Stadsbestuur en digitale veiligheid

Een analyse van beleidsplannen

Wouter Stol en Willem Bantema

1. Inleiding

Een stad kan pas veilig zijn als zij ook digitáál veilig is. Daarvoor heeft het bestuur van de betreffende gemeente een verantwoordelijkheid. Eerder benoemden we vijf gemeentelijke *work packages* voor digitale veiligheid.[1] Ten eerste dient de gemeente in eigen huis haar informatiebeveiliging op orde te hebben. Ten tweede dient zij een coördinerende rol te vervullen om andere actoren te stimuleren, te faciliteren en met elkaar in verbinding te brengen: de klassieke gemeentelijke 'regierol'[2] maar dan voor digitale veiligheid. Ten derde dient de gemeente te zorgen dat evenementen in haar gemeente digitaal veilig zijn. Ten vierde zullen gemeenten zich dienen te informeren over mogelijk ophanden zijnde ordeverstoringen, wat tegenwoordig inhoudt dat zij ook op de hoogte moeten blijven ('monitoren') van wat zich online daarover aandient. Ten vijfde dient de gemeente maatregelen te nemen indien online activiteiten de offline openbare orde in de gemeente (dreigen te) verstoren. In deze bijdrage bouwen we voort op deze vijf gemeentelijke *work package*s inzake digitale veiligheid.

In paragraaf 2 presenteren we aanvullend als zesde *work package* het gemeentelijk optreden bij een 'cybercrisis' ofwel een crisis met een digitale oorzaak, zoals een waterkering die uitvalt door een hack. Zo'n crisis met digitale oorzaak vraagt een specifieke voorzorg en repressie en daarin heeft de gemeente een verantwoordelijkheid. Het definiëren van gemeentelijke *work packages* geeft een theoretisch overzicht, maar de vraag is of 'digitaal' inmiddels ook echt doordringt in gemeentelijke beleidsplannen en naar welke *work packages* de aandacht dan uitgaat[3] In paragraaf 3 en 4 presenteren we een verkenning van wat gemeenten inmiddels (zeggen te) doen aan digitale veiligheid. Paragraaf 5 tot slot bevat conclusies en discussie.

2. Gemeenten en 'cybercrises' of crises met digitale oorzaak

De eerder genoemde vijf *work packages* (informatiebeveiliging, regierol, evenementenveiligheid, monitoren, maatregelen) dekken nog niet de situatie van een 'cybercrisis' ofwel een crisis met een digitale oorzaak, zoals een elektriciteitscentrale of waterkering die uitvalt door een hack of door een ddos- of ransomware-aanval. Artikel 1 van de Wet veiligheidsregio's definieert een crisis als 'een situatie waarin een vitaal belang van de samenleving is aangetast of dreigt te worden aangetast'. Voor een cybercrisis geldt dat de genoemde situatie langs digitale weg tot stand komt. De essentie van een cybercrisis is dus nog steeds offline (bv. een uitgevallen centrale) maar wordt wel digitaal veroorzaakt (bv. een hack).[4] Net als bij elke andere crisis heeft de gemeente bij een cybercrisis een rol. Een cybercrisis vergt een specifieke aanpak.

De eerste reden daarvoor is dat voor het herstellen van de oude situatie ándere instanties moeten worden ingeschakeld dan het geval is bij een analoge crisis. Is de oorzaak digitaal, dan zal

---

1 W. Stol & W. Bantema, 'De gemeente en de digitaal veilige stad', in: J.W. Sap & E. Kolthoff (red.) *De veilige stad als collectief doel*, Nijmegen: Ars Aequi Libri 2019, p. 123-130.

2 C. Tielenburg & W. Stol, 'Rijk, provincie, gemeente en andere bestuursorganen', in: W. Stol e.a. (red.) *Basisboek integrale veiligheid,* Den Haag: Boom criminologie, 2016, p. 199-214.

3 De vraag of de voornemens inzake digitaal veiligheidsbeleid ook daadwerkelijk tot uitvoering komen of zijn gekomen, valt buiten het bestek van deze bijdrage

4 Een crisis die er uit bestaat dat enkel de online openbare orde is verstoord, blijft hier buiten beschouwing.

een Computer Emergency Response Team (CERT) of in elk geval een digitaal specialist moeten worden ingeschakeld om de oude situatie te herstellen. De gemeente moet dus een overzicht hebben van wiens hulp kan worden ingeroepen bij crises met een digitale oorzaak.

De tweede reden dat de gemeente zich specifiek moet voorbereiden op een crisis met een digitale oorzaak is dat een digitale oorzaak tot specifieke vragen kan leiden bij burgers of niet-getroffen instanties: wat is er aan de hand en wat staat er nog meer te gebeuren? Digitale verstoringen zijn minder inzichtelijk en minder eenvoudig te begrijpen dan analoge verstoringen. Langs digitale weg kan de oorzaak van de cybercrisis snel ook elders opduiken en daar wanorde veroorzaken. Een crisis met een digitale oorzaak zal dan ook sneller onrust veroorzaken. Het is een taak van de gemeente om haar inwoners op een passende wijze voor te lichten over een ontstane crisis en over de mogelijke gevolgen en óók is haar taak om te beoordelen of regionale of landelijke voorlichting nodig is. Bij een crisis met digitale oorzaak zal de gemeente dus haar crisiscommunicatie dienen af te stemmen op specifieke vragen of onzekerheden waartoe de digitale oorzaak aanleiding geeft. Dat is het principe, maar ons is geen onderzoek bekend dat vervolgens helder maakt (i) welke onzekerheden een digitale oorzaak precies oproept en bij wie, en (ii) hoe daarop in crisiscommunicatie goed kan worden ingespeeld. Hier ligt een taak voor de communicatiewetenschap.

3. Digitale veiligheid in beleid van 27 gemeenten

3.1 Methode

Om een beeld te krijgen van de aandacht voor digitale veiligheid in gemeentelijk beleid hebben we een deskresearch uitgevoerd. Bij 31 gemeenten zochten we via (de zoekfunctie van) de gemeentelijke website naar een veiligheidsbeleidsplan, coalitieakkoord, begroting, informatiebeveiligingsbeleid en evenementenbeleid. Vaak waren dat aparte documenten (pdf-formaat) maar in enkele gevallen staat bijvoorbeeld het veiligheidsbeleid of een begroting beschreven op de website (html-formaat). In geval van evenementen hebben we soms informatie vergaard door een aanmeldingsformulier voor een evenement in te vullen (uiteraard zonder deze in te dienen).

Op de website van de gemeenten is gezocht op "veiligheidsbeleid", "veiligheid", "evenement", "begroting", "coalitieakkoord", "informatiebeveiliging" en "cyber". Binnen de aangetroffen documenten of webpagina's is vervolgens gezocht op "cyber", "internet" en "digita". We hebben aldus per gemeente beoordeeld of de gemeente in haar uitingen aandacht heeft voor de door ons beschreven zes gemeentelijke *work packages* voor digitale veiligheid.[5] Een gemeente hoeft in onze benadering geen geheel uitgewerkt digitaal veiligheidplan te hebben. Een enkele zin was genoeg om te noteren dat de gemeente in haar beleid aandacht heeft voor een specifieke *work package.* Een zin zoals 'Het MKB krijgt voorlichting over cybercrime' in een coalitieakkoord, is bijvoorbeeld al genoeg om te noteren dat deze gemeente in haar beleid aandacht heeft voor het *work package* 'regierol'. Het op de gemeentelijke website opnemen van een verwijzing naar www.politie.nl met de opmerking dat men daar aangifte kan doen van onder meer internetfraude of het in een beleidsplan aantreffen van de zinsnede 'digitalisering vereist digitale weerbaarheid', is niet beoordeeld als het invulling geven aan de regierol, omdat dergelijke teksten niet op een gemeentelijke activiteit wijzen.

