEIDSDOCUMENTEN

In deze bijlage geven we een opsomming van de verschillende beleidsinitiatieven en in kaart gebrachte bevoegdheden. Deze zijn in meer detail opgenomen in onderstaand Excel-bestand:

- 250514 Overzicht lopende initiatieven uitwerking bestuurlijk convenant digitale veiligheid.xlsx

Lopende acties en beleid

In het Excel bestand is onder andere informatie over wie betrokken zijn, op welke systeemuitdaging het van toepassing is en op welke incidentcategorie, een link naar relevante documentatie en de status opgenomen.

#	**Lopende actie en beleid**
1	Uitwerking voorstel samenwerking met hoogleraar LEI inzake in kaart brengen lokale bevoegdheden digitale veiligheid & criminaliteit
2	Inzichtelijk maken niveau van feitelijke veiligheid van gemeenten
3	Project Online Content Moderatie (PrOCoM)
4	Analyse wetgeving en jurisprudentie online aangejaagde openbare ordeverstoringen
5	Versimpeling en doorontwikkeling ENSIA (ikv toezichtlandschap digitale veiligheid/informatiebeveiliging)
6	Doorontwikkeling van verantwoordings-systematiek ENSIA (Eenduidige Normatief Single Information Audit)
7	Onderzoek naar de kwalitatieve en kwantitatieve behoefte van gemeenten aan arbeidskrachten o.g.v. digitale veiligheid (in voorbereiding)
8	Project 'Frisse blik op arbeidskrapte bij gemeenten'
9	Bestuurlijke peer-to-peer gesprekken digitale veiligheid
10	Cyberoefendriehoek
11	Gezamenlijk oefenen
12	City Deal Cybercrime (pilots)
13	City Deal Cybercrime (investering)
14	Regelgeving
15	Programma Cyclotron
16	Landelijk Dekkend Stelsel (LDS)/ Cyberweerbaarheidsnetwerk (CWN)
17	Onderzoek- en opsporingscapaciteit cybercriminelen
18	Opzet Risicobeheerfonds Cyber
19	Herkenbare overheid
20	Register internetdomeinen
21	Uniforme domeinnaamextensie
22	Ontwikkeling overheidsbreed internetdomeinbeleid

23	Kennisverbreding/-deling, verdieping
24	Regelgeving/BIO
25	Voorlichtingscampagnes/Awareness
26	Voorlichtingscampagnes cyberveiligheid
27	Voorlichtingscampagnes (veiliginternetten.nl)
28	Verkenning leveranciersmanagement
29	Verkenning leveranciersmanagement (tool inkoopeisen)
30	Uitwerking informatiebehoefte G4 (intern en extern)
31	Onderzoekssamenwerking DVDH TU Delft
32	Ondersteuningsprogramma BIO voor de gehele overheid
33	Uitbreiding en doorontwikkeling van de service IB&P-hulp
34	Monitoring/benchmarktooling
35	Kennisverbreding/-deling, verdieping
36	Onderzoek om de cyberweerbaarheid van de lagere overheden in kaart te brengen
37	Handreiking online monitoring door gemeenten ihkv OOV
38	Lokale cross-sectorale deeloefening met partijen in de stad tijdens ISIDOOR 2023
39	ISIDOOR (IV)
40	Uitwerken Sturingsmodel NLCS irt lokaal bestuur
41	Verkenning bevoegdheden openbare orde politie online
42	Lokale ecosysteemontwikkeling en cyberweerbaarheidscentra en netwerken: cross-sectoraal en voor lokale 'topsectoren'
43	Regionale aanpak digitale criminaliteit in regionale samenwerkingsverbanden
44	Impactanalyse naar de uitvoeringslast van informatiebeveiliging voor gemeenten
45	Onderwijssamenwerking DVDH DIVD Academy
46	Juridische grenzen en kansen bij openbare-ordehandhaving
47	Lokaal bestuur in een digitaliserende samenleving
48	Gemeentelijke online monitoring
49	Burgermeesters in cyberspace
50	Proeflokalen OOV op orde
51	Dreigingsbeeld informatiebeveiliging Nederlandse Gemeenten
52	Bestuurlijke bevoegdheden cyber
53	Cybergevolgbestrijding
54	Kennis en kunde voor regionale cybergevolgbestrijding
55	Handreiking Cybergevolgbestrijding ter versterking van digitale weerbaarheid G4-gemeenten
56	Project Cyberbeelden
57	Zicht-op dashboards - gedigitaliseerde criminaliteit
58	Cybersessions
59	VNG-handreikingen en andere best practices (i.k.v. BIO) voor gemeenten
60	Onderzoek wetgevingskader informatieveiligheid (2020)
61	Onderzoek toezicht op informatieveiligheid (2022)
62	Landelijk Crisisplan Digitaal (LCP)
63	Toolbox Veilig Inkopen (2024)
64	Publicatie AIVD/MIVD: Cyberaanvallen door statelijke actoren - zeven momenten om een aanval te stoppen
65	Cyberscenario's voor veiligheidsregio's
66	Samenhangend Inspectiebeeld cybersecurity vitale processen
67	Basismaatregelen voor cybersecurity van IACS
68	Basis-beveiligingsmaatregelen Slimme Apparaten (IoT)
69	Security Check Procesautomatisering
70	Focusblad Digitale Veiligheid
71	Geldezel tool

