

# **Smart Safety & Security Talk: Bestuurlijk convenant Digitale Veiligheid**

Frank van Summeren



# Uitgangspunten onderzoek

## Belangrijke uitgangspunten NLCS

1. Centraal waar het kan, decentraal waar het moet
2. Groot helpt klein
3. De overheid geeft het goede voorbeeld



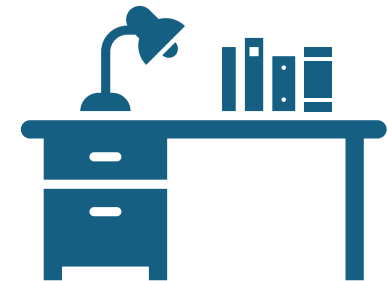
## Systeemuitdagingen uit bestuurlijk convenant

1. De vertaling van het fysieke veiligheidsstelsel naar het digitale veiligheidsstelsel (met verantwoordelijkheden, rollen, taken en bevoegdheden)
2. De informatiepositie van gemeenten voor de digitale veiligheid van hun eigen organisatie én van maatschappelijk relevante organisaties, burgers en ondernemers
3. De structurele financiering voor uitvoering van de NLCS op lokaal niveau



# Aanpak

- 100 publicaties (onderzoeksrapporten, evaluaties, handreikingen, enz.)
- Ruim 200 gesprekken met bestuurders van overheden.
- Gesprekken met ongeveer 60 stakeholders (werkzaam bij ministeries, provincies, gemeenten, politie, OM, WS, VR's, RIEC's, enz.).
- Consultatie bestuurlijke gremia (bestuur en veiligheid, informatiesamenleving, cyberburgemeesters, strategisch beraad, enz.)



# Onderzoeksrapport Cyberweerbaarheid binnen gemeentegrenzen

**CYBERWEERBAARHEID  
BINNEN  
GEMEENTEGRENZEN**

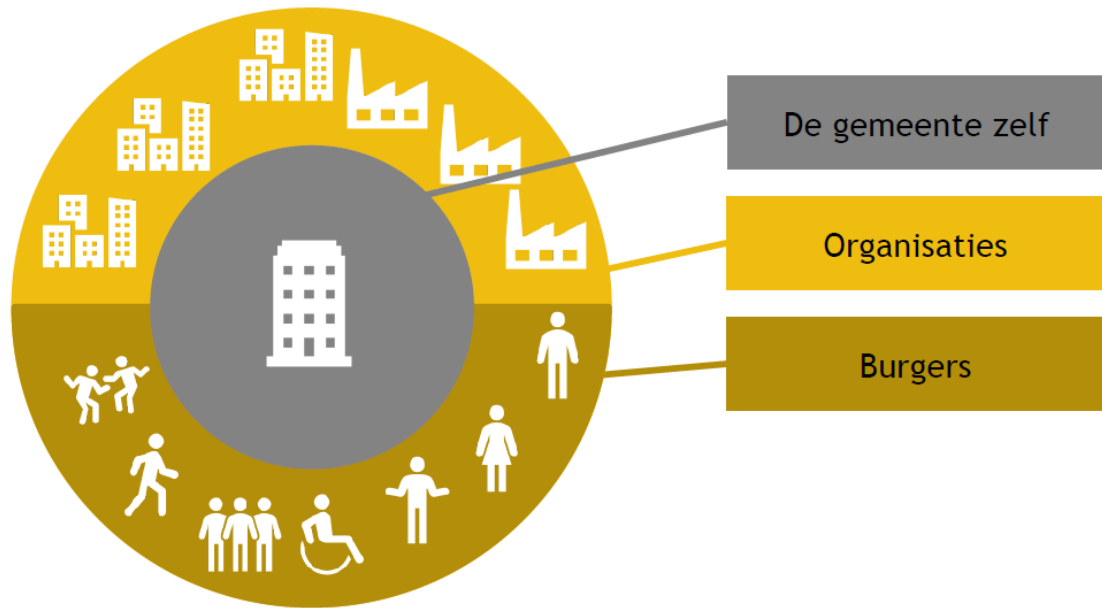
Uitwerking van het Bestuurlijk  
Convenant Digitale Veiligheid  
Gemeenten en het Rijk

Peter Obergsm  
Frank van Sambeeren  
29 augustus 2020

1



# Negen incidenttypen



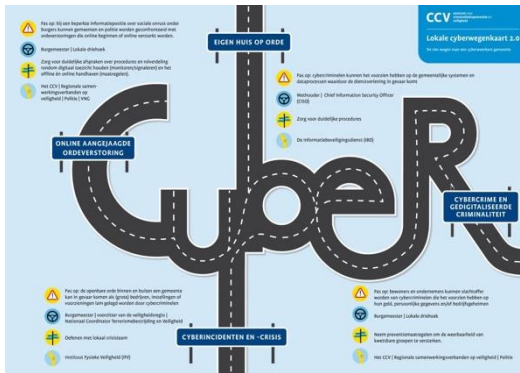
1. Incidenten m.b.t. gemeenteprocessen en -systemen

2. Incidenten bij instellingen met maatschappelijke impact
3. Incidenten met infrastructuur in de openbare ruimte (OT/IoT)
4. Misbruik van bedrijven voor criminele activiteiten
5. Digitale criminaliteit gericht op bedrijven

6. Misbruik van burgers voor criminele activiteiten
7. Digitale criminaliteit gericht op burgers
8. Lokaal daderschap digitale criminaliteit
9. Online ordeverstoring en desinformatie die leidt tot maatschappelijk onbehagen



# Vier incidentcategorieën



- A. Eigen huis op orde
- B. Cyberincidenten en crisis
- C. Cybercrime en gedigitaliseerde criminaliteit
- D. Online aangejaagde ordeverstoring

- A. Interne digitale veiligheid gemeenten
- B. Ontwrichting binnen de gemeentegrenzen door een cyberincident
- C. Cybercrime en gedigitaliseerde criminaliteit die zich binnen de gemeentegrenzen manifesteert