Nederland heeft momenteel 355 gemeenten. De grote vier (G4) bespreken we apart (paragraaf 4). De resterende 351 gemeenten plaatsten we in alfabetische volgorde en daarvan selecteerden we steeds elke 13^{e} gemeente, te beginnen bij nummer 13 en eindigend bij nummer 251, wat

[5] Een document van 39 bladzijden met de ruwe data is op te vragen bij de auteurs.

resulteerde in een selectie van 27 gemeenten. Tabel 1 geeft deze weer op volgorde van inwoneraantal. De selectie bevat 7 gemeenten met minder dan 30.000 inwoners, 11 met 30-50.000, 5 met 50-100.000 en 4 met meer dan 100.000 inwoners. Geografisch gezien zijn de 27 gemeenten niet egaal over Nederland verspreid. De selectie bevat bijvoorbeeld 6 gemeenten uit Zuid-Holland, 5 uit Noord-Holland en geen uit Drenthe en Groningen.

Onbekend is of de 27 geselecteerde gemeenten qua aandacht voor aspecten van digitale veiligheid afwijken van de andere gemeenten en of de 27 dus een goed beeld geven van de situatie in 'de Nederlandse gemeenten min de G4'. De bevindingen moeten dus met voorzichtigheid worden geïnterpreteerd. We reiken de bevindingen dan ook aan als enkel een indicatie. Wie op een bepaald onderwerp resolute conclusies wil trekken, is aangewezen op vervolgonderzoek.

Onze deskresearch beperkt zich verder tot hetgeen gemeenten op hun website aan informatie aanbieden over hun beleidsvoornemens. Dat is niet hetzelfde als álles waarvoor gemeenten aandacht hebben of álles wat zij daadwerkelijk doen. Het is mogelijk dat op de website niets staat over digitale veiligheid maar dat de betreffende gemeente daaraan de facto wel aandacht geeft. Andersom is ook niet uitgesloten. Verder is het mogelijk dat we informatie hebben gemist, bijvoorbeeld omdat de gebruikte trefwoorden ons daar niet naartoe hebben geleid. Kortom, ons onderzoek geeft zicht op wat de 27 gemeenten op hun website extern communiceren over hun voornemens inzake digitale veiligheid, voor zover onze trefwoorden de informatie daarover hebben getraceerd.

Tabel 1: Gemeenten in de steekproef en hun aandacht in beleid voor de zes gemeentelijke work packages: (1) informatiebeveiliging in eigen huis, (2) regierol, (3) evenementenveiligheid, (4) monitoren internet, (5) maatregelen ivm ordehandhaving, (6) cybercrises

	Gemeente	**Provincie**	**Inwoners ***	**1**	**2**	**3**	**4**	**5**	**6**
1	Ameland	Friesland	3.727	x					
2	Hardinxveld-Giessendam	Zuid-Holland	18.280	x		x		x	
3	Dantumadiel	Friesland	18.934	x					
4	Roerdalen	Limburg	20.593	x					
5	Koggenland	Noord-Holland	22.834	x					
6	Stein	Limburg	24.986	x					
7	Sint-Michielsgestel	Noord-Brabant	29.158	x					
8	Tytsjerksteradiel	Friesland	31.997	x	x				x
9	Maassluis	Zuid-Holland	33.127	x					
10	Beekdaelen	Limburg	35.944	x					
11	Bronckhorst	Gelderland	36.016	x					
12	Montferland	Gelderland	36.102	x					
13	Hellevoetsluis	Zuid-Holland	40.107	x					
14	Dronten	Flevoland	41.462	x					
15	De Bilt	Utrecht	43.164	x	x				
16	Noordoostpolder	Flevoland	47.157	x					
17	Hollands Kroon	Noord-Holland	48.374	x					
18	Waalwijk	Noord-Brabant	48.627	x	x				
19	Pijnacker-Nootdorp	Zuid-Holland	55.190	x					
20	Oosterhout	Noord-Brabant	55.967	x					

21	Gooise Meren	Noord-Holland	58.151	x					
22	Velsen	Noord-Holland	68.625	x					
23	Leidschendam-Voorburg	Zuid-Holland	76.472	x					
24	Westland	Zuid-Holland	110.220	x	x				
25	Zwolle	Overijssel	128.617	x	x				
26	Zaanstad	Noord-Holland	156.703	x	x				
27	Enschede	Overijssel	159.934	x					
	TOTAAL			27	6	1	0	1	1

* Ministerie van Sociale Zaken en Werkgelegenheid: https://www.uitvoeringvanbeleidszw.nl/subsidies-en-regelingen/verander opgave-inburgering-pilots/tabel-aantal-inwoners-gemeenten-per-1-januari-2019, geraadpleegd op 02-02-2020.

3.2 Bevindingen

Informatiebeveiliging

Alle 27 gemeenten melden op hun website dat ze aandacht besteden aan het beveiligen van de informatie die zij hebben over hun burgers (tabel 1). Vaak doen zij dat onder het kopje ‘privacyverklaring’ en verwijzen ze naar wetgeving waaraan zij hebben te voldoen. Gemeente Stein meldt bijvoorbeeld: ‘De gemeente Stein beveiligt persoonsgegevens zo goed als mogelijk tegen verlies of tegen enige vorm van onrechtmatig gebruik. Hiervoor nemen we alle passende technische en organisatorische maatregelen. Wij houden ons aan de regels voor gegevensbescherming die voor gemeenten gelden.’[6] Geregeld verwijzen gemeenten naar de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en naar de Algemene Verordening Gegevensbescherming (AVG). In een ‘raadsinformatiebrief’ van 15 maart 2019 schrijft burgemeester De Haan van Maassluis bijvoorbeeld: ‘Gemeenten krijgen ondersteuning van de VNG bij het Informatiebeveiligingsbeleid. Hiervoor is de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) ontwikkeld. Deze is in 2013 door de gemeenten vastgesteld. De BIG bevat de normen die nodig zijn om te zorgen voor een stabiele en veilige informatiebeveiliging binnen een gemeente. De normen in de BIG zijn afgestemd op de Wet bescherming persoonsgegevens (WBP) en vanaf 25 mei 2018 op de Algemene Verordening Gegevensbescherming (AVG), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (de SUWI-wet), de Gemeentelijke Basisadministratie (GBA en de opvolger BRP), Basisregistratie Adressen en Gebouwen (BAG) en de Wet Paspoortuitvoeringsregeling (PUN). In 2020 gaan gemeenten, Rijk, waterschappen en provincies gebruik maken van één uniform normenkader voor informatiebeveiliging: de Baseline Informatiebeveiliging Overheid (BIO).’[7] Gemeente De Bilt vertrekt in haar ‘Programmabegroting 2020. Meerjarenraming 2021-2024.’ niet zozeer vanuit wettelijke kaders maar meer vanuit mens en organisatie: ‘In onze eigen organisatie zijn op de verschillende domeinen medewerkers op operationeel niveau belast met informatieveiligheid. 2020 staat in het teken van de permanente bewustwording van cybersecurity en het permanent monitoren en verbeteren van de veiligheid van onze geautomatiseerde en analoge informatieverwerking.’[8]

6 https://www.gemeentestein.nl/register-van-verwerkingen, geraadpleegd 2 februari 2020.

7 https://maassluis.raadsinformatie.nl/document/7425418/1/Raadsinformatiebrief_Verantwoording_Informatie beveiliging_2018_en_informatiebeveiligingsbeleid_2019/, geraadpleegd 2 februari 2020.

8 https://www.debilt.nl/bestuur-en-organisatie/college/financien-en-jaarverslagen/, geraadpleegd 3 februari 2020.