72	Online aangejaagde openbare-ordeverstoringen - Toelichting bij het digitale barrièremodel
73	Handelingsperspectief bij online aangejaagde openbare-ordeverstoringen
74	Fenomenenkaart online aangejaagde openbare-orde verstoringen
75	Tools van het Digital Trust Center
76	Meldknop.nl
77	Interventiekaart online aangejaagde openbare- ordeverstoringen
78	Sectorale evaluatie ISIDOOR-4
79	(Voorbereiding op) digitale ontwrichting
80	Stappenplan Cyberoefendriehoek
81	Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten
82	Digitale Agenda Gemeenten 2024
83	Cyber- en IT-crisisplan gemeente Den Haag
84	Cyberscenario's voor veiligheidsregio's
85	Overzicht van samenwerkingsverbanden
86	Actieprogramma Veilig Ondernemen
87	Veiligheidsagenda 2023-2026
88	Cybercrime beeld 2024
89	Cyberbeveiligingswet
90	Baseline Informatiebeveiliging Overheid (BIO)
91	Protocol Online Onderzoek

Bevoegdheden

In het Excel bestand is onder andere het wettelijk kader, een omschrijving en de incidentcategorie opgenomen.

#	**Bevoegdheid/wet**
B.1	Toezicht op evenementen
B.2	Informatieplicht
B.3	Noodbevel
B.4	Noodverordening
B.5	Algemene bevoegdheid ter handhaving openbare orde
B.6	Openbare ordebevoegdheden
B.7	Bestrijding voetbalvandalisme en ernstige overlast
B.8	Bestuurlijke ophouding
B.9	Bewaking en beveiliging van personen, objecten en diensten
B.10	Cameratoezicht om de openbare orde te handhaven
B.11	Informatie-uitwisseling voor de handhaving van de openbare orde
B.12	Noodbevoegdheden ter handhaving van de openbare orde of ter beperking van gevaar
B.13	Beperkende bevoegdheden bij een samenkomst op een openbare plaats
B.14	Preventief fouilleren voor de handhaving van de openbare orde
B.15	Toezicht op openbare samenkomsten
B.16	Preventieve last onder dwangsom
B.17	Last onder dwangsom
B.18	Meldplicht
B.19	Groepsverbod
B.20	Gebiedsverbod
B.21	Gedragsaanwijzing
B.22	Bevoegdheid tot binnendringen in geautomatiseerd werk
B.23	Verbod op onrechtmatige uitlatingen gericht op openbare-ordeverstoring
B.24	Wet digitale overheid
B.25	Wet Veiligheidsregio's