Bij de twee gemeenten Montferland en Oosterhout vonden we een uitgewerkt disclosure-beleid.[9] Montferland schrijft: 'Als u een zwakke plek in één van onze systemen heeft gevonden horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze systemen en gegevens beter te kunnen beschermen.' Op de website van Oosterhout staat: 'Als u een zwakke plek in één van onze systemen heeft gevonden horen wij dit graag zodat we zo snel mogelijk maatregelen kunnen nemen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.' De formulering lijkt afgeleid van een standaardtekst (en waarom ook niet) maar het voeren van een actief disclosurebeleid is bij gemeenten kennelijk nog geen regel. Een enkele gemeente haakt in op de actualiteit en meldt dat maatregelen zijn genomen in verband met het in januari 2020 geopenbaarde beveiligingsprobleem in het computerprogramma Citrix, zoals Pijnacker-Nootdorp. 'Op advies van het Nationaal Cyber Security Centrum van het ministerie van Justitie en Veiligheid heeft de gemeente Pijnacker-Nootdorp op vrijdag 17 januari Citrix preventief uitgeschakeld vanwege een kwetsbaarheid in het systeem.'[10]

Het totaalbeeld dat oprijst uit de websites van de 27 gemeenten is dat informatiebeveiliging en daarmee privacybescherming van alle gemeenten aandacht krijgen. De wettelijke basis helpt daarbij. Voor gemeenten is dat een duidelijk en handzaam vertrekpunt. Er lijkt evenwel een verschil met wat we 'actieve informatiebeveiliging' zouden kunnen noemen: het vergroten van de digitale weerbaarheid van de gemeente middels het uitnodigen van bezoekers om kwetsbaarheden te melden (disclosurebeleid), proactief aan de slag gaan met de digitale weerbaarheid van medewerkers en extern communiceren over gemeentelijke maatregelen tegen kwetsbaarheden (Citrix). Informatiebeveiliging is een gearriveerd onderwerp, maar onze verkenning geeft verder de indruk dat niet alle gemeenten een expliciete, voorbeeldstellende rol nemen in het bredere maatschappelijke goed van digitale weerbaarheid.

Regierol inzake digitale veiligheid

Bij zes gemeenten vonden we op hun website, of daaraan gelinkt, tekst die verwees naar een gemeentelijke verantwoordelijkheid (regierol) voor digitale veiligheid in de samenleving, geconcretiseerd in activiteiten. Op volgorde van gemeentegrootte gaat het om: Tytsjerksteradiel, De Bilt, Waalwijk, Westland, Zwolle en Zaanstad (tabel 1). Hierna volgt wat we bij hen aantroffen.

(1) De beleidsnotitie inzake veiligheid van Tytsjerksteradiel, eindigt met een paragraaf 'overige aandachtspunten' en daarin de zin: 'Lokaal zijn al een aantal initiatieven gestimuleerd in het kader van cyberveiligheid.'[11] Welke initiatieven dat zijn, blijft onvermeld. In de programmabegroting 2020-2023 van deze gemeente staat de 'Preventieve taak op het gebied van cybercrime' genoemd als nieuwe gemeentetaak.[12] (2) In De Bilt vermeldt het coalitieakkoord 2018-2022 dat de gemeente cybercriminaliteit wil voorkomen met voorlichting.[13] (3) Waalwijk geeft op haar website haar

[9] resp. https://www.montferland.info/direct-regelen/beveiligingslek-of-datalek-ontdekt_46154/ en https://www.oosterhout.nl/metamenu/over-de-gemeente/veiligheid-systemen/, beide geraadpleegd 2 februari 2020.

[10] https://www.pijnacker-nootdorp.nl/artikelen/pijnacker-nootdorp-schakelt-citrix-uit.htm, geraadpleegd 2 februari 2020.

[11] https://www.t-diel.nl/organisatie-bestuur-t-diel/besluiten-van-het-college_43907/item/persbesluitenlijst-24-september-2019_44971.html, geraadpleegd 3 februari 2020.

[12] https://www.t-diel.nl/inwoners-t-diel/pdfs_44124/, geraadpleegd 3 februari 2020.

[13] https://www.debilt.nl/bestuur-en-organisatie/college/samenstelling-college/, geraadpleegd 3 februari 2020.

inwoners een serie tips om de kans op slachtofferschap van cybercriminaliteit te verkleinen.[14] Er staan verder geen gemeentelijke activiteiten genoemd. (4) Voor gemeente Westland betekent veiligheid voor ondernemers dat zij 'bewust zijn en blijven van de risico's, bijvoorbeeld op het vlak van cybercrime' en de gemeente versterkt dat door 'awareness-/weerbaarheids trainingen'.[15]

(5) In de ´Veiligheidsvisie 2019-2020´ van de gemeente Zwolle is digitale veiligheid en terugkerend thema.[16] In het voorwoord zet burgemeester Henk Jan Meijer direct de toon als hij schrijft: 'Er zijn meer ontwikkelingen die de komende jaren onze extra aandacht vragen. Zo wordt digitale veiligheid steeds belangrijker. De afhankelijkheid van de samenleving van het internet neemt toe en dit brengt kwetsbaarheden met zich mee. We hebben bijvoorbeeld te maken met hackers die persoonlijke gegevens willen stelen of met geraffineerde vormen van internetoplichting.' Voor de gemeente Zwolle is 'het versterken van de digitale veiligheid' een van de zes opgaven die zij zichzelf stelt op veiligheidsgebied. In de Veiligheidsvisie is 'digitale veiligheid' dan ook een aparte paragraaf. In het document staat onder meer: 'In onze strategie richten we ons op het versterken van onze eigen digitale weerbaarheid en dat van de samenleving, omdat deze achterblijft bij de dreiging en juist weerbaarheid daaraan een tegenwicht kan bieden. (...) [W]e hebben oog voor de wederzijdse beïnvloeding van de digitale en fysieke wereld in veiligheidssituaties. Bij inwoners en ondernemers versterken we de bewustwording van digitale risico's. We hebben daarin ook aandacht voor digitale zelfredzaamheid, zodat mensen weten wat zij zelf kunnen doen.' Over de aanpak van digitale onveiligheid staat: 'De verwachting is dat cybercrime toeneemt en de digitale dreigingen toenemen. Omdat de weerbaarheid daartegen in de samenleving achterblijft, zien we aanleiding om onze strategie op deze onderdelen de komende jaren uit te bouwen en te verstevigen.' Bij de aanpak van onveiligheid in winkelgebieden en bedrijventerreinen 'is aandacht voor criminaliteit en overlast, maar ook voor verkeers- en brandveiligheid en cybercrime.' Kortom, in gemeente Zwolle is digitale veiligheid niet ergens een aandachtspunt maar een thema in veiligheidsbeleid.

(6) Gemeente Zaanstad geeft op haar website aandacht aan cybercrimebestrijding.[17] 'De gemeente Zaanstad wil samen met de politie de cybercriminaliteit in Zaanstad terugdringen. Om nog beter tegen cybercriminaliteit te kunnen optreden is de gemeente benieuwd naar uw ervaringen. Deze kunt u sturen naar meldcyber@zaanstad.nl. Vragen over dit onderwerp, kunt u ook via dit mailadres stellen. Bijvoorbeeld bij welke betrouwbare instanties u terecht kunt met vragen over het voorkomen van online oplichting. De gemeente helpt u hier graag mee op weg.'

Overige work packages

Bij één gemeente vonden we een tekst die suggereert dat de gemeente een verbinding maakt tussen digitalisering en de veiligheid van een evenement (*work package* 3). In het 'Evenementenbeleid Gemeente Hardinxveld-Giessendam', vastgesteld op 17 februari 2015, staat in bijlage 1 in het aanvraagformulier voor een evenementenvergunning de vraag via welke media voor het evenement reclame wordt gemaakt, met daaronder als één van de opties 'internet, zoals; ...'. Mogelijk dat de gemeente dit heeft opgenomen na 'project x' in Haren op 21 september 2012, toen berichtgeving via internet zorgde voor een massale toeloop naar een evenement. We hebben niet van alle 27

[14] https://www.waalwijk.nl/inwoners/cybercrime_43188/, geraadpleegd 3 februari 2020.

[15] https://www.gemeentewestland.nl/fileadmin/documenten/veiligheid/WVB20192022.pdf, geraadpleegd 3 februari 2020.

[16] https://www.zwolle.nl/sites/default/files/veiligheidsvisie-2019-2022.pdf, geraadpleegd 11 februari 2020.

[17] https://www.zaanstad.nl/mozard/!suite86.scherm0325?mVrg=14631&mNch=qqc6hun3jg, geraadpleegd 11 februari 2020.

gemeenten in tabel 1 een aanvraag voor een evenement ingevuld (wat vaak nodig is om de vragen te zien die aan de aanvrager worden gesteld), dus we sluiten zeker niet uit dat ook andere gemeenten deze vraag stellen aan een aanmelder van een evenement. Bij geen van de 27 gemeenten vonden we een verwijzing naar het monitoren van internet (*work package* 4). Bij één gemeente vonden we een tekst die men zou kunnen interpreteren als een voornemen tot het nemen van maatregelen tegen online activiteiten die de offline openbare orde (dreigen te) verstoren (*work package* 5). In haar 'Uitvoeringsplan Integraal Veiligheidsbeleid 2014-2015', vastgesteld op 24 november 2014, schrijft gemeente Hardinxveld-Giessendam: 'Vormen van georganiseerde criminaliteit zijn de productie van en handel in drugs, mensensmokkel/-handel, internetcriminaliteit, wapenhandel. Gemeenten kunnen de bewegingsruimte voor deze vormen van criminaliteit inperken door bij beschikkings- en aanbestedingsprocedures kritisch te werk te gaan (BIBOB) en/of een integrale bestuurlijke aanpak van georganiseerde criminaliteit of specifieke branches daarbinnen vorm te geven. De Wet Bevordering Integriteitsbeoordelingen door het Openbaar Bestuur (Wet Bibob) is per 1 juli 2013 uitgebreid.' Er staat niet toegelicht welke beschikkings- en aanbestedingsprocedures de gemeente in verband brengt met internetcriminaliteit. Van Wamelen[18] onderzocht in 2018 welke bevoegdheden uit de Gemeentewet, Politiewet 2012 en Wet Bibob, een gemeente mogelijkheden geeft om een bijdrage te leveren aan de bestrijding van cybercrime. Zij concludeert over de wet Bibob dat er geen sprake is van het afgeven van vergunningen voor het bouwen of exploiteren in de virtuele wereld. 'Er kan enkel sprake zijn van het intrekken of het weigeren van een vergunning welke geldig is voor de fysieke wereld maar waarbij de aanvrager misbruik kan maken in de virtuele wereld. Een voorbeeld hierbij is het aanvragen van een vergunning voor een computercafé waarmee men strafbare feiten pleegt in de virtuele wereld.' Of gemeente Hardinxveld-Giessendam daarop het oog had, is ons niet gebleken. Tot slot vonden we bij één gemeente tekst die wijst op een gemeentelijke taak bij cybercrises (*work package* 6). In de notitie 'Veiligheidsbeleid Achtkarspelen en Tytsjerksteradiel: Feiligens yn Ferbûnens 2019-2022'[19] staat onder het kopje 'Overige aandachtspunten' bij 'cyberveiligheid': 'Lokaal zijn al een aantal initiatieven gestimuleerd in het kader van cyberveiligheid. Daarnaast is dit thema actueel in de crisisbeheersing. Dit blijft de komende periode de aandacht houden.' Concrete activiteiten staan niet genoemd.

4. Digitale veiligheid in beleid van de G4

Naast het onderzoek bij de selectie van 27 gemeenten (paragraaf 3) deden we hetzelfde bij de vier grootste gemeenten (G4: Utrecht, Den Haag, Rotterdam, Amsterdam). Ook wat we aantroffen op de websites van de G4 gespreken we per thema. Tabel 2 geeft een overzicht van de bevindingen.

Tabel 2: de G4 en hun aandacht in beleid voor de zes gemeentelijke work packages: (1) informatiebeveiliging in eigen huis, (2) regierol, (3) evenementenveiligheid, (4) monitoren internet, (5) maatregelen ivm ordehandhaving, (6) cybercrises

Gemeente	Provincie	Inwoners *	1	2	3	4	5	6

[18] S. van Wamelen, *De bevoegdheid van het gemeentebestuur in de virtuele wereld. Een onderzoek naar de bevoegdheid van het gemeentebestuur bij de strafrechtelijke strijd tegen cybercrime, op grond van de Gemeentewet, Politiewet 2012 en Wet Bibob,* Heerlen: Open Universiteit, 2018 (masterscriptie).

[19] https://www.t-diel.nl/organisatie-bestuur-t-diel/besluiten-van-het-college_43907/item/persbesluitenlijst-24-september-2019_44971.html, geraadpleegd 11 februari 2020.

1	Utrecht	Utrecht	347.483	x	x				x
2	's-Gravenhage	Zuid-Holland	532.561	x	x				x
3	Rotterdam	Zuid-Holland	638.712	x	x		x		x
4	Amsterdam	Noord-Holland	854.047	x	x		x		x
	TOTAAL			4	4	0	2	0	4

* Ministerie van Sociale Zaken en Werkgelegenheid: https://www.uitvoeringvanbeleidszw.nl/subsidies-en-regelingen/verander opgave-inburgering-pilots/tabel-aantal-inwoners-gemeenten-per-1-januari-2019, geraadpleegd op 02-02-2020.

Informatiebeveiliging

Alle G4-gemeenten besteden ruim aandacht aan privacybeleid en informatiebeveiliging (*work package* 1), steeds met de AVG als voornaam vertrekpunt. De G4 heeft aparte functionarissen belast met privacy en gegevensbescherming. Den Haag heeft bijvoorbeeld een 'Functionaris Gegevensbescherming' waarheen inwoners zich per mail kunnen wenden.[20] Artikel 7 lid 1 van de Privacyverordening gemeente Utrecht luidt: 'Elk organisatieonderdeel heeft een contactpersoon die belast is met de coördinatie en uitvoering van het privacy- en beveiligingsbeleid van het betreffende organisatieonderdeel.' Rotterdam heeft een functionaris gegevensbescherming en privacy officers. Tegelijk stelt deze gemeente nadrukkelijk dat het lijnmanagement verantwoordelijk is en de privacy officer dat ondersteunt.[21] Amsterdam heeft een Commissie Persoonsgegevens Amsterdam die de gemeente adviseert over haar privacybeleid en de uitvoering daarvan.[22] In het licht van onze inventarisatie volstaat het hier om te concluderen dat de bescherming van eigen gegevens ('eigen huis op orde') in de G4 een duidelijk gearriveerd onderwerp is, met beleid, functionarissen en maatregelen. Net als bij de 27 eerder genoemde gemeenten geldt de AVG ook voor de G4 als belangrijk vertrekpunt.

Bij de gemeenten Den Haag en Rotterdam troffen we een webpagina over disclosurebeleid.[23] Verder vonden we, net als bij de overige gemeenten (paragraaf 3.2), geen informatie die toont dat de G4 proactief werken aan weerbaarheidsprogramma's voor de eigen organisatie en medewerkers.

Regierol inzake digitale veiligheid

Alle G4-gemeenten zien een rol voor zichzelf bij het bevorderen van digitale veiligheid in de stad (*work package* 2). Het vergroten van de digitale weerbaarheid van burgers en (MKB-)bedrijven is voor alle vier een thema. Daarbij vallen termen zoals 'bewustwording' en 'voorlichting'. Het 'Integraal veiligheidsplan 2019 – 2022' van Utrecht geeft de gedeelde visie beknopt weer: 'De maatschappelijke weerbaarheid blijft achter bij de groeiende dreiging van cybercriminaliteit. Bewustwording is nodig zodat we de weerbaarheid vergroten en de digitale veiligheid zoveel als mogelijk kunnen waarborgen.'[24] Ook het bevorderen van (publiek-private) samenwerking tegen cybercrime komt in de plannen voor, evenals zorg voor digitale veiligheid van vitale infrastructuur, met in Rotterdam

[20] https://www.denhaag.nl/nl/verklaring-inzake-gegevensbescherming.htm#wijziging-verklaring-inzake-gegevensbescherming, geraadpleegd 17 februari 2020.

[21] https://www.rotterdam.nl/bestuur-organisatie/uw-gegevens/Privacybeleid-gemeente-Rotterdam_2018-0517.pdf, geraadpleegd 17 februari 2020.

[22] https://www.amsterdam.nl/bestuur-organisatie/organisatie/overige/adviesraden/commissie-persoonsgegevens-amsterdam/, geraadpleegd 17 februari 2020.

[23] https://www.denhaag.nl/nl/algemeen/responsible-disclosure.htm en https://www.rotterdam.nl/bestuur-organisatie/responsible-disclosure/; beide geraadpleegd 2 maart 2020.