B.26	Paspoortuitvoeringsregeling (PUN)
B.27	Paspoortwet
B.28	Wet basisadministraties persoonsgegevens BES
B.29	Basisregistratie Personen (BRP)
B.30	Algemene verordening gegevensbescherming (AVG)
B.31	Digitale persoonsidentificatie (DigiD)
B.32	Basisregistratie Adressen en Gebouwen (BAG)
B.33	Wet basisregistratie adressen en gebouwen
B.34	Organisatiewet Kadaster
B.35	Basisregistratie Grootschalige Topografie (BGT)
B.36	Basisregistratie Ondergrond (BRO)
B.37	Handelsregisterwet
B.38	Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet)
B.39	Werkloosheidswet
B.40	Wet inkomensvoorziening oudere werklozen
B.41	Ziektewet
B.42	Wet op de arbeidsongeschiktheidsverzekering
B.43	Wet werk en inkomen naar arbeidsvermogen
B.44	Toeslagenwet
B.45	Algemene Ouderdomswet
B.46	Algemene nabestaandenwet
B.47	Algemene Kinderbijslagwet
B.48	Wet arbeidsongeschiktheidsverzekering zelfstandigen
B.49	Wet arbeidsongeschiktheidsvoorziening jonggehandicapten
B.50	Participatiewet
B.51	Wet Maatschappelijke Ondersteuning
B.52	Jeugdwet
B.53	Algemene Plaatselijke Verordening (APV)
B.54	Wet gegevensverwerking door samenwerkingsverbanden
B.55	Wetboek van Strafvordering (WvSv)
B.56	Bevel tot ontoegankelijk maken van gegevens
B.57	Vervolging en veroordeling wegens opruiing
B.58	Vervolging en veroordeling wegens verspreiding van opruiend materiaal
B.59	Vervolging en veroordeling wegens voorbereiding van openlijke geweldpleging
B.60	Vervolging en veroordeling wegens Smaad
B.61	Vervolging en veroordeling wegens Laster
B.62	Gedragsaanwijzing aan verdachte die de openbare orde ernstig heeft verstoord en waarbij grote vrees voor herhaling bestaat

C. OPSOMMING VAN DIVERSE SUGGESTIES IN HET DOCUMENT

In het document worden op diverse plekken al concrete suggesties gedaan voor oplossingsrichtingen die niet bij de conclusies en aanbevelingen op hoofdlijnen terugkomen. In onderstaande tabel worden deze opgesomd met verwijzing naar de pagina waar deze suggestie terug te vinden is.

#	Oplossingsrichting	Pagina
1	Wederkerigheid inbrengen in de relatie met stelselhouders: gemeenten zicht geven over de status van de beveiliging van de landelijke voorzieningen zodat zij een goede inschatting kunnen maken van risico's die zij (kunnen) lopen.	40

2	Gemeenten stimuleren netwerkkaarten te maken waarin duidelijk wordt welke stakeholders bij een incident in het digitale domein betrokken moeten worden.	40
3	Mogelijk kan threat intelligence voor hoger volwassen gemeenten die dit kunnen verwerken gezamenlijk worden ingekocht. Hier kan een rol zijn weggelegd voor de IBD.	42
4	In het register met cyberincidenten die worden gemeld i.k.v. de Cbw kan bij melding het advies worden gegeven aan melders om bij risico's i.k.v. openbare orde en veiligheid de gemeente vroegtijdig te informeren.	47
5	Uitwerken van oefenscenario's die expliciet ingaan op de verschillen tussen het fysieke en digitale domein	48
6	Het maken van een bredere stakeholderkaart met betrokken organisaties bij het bestrijden van cybercrime en gedigitaliseerde criminaliteit	56