[24] *Een veilige stad voor iedereen. Integraal Veiligheidsplan 2019-2022.* (Beleidsnota van de gemeente Utrecht, z.j.), p. 6.

speciale aandacht voor de digitale veiligheid van de haven.[25] Voorbeelden van concrete (voorgenomen) activiteiten om de digitale veiligheid te bevorderen, zijn:

- Utrecht: '1. Opbouwen stedelijk weerbaarheidsbeeld digitale veiligheid. 2. Beter zicht op daders, slachtoffers en incidenten; 3. Vergroten van het bewustzijn over digitale risico's.'[26];
- Den Haag: 'we stimuleren de kennisvergroting in het MKB'[27]; inrichten van een 'Cyber Resilience Exchange Platform' waar 'burgers, bedrijven en overheden informatie kunnen delen over cyberincidenten, hun impact en manieren om ze op te lossen en te voorkomen. (...) Het verhogen van de digitale weerbaarheid van kwetsbare groepen. Versterken van kennisontwikkeling en publiek-private innovatiesamenwerking op het gebied van cybersecurity.'[28];
- Rotterdam: 'het laten uitvoeren van (wetenschappelijk) onderzoek, het opstellen van een dreigingsbeeld, het organiseren van de juiste technische kennis en het volgen van opleidingen'; in 2019 is voor het eerst 'de Veiligheidsmonitor uitgezet inclusief cybercrime gerelateerde vragen'[29];
- Amsterdam: veiligheidseisen stellen aan Internet of Things-apparaten; bewustwordingscampagnes voor weerbaarheidsvergroting, digitaal weerbaarder maken van met name jeugd, private organisaties en maatschappelijke instellingen, onderzoek doen naar cybercriminaliteit, aandacht voor cybercrime opnemen in de Toolbox voor Veilig Ondernemen, uitvoereen phishing test bij het MKB, verbeteren aangifteproces cybercrime.[30]

In Rotterdam en Den Haag is 'digitaal' een integraal onderdeel van het gemeentelijk veiligheidsbeleid. In het Rotterdamse *Veiligheidsprogramma 2018-2023* komt 'cyber' zeventien maal voor, in het Haagse *Integraal Veiligheidsplan 2019-2022* 28 maal.[31] Zelfs de titel van het Rotterdamse beleidsplan ('Veilig@Rotterdam') verraadt aandacht voor digitaal. Amsterdam lanceerde in november 2019 een aparte Agenda Digitale Veiligheid. Daarin schrijft burgemeester Halsema in het voorwoord: 'Als burgemeester van deze stad ben ik verantwoordelijk voor de openbare orde en veiligheid, waaronder ook de virtuele openbare ruimte.'[32] Dat is een vèrstrekkende uitspraak, om twee redenen. Ten eerste breidt de uitspraak de gemeentelijke verantwoordelijkheid uit tot een gebied waarvan de grens niet vaststaat. Ten tweede, en daar gaat het ons hier om, is het een schetsmatige

---

25 *Een veilige stad voor iedereen. Integraal Veiligheidsplan 2019-2022.* (Beleidsnota van de gemeente Utrecht, z.j.); *Gemeente Den Haag. Integraal Veiligheidsplan Den Haag 2019-2022* (Beleidsnota van de gemeente Den Haag z.j.); *Veilig@Rotterdam. Veiligheidsprogramma 2018-2023* (Beleidsnota van de gemeente Rotterdam 2018); *Agenda Digitale Veiligheid Gemeente Amsterdam* (Beleidsnota van de gemeente Amsterdam 2019).

26 *Een veilige stad voor iedereen. Integraal Veiligheidsplan 2019-2022.* (Beleidsnota van de gemeente Utrecht, z.j.), p. 41.

27 *Samen voor de stad. Coalitieakkoord 2019-2022.* (Beleidsnota van de gemeente Den Haag 2019), p. 15.

28 Ibidem, p. 44.

29 *Veilig@Rotterdam. Veiligheidsprogramma 2018-2023* (Beleidsnota van de gemeente Rotterdam 2018), p. 28; https://www.watdoetdegemeente.rotterdam.nl/begroting2020/programmas/openbare-orde-en-veilighe/opnebare-orde-en-veilighe/, geraadpleegd 17-02-2020.

30 Gemeente Amsterdam (2019) *Agenda Digitale Veiligheid Gemeente Amsterdam*. Amsterdam: Gemeente Amsterdam, p. 5, p.12-13, p.16.

31 Het Haagse plan telt 55 bladzijden met tekst en het Rotterdamse 32. Het aantal keren 'cyber' per pagina met tekst is in Den Haag dus 0,51 en in Rotterdam 0,53.

32 Een primeur is deze uitspraak niet want op 1 november 2016 trad in de Belgische gemeente Jette een nieuw Algemeen Politiereglement in werking waarvan artikel 1 luidt: 'Het huidige reglement is van toepassing op de openbare ruimte en iedere reële of virtuele, voor het publiek toegankelijke ruimte. Bron: https://jetteadm.irisnet.be/nl/pdf/veiligheid/algemeen-politiereglement, geraadpleegd 31 januari 2020. De woorden 'cyber', 'virtuele' en 'internet' komen in de rest van het reglement niet voor.

toeëigening van een verantwoordelijkheid die vervolgens niet staat uitgewerkt in een stelsel van concreet bestuur voor de virtuele ruimte.

De bevindingen overziend constateren we ten eerste dat de G4 een regierol inzake digitale veiligheid hebben omarmd als integraal onderdeel van hun gemeentelijke verantwoordelijkheid. Over de doelen bestaat grote overeenstemming: de weerbaarheid van burgers en bedrijven moet omhoog. We zien vervolgens een diversiteit aan voorgenomen activiteiten. Die diversiteit geeft niet direct een beeld van een uitgekristalliseerd coherent beleid. Dat is begrijpelijk daar het een nieuw beleidsterrein betreft dat nog volop in ontwikkeling is. Ook dat kennisbehoeften worden uitgesproken onderstreept dat de G4 zich hier in een ontwikkelfase bevinden.

Evenementenveiligheid en monitoren van internet.

Over de digitale veiligheid van evenementen (*work package* 3) kunnen we kort zijn: ook bij de G4 hebben we daarvoor geen aandacht geconstateerd in het bestudeerde materiaal.

Wel zagen we bij Rotterdam en vooral Amsterdam aandacht voor monitoren van wat op internet gaande is (*work package* 4). In het Rotterdamse veiligheidsprogramma 2018-2023 staat: 'Om mensenhandel en uitbuiting in de (illegale) prostitutie uit te bannen, wordt de huidige prostitutie- en mensenhandel aanpak herijkt, *waarbij extra aandacht uitgaat naar het internet* en de fenomenen arbeids- en criminele uitbuiting en slecht werkgeverschap.' (onze nadruk).[33]

In de Amsterdamse Agenda Digitale Veiligheid speelt monitoren van internet een grotere rol. Onder de kop 'Democratie en bestuurlijke stabiliteit' komt aan bod dat mensen soms beperkt geïnformeerd zijn (informatiebubbels) en te maken krijgen met nepniews. De gemeente wil nepnieuws in beeld brengen en afzwakken dan wel corrigeren. 'De aanpak moet gericht zijn in het versterken van de monitoring en mitigatie capaciteit van de gemeente door het aanleggen van een informatie-infrastructuur die dieper in de vezels van de Amsterdamse (sub)gemeenschappen doordringt. Dit om beter te kunnen monitoren, effectiever informatie te verspreiden en beter te kunnen reageren.'[34] (Gemeente Den Haag uit in zekere zin ook haar zorg aangaande nepnieuws maar kiest voor een andere aanpak. Ze schrijft in haar coalitieakkoord over 'goed burgerschap' en stelt dat in het onderwijs aandacht moet worden besteed aan de vraag hoe je digitale informatie goed beoordeelt.[35]) Een andere toepassing van monitoren ziet Amsterdam bij de aanpak van illegale hotels/pensions: 'Het aantal controles wordt opgevoerd, internetonderzoek wordt uitgebreid en de juridische aanpak verstevigd.'[36] Eveneens bij handhaving op het water zet de gemeente monitoring in: 'De Nota Varen deel 1 vermeldt dat de handhaving op het water uitgebreid moet worden en dat deze met het digitaal monitoren van vaarbewegingen slimmer en gerichter kan worden ingezet.'[37]

Bij gemeente Utrecht vinden we geen verwijzingen naar monitoring maar de 'Privacyverordening gemeente Utrecht' lijkt hiervoor wel regels te stellen. Artikel 7 over 'Big data en tracking' stelt onder meer dat big data-gegevens door de gemeente uitsluitend mogen 'worden verzameld, opgeslagen en gedeeld, als ze niet herleidbaar zijn tot een persoon' en alleen dan wanneer gebruik wordt gemaakt van 'brongegevens die door daartoe geautoriseerde personen zijn verzameld'. Big

[33] *Veilig@Rotterdam. Veiligheidsprogramma 2018-2023* (Beleidsnota van de gemeente Rotterdam 2018), p. 20.
[34] *Agenda Digitale Veiligheid Gemeente Amsterdam* (Beleidsnota van de gemeente Amsterdam 2019), p. 22.
[35] *Samen voor de stad. Coalitieakkoord 2019-2022.* (Beleidsnota van de gemeente Den Haag 2019), p. 19.
[36] *Agenda Digitale Veiligheid Gemeente Amsterdam* (Beleidsnota van de gemeente Amsterdam 2019), p. 16.
[37] *Gemeente Amsterdam Begroting 2020* (Beleidsnota van de gemeente Amsterdam, 2019), p. 404.

data gebruiken om over personen informatie te vergaren, bijvoorbeeld over kamerverhuur, lijkt niet zomaar in overeenstemming te brengen met deze privacyverordening.

Maatregelen voor ordehandhaving en Cybercrises

Work package 5 betreft het nemen van maatregelen indien online activiteiten de offline openbare orde in de gemeente (dreigen te) verstoren. De gemeente Utrecht noteert in relatie daarmee: 'Een goede voorbereiding op de gevolgen die cybercriminaliteit kan hebben op de openbare orde in relatie tot crisisbeheersing en maatschappelijke onrust is essentieel.' De zinsnede 'Een goede voorbereiding is essentieel' beoordelen we echter niet als een verwijzing naar (voor)genomen maatregelen (zie paragraaf 3.1). Bij de andere leden van de G4 treffen we eveneens geen verwijzingen naar maatregelen tegen een (dreigende) ordeverstoring die wordt aangejaagd vanuit de digitale wereld. Gemeenten Den Haag verwoordt de gedeelde gemeentelijke handelingsverlegenheid in het *Integraal Veiligheidsplan Den Haag 2019-2022*: 'Op het gebied van openbare orde en crisisbeheersing in het digitale domein bestaat, ook landelijk, nog veel onduidelijkheid ten aanzien van de bevoegdheden en instrumenten die de burgemeester tot haar beschikking heeft of zou moeten hebben. Het klassieke instrumentarium is immers niet (specifiek) toegesneden op de digitale wereld. Daarnaast is het de vraag op welk schaalniveau en vanuit welke rollen en verantwoordelijkheden, bevoegdheden en instrumenten interventies het best kunnen worden georganiseerd: de digitale wereld is mondiaal en beperkt zich zeker niet tot de gemeentegrenzen. De komende periode zal er geïnvesteerd worden in het in kaart brengen van stakeholders en relevante netwerken, gericht op vergroting van de weerbaarheid van de stad op deze punten.'[38] Concrete maatregelen ontbreken ook hier. Op het gebied van cybercrises (*work package 6)* zijn de gemeenten verder op weg.

Gemeente Utrecht schrijft in haar 'Integraal Veiligheidsplan 2019-2022' als een te ondernemen activiteit het 'optimaal voorbereiden op cybercrises'.[39] In haar begroting voor 2020 staat: 'Daarnaast treffen we voorbereidingen op het bestrijden van een cybercrisis met gevolgen voor de (fysieke) veiligheid van de stad. Omdat het niet de vraag is òf er zich op dit vlak een crisis gaat voordoen, maar het de vraag is 'wanneer' deze zich een keer aandient, dienen wij ons daarop voor te bereiden door op voorhand beelden te vormen van mogelijke gevolgen en te treffen maatregelen. (...) Dit doen we samen met de vier grote gemeenten en regionale veiligheidspartners.'[40] Gemeente Den Haag legt ook een verband tussen cyber en crises: 'Steeds meer onderwerpen op het gebied van veiligheid krijgen te maken met een digitale component. Zo kunnen problemen ten aanzien van de openbare orde en veiligheid ontstaan in het digitale domein, manifesteert criminaliteit zich steeds vaker via het internet en vormt cyber een risico op het gebied van crisisbeheersing.[41] Als concrete maatregel noemt Den Haag het in G4-verband ontwikkelen van een Handreiking Cybergevolgbestrijding (CGB). 'De handreiking moet duidelijkheid geven over de rolverdeling bij dergelijke incidenten en over de instrumenten waarover het bestuur in die gevallen beschikt. Verder zal duidelijk worden welk netwerk van partners nodig is om dergelijke crises effectief te beteugelen.' [42] Rotterdam schrijft in haar Veiligheidsprogramma 2018-2023: 'Grootschalige cyberincidenten kunnen een grote impact hebben op de openbare orde en (fysieke) veiligheid van onze stad. Daarom wordt

[38] *Integraal Veiligheidsplan Den Haag 2019-2022.* (Beleidsplan van de gemeente Den Haag z.j.), p.7.

[39] Een veilige stad voor iedereen. Integraal Veiligheidsplan 2019-2022. (Beleidsnota van de gemeente Utrecht, z.j.), p. 41.

[40] https://utrecht.begroting-2020.nl/p24407/prestaties, geraadpleegd 24 februari 2020.

[41] *Integraal Veiligheidsplan Den Haag 2019-2022.* (Beleidsplan van de gemeente Den Haag z.j.), p.6.

[42] Ibidem, p.43.

ingezet op (nieuwe vormen van) crisisbeheersing. Daardoor zijn we met alle crisispartners voorbereid op een cybercrisis of een crisis met een cybercomponent.'[43] In haar Agenda Digitale Veiligheid besteedt ook Amsterdam aandacht aan cybercrises. De gemeente wil goed voorbereid zijn en 'beschikken over de juiste middelen en communicatielijnen om (de gevolgen van) een cybercrisis te beheersen' en is daarom 'gestart met het opzetten van een plan van aanpak.'[44] De gemeente gaat er voor zorgen 'dat er uiterlijk op 1 januari 2021: a) een crisisplan is waarin o.a.: wat te doen, door wie, waarmee in geval van een digitale calamiteit door uitval of criminaliteit. Dat plan is dan bij voorkeur tenminste één keer geoefend. Het bestaat uit onder meer noodscenario's en communicatie strategieën en middelen;'[45] Dat doet Amsterdam niet alleen. 'Bij crisisbeheersing en incident-management vraagt een cyberverstoring om de inrichting van een proces dat zich richt op het voorkomen van nieuwe risico (gevolgen) en het treffen van adequate maatregelen bij het optreden daarvan. (...) Samen met de G4 en het Ministerie VenJ (sic) is er opdracht verstrekt aan adviesbureau Berenschot om een cybergevolgbestrijding (CGB) op te stellen. Hieronder worden alle activiteiten verstaan die worden ontplooid om de situatie te normaliseren nadat een digitale verstoring heeft plaatsgevonden.'[46] Het beeld dat uit de teksten oprijst is dat de G4 onderkennen dat een cybercrisis een aparte aanpak vergt, dat de G4 dit onderwerp hebben opgepakt in samenwerking met relevante partners, en dat een concrete uitwerking nog gerealiseerd moet worden.

5. Beperkingen, conclusies en discussie

5.1 Beperkingen

We verkenden wat gemeenten (zeggen te) doen aan digitale veiligheid. Het geschetste beeld is geordend volgens zes door ons onderscheiden gemeentelijke *work packages* en gebaseerd op wat we daarover aantroffen op 31 gemeentelijke websites en de direct daaraan gelinkte documenten (zie ook paragraaf 3.1). Deze aanpak kent enkele beperkingen. Ten eerste hebben we de G4 wel compleet bestudeerd maar van de overige 351 gemeenten een steekproef van 27 getrokken, waarvan we niet weten hoe representatief die is waar het gaat om beleid inzake digitale veiligheid. Ten tweede is wat te lezen valt op een gemeentelijke website niet gelijk aan wat er door die gemeente aan activiteiten wordt ontplooid. Mogelijk is dat laatste minder, maar het kan ook meer zijn. Zo merkten we in 2019 op dat gemeente Maassluis bijeenkomsten tegen cybercrime organiseert,[47] terwijl we dat niet terugzien in onderhavige inventarisatie (tabel 1). Strikt genonen toont het door ons geschetste beeld dus niet wat een gemeente doet maar wat een gemeente op haar website zègt te doen, en dat kan meer of minder zijn dan wat de gemeente werkelijk doet. We vatten de op de website gemelde acties inzake digitale veiligheid vooralsnog op als indicatie van gemeentelijke activiteit omdat in beleidsstukken genoteerde voornemens niet zomaar langdurig onuitgevoerd kunnen blijven, maar we hebben de uitvoering niet gecheckt. Ten derde kunnen we informatie hebben gemist. We hebben bij elke gemeente gezocht naar een veiligheidsbeleidsplan, coalitieakkoord, begroting, informatieveiligheidsbeleidsplan en een evenementenbeleidsplan. Vaak vonden we een document in pdf-formaat, soms stond tekst (bv. een begroting) verspreid over

[43] *Veilig@Rotterdam. Rotterdamse veiligheidsprogramma 2018-2023.* (Beleidsnota van de gemeente Rotterdam, 2018), p. 28.

[44] *Agenda Digitale Veiligheid Gemeente Amsterdam*. (Beleidsnota gemeente Amsterdam 2019), p. 6.

[45] ibidem, p. 19.

[46] ibidem, p.20.

[47] W. Stol & W. Bantema 'De gemeente en de digitaal veilige stad', in: J.W. Sap & E. Kolthoff (red.) *De veilige stad als collectief doel,* Nijmegen: Ars Aequi Libri 2019, p. 124.

verschillende pagina's van de website. Evenementenbeleidsplannen zagen we het minst omdat evenementenbeleid voor de websitebezoeker vaak is geoperationaliseerd als aanvraagformulier. We vulden niet bij elke gemeente zo'n formulier compleet in. Ondanks de beperkingen geven onze bevindingen wel een beeld van wat er leeft binnen gemeenten. Vermoedelijk is het gemeentelijke denken over digitale veiligheid verder dan de websites tonen, maar op hoofdlijnen laten de resultaten wel enkele conclusies toe over waar gemeenten staan in hun ontwikkeling inzake beleid en maatregelen aangaande digitale veiligheid.

5.2 Conclusies en discussie

Ons vertrekpunt waren zes gemeentelijke *work packages* inzake digitale veiligheid: (1) wat informatiebeveiliging betreft het eigen huis op orde hebben, (2) andere actoren stimuleren in digitale veiligheid ('regierol'), (3) zorgen voor de digitale veiligheid van evenementen, (4) zich online informeren over mogelijk ophanden zijnde ordeverstoringen ('monitoren'), (5) maatregelen nemen tegen online activiteiten die de offline openbare orde in de gemeente (dreigen te) verstoren, (6) maatregelen nemen bij cybercrises. Deze zes komen achtereenvolgens aan bod.

(1) Informatiebeveiliging. Een eerste conclusie is dat het *work package* 'informatiebeveiliging' volop aandacht krijgt: alle bezochte gemeenten noteren activiteiten op dat vlak. De formele regelingen dienaangaande, met name de AVG, worden meestal als vertrekpunt genoemd. Sommige gemeenten vermelden een responsible disclosure beleid. De eind 2018 door het Nationaal Cyber Security Centrum (NCSC) gepresenteerde term 'Coordinated Vulnerability Disclosure'[48] kwamen we daarbij overigens niet tegen, wat zou kunnen betekenen dat de bewuste gemeenten de ontwikkelingen niet nauwlettend hebben gevolgd. Informatiebeveiliging is dan wel een gearriveerd onderwerp en omgezet in tal van concrete beleidsvoornemens, onze verkenning geeft tegelijk de indruk dat gemeenten in hun beleid geen al te grote plek inruimen voor het (pro)actief vorm geven aan de digitale weerbaarheid van de organisatie en haar medewerkers.

(2) Regierol. Een tweede conclusie is dat ná informatiebeveiliging de regierol inzake digitale veiligheid het vaakst naar voren komt. Met name het middels voorlichting stimuleren van digitale weerbaarheid van burgers en bedrijven komt geregeld terug. Alle G4-gemeenten maken melding hiervan, alsook 6 van de 27 andere bezochte gemeenten. Eerder konden we ook al eenvoudig enkele voorbeelden geven van gemeenten die zich manifesteren op het gebied van cybercrimebestrijding: Den Helder, Leeuwarden, Maassluis en Scherpenzeel haalden daarmee de pers.[49] Andere activiteiten dan voorlichting zien we vooral genoemd in de G4, zoals het vergroten van de eigen kennis over de digitale veiligheidsproblematiek en het stellen van veiligheidseisen aan IoT-apparaten. Over het geheel genomen is onze conclusie dat de regierol aangaande digitale veiligheid als gemeentelijke taak is gearriveerd. Gemeenten willen bijdragen aan de maatschappelijke weerbaarheid tegen digitale dreigingen. Hoewel deze taak bij de meeste gemeenten nog niet onder woorden is gebracht (tabel 1) is de ontwikkeling zichtbaar. Dat alle G4-gemeenten deze taak duidelijk benoemen, onderstreept dat het menens is. Het is een níeuwe taak en twee bevindingen illustreren dat: a. de wens om kennis op te bouwen omtrent de digitale veiligheid in de eigen gemeente, b. het nog ontbreken van een uitgekristalliseerd coherent beleid. De landelijke overheid hoeft gemeenten niet meer te overtuigen van een rol op dit gebied maar kan hen nog wel helpen met het concreet invullen er van.

(3) Evenementen. Een derde conclusie is dat er meer zorg van de nationale overheid mag uitgaan naar de gemeentelijke verantwoordelijkheid inzake de veiligheid van evenementen. Een

[48] *Coordinated Vulnerability Disclosure: de Leidraad* (Beleidsnota van het ministerie van J&V 2018)

[49] W. Stol & W. Bantema, a.w., 2019, p. 123-130

veilig evenement is vandaag de dag ook een digitaal veilig evenement. Dit is bij gemeenten nog geenszins in beleid gearriveerd. Een 'digitaal Haaksbergen'[50] is echter eenvoudig denkbaar want veel apparaten worden tegenwoordig digitaal aangestuurd. Bij de gemeente Amsterdam leeft de gedachte dat de gemeente eisen kan stellen aan IoT-apparaten. Dat idee kan worden uitgebreid met de notie dat de gemeente eisen kan stellen aan digitaal aangestuurde apparatuur die wordt gebruikt bij evenementen, en aan de digitale veiligheidsmaatregelen bij evenementen (bv. crowd management met digitale middelen). Het is een gemeentelijke verantwoordelijkheid waarbij een landelijke aanpak lijkt aangewezen om doublures te voorkomen.

(4) Monitoren. Gemeentelijke verantwoordelijkheden vergen dat de gemeente weet wat er leeft onder haar inwoners, bedrijven en andere organisaties. Speciaal moet zij zich informeren over mogelijk ophanden zijnde ordeverstoringen. Dat houdt ook in het online 'monitoren' van wat er binnen de gemeente speelt. We hebben dat als vierde work package opgevoerd. Maar hier is een dilemma. Uit work package 1 weten gemeenten dat zij een zorg hebben voor de bescherming van persoonsgegevens en dus de privacy van burgers. Het 'monitoren' van wat in de gemeente gaande is, kan met de privacybescherming op gespannen voet komen te staan. Van gemeenten wordt hier dus een balanceeract gevraagd tussen enerzijds 'weten wat er speelt' en anderzijds de privacybescherming op basis van artikel 8 EVRM en de AVG. We troffen geen beleid aan waarin een gemeente dit dilemma benoemt en een te bewandelen weg uitstippelt. Rotterdam geeft aandacht aan internet bij de aanpak van mensenhandel en uitbuiting in de (illegale) prostitutie; Amsterdam noemt online monitoring bij de aanpak van illegale hotels/pensions en de handhaving van vaarbewegingen. Tevens wil Amsterdam monitoring inzetten om nepnieuws op te sporen en tegen te gaan, 'door het aanleggen van een informatie-infrastructuur die dieper in de vezels van de Amsterdamse (sub)gemeenschappen doordringt. Dit om beter te kunnen monitoren, effectiever informatie te verspreiden en beter te kunnen reageren.'[51] Het laatste voornemen is van een andere orde dan het monitoren voor ordehandhaving, want het gaat in de richting van het monitoren ter identificatie van ondeugdelijke opvattingen dan wel onjuiste interpretaties van feiten, en het vervolgens corrigeren van die standpunten. Tegelijk staat in dezelfde Amsterdamse *Agenda Digitale Veiligheid*: 'Daar waar Amsterdam bekend staat om zijn openheid, vrijheid, diversiteit en inclusiviteit is ook nadrukkelijk aandacht voor een veilige en open digitale samenleving in Amsterdam.' Het coalitieakkoord meldt: 'In onze stad zijn individuele vrijheid en vrijheid van meningsuiting een groot goed. Dat koesteren en verdedigen we. Amsterdam biedt altijd ruimte voor het vrije woord, creativiteit en ondernemerschap, dat zit in de genen van de stad.' De vraag is nu hoe de door de gemeente gekoesterde 'Amsterdamse vrijheid' zich verhoudt tot de gemeentelijke ambitie om onjuiste opvattingen van Amsterdamse subgemeenschappen te corrigeren.

Het onbreekt in gemeenten aan beleid waarin 'online bijhouden wat er speelt' vorm krijgt in balans met het recht op privacy. In het strafrecht is daaraan veel aandacht besteed vanwege het toepassen van opsporingsbevoegdheden in een digitale omgeving. Gemeenten zouden zijn gebaat bij een soortgelijk debat over bestuurlijke verantwoordelijkheden en bevoegdheden in een digitale samenleving, in relatie tot artikel 8 EVRM. De vraag hoe nepnieuws kan worden tegengegaan en

[50] In Haaksbergen reed op 28 September 2014 een zogenoemde monstertruck bij een demonstratie, waarvoor de gemeente vergunning had verleend, het publiek in met drie doden en zo'n 30 gewonden tot gevolg. Kernelementen in de discussie over de oorzaak zijn: technische problemen met de besturing, inadequate reactie van de bestuurder, onvoldoende veiligheidsmaatregelen geëist in de verleende vergunning.

[51] *Agenda Digitale Veiligheid Gemeente Amsterdam* (Beleidsnota van de Gemeente Amsterdam 2019), p. 22.

waar de grenzen liggen, kan onderdeel zijn daarvan. Afgaande op de websites zijn gemeenten het niet op voorhand met elkaar eens. Den Haag bijvoorbeeld bestrijdt nepnieuws liever via educatie.[52]

(5) Ordehandhaving. Ordeverstoringen worden vandaag de dag niet zelden veroorzaakt of gestimuleerd vanuit een digitale omgeving. Voor gemeenten is de vraag of zij in zo'n geval maatregelen kunnen nemen tegen de online 'aanjager' van de ordeverstoring en zo ja, hoe zij dat dan uitvoeren. We lazen daarover op de websites geen concrete ideeën. Onderzoek van Bantema e.a. liet zien dat het online inzetten van bestaande bevoegdheden tegen activiteiten die de openbare orde (dreigen te) verstoren, op verschillende juridische bezwaren stuit.[53] Uit ander onderzoek weten we dat gemeenten wel degelijk actie ondernemen tegen online activiteiten die de openbare orde (dreigen te) verstoren. Communicatie staat daarbij centraal. De gemeente nodigt bijvoorbeeld iemand die online een (illegaal) feest aankondigt uit voor een gesprek, of geeft voorlichting om valse beelden of nepnieuws van een tegengeluid te voorzien.[54] Maar in beleid zijn dergelijke handelingsopties nog niet neergeslagen. De gemeentelijke verantwoordelijkheid inzake de openbare orde en de transparantie die van overheidsoptreden mag worden verwacht, vergen dat dit wel gebeurt en dat gemeenten in hun beleidsstukken dus concrete plannen opnemen ter invulling van *work package* 5. Gemeenten dienen hieraan samen met landelijke partners zoals de ministeries van BZK en J&V, de VNG en het CCV vorm te geven. Waar kennis nog ontbreekt, bijvoorbeeld over de juridische (on)mogelijkheden van bepaalde maatregelen of over de effectiviteit er van, is vervolgonderzoek gewenst.

(6) Cybercrises. Dat crises net zoals ordeverstoringen een online oorzaak kunnen hebben én dat die cybercrises een eigen aanpak vergen, is bij de G4 zichtbaar. Zij pakken dit onderwerp gezamenlijk op.[55] In de overige 27 gemeenten lezen we enkel bij Tytsjerksteradiel dat cyberveiligheid relevant is in relatie tot crisisbeheersing. 'Dit blijft de komende periode de aandacht houden.'[56] Het onderwerp is geland, de G4 plus het ministerie van J&V acteren op dit thema. Van daaruit kunnen plannen van aanpak worden verwacht die kunnen worden gedeeld met relevante partijen, waaronder de overige Nederlandse gemeenten.

In 2013 concludeerden Stol & Jansen: 'de rol van de burgemeester in de online veiligheidszorg, is een vergeten onderwerp'.[57] Dat is nu, zeven jaar later, significant anders. We startten deze bijdrage met zes gemeentelijke work packages voor digitale veiligheid. Op slechts twee daarvan is 'digitaal' nog hoegenaamd niet aangekomen in gemeentelijk beleid: de digitale veiligheid van evenementen en het nemen van maatregelen tegen online ordeverstorende activiteiten. Allereerst dient nu nader onderzoek te worden gedaan naar de (potentiële) problemen op deze twee gebieden en naar

---

52 *Samen voor de stad. Coalitieakkoord 2019-2022.* (Beleidsnota van de gemeente Den Haag), p. 19.

53 Bantema, W., S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.Ph. Stol (2018). *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld*. Den Haag: Sdu (reeks Politie en Wetenschap).

54 W. Bantema,S. Westers., S.A.J.,Munneke & W. Stol. *Niet bevoegd, wel verantwoordelijk? Handhavingsmogelijkheden bij online aangejaagde ordeverstoringen.* Boom Bestuurskunde: Den Haag (te verwachten); W. Bantema & W. Stol, 'Hoe de gemeente kan bijdragen aan een digitaal veilige samenleving' *Cahier Politiestudies*, (te verwachten), jrg. 12, nr. 3.

55 *Agenda Digitale Veiligheid Gemeente Amsterdam* (Beleidsnota van de gemeente Amsterdam 2019), p. 20.

56 *Veiligheidsbeleid Achtkarspelen en Tytsjerksteradiel: Feiligens yn Ferbûnens 2019-2022* (Beleidsnota van de gemeenten Achtkarspelen en Tytsjerksteradiel, z.j.).

57 W. Stol & J. Jansen (2013) 'Politie in een digitaliserende samenleving. Waar staat de politie nu, wat vraagt aandacht?', *IPA-actief* 2013, jrg. 7, nr. 342, pp. 11-17.

ervaringen die gemeenten, ondanks de geringe aandacht hiervoor in beleidsplannen, in de praktijk tóch al hebben opgedaan. Daarbij is aandacht vereist voor juridische aspecten (bevoegdheden, grondrechten) en naar de praktische haalbaarheid en de effectiviteit en van verschillende handelingsopties. Op het gebied van maatregelen tegen online activiteiten die de openbare orde (dreigen te) verstoren (*work package* 5) zijn in de praktijk al gemeentelijke activiteiten waar te nemen[58]; ten aanzien van de digitale veiligheid van evenementen (*work package* 3) geldt dat hun verantwoordelijkheid vereist dat gemeenten de eerste stappen gaan zetten. Bij verscheidene gemeenten is evenenementenveiligheid weliswaar een speerpunt in veiligheidsbeleid, maar vaak ten onrechte nog zonder aandacht voor digitale veiligheid.

[58] W. Bantema & S. Westers a.w.; W. Bantema & W. Stol a.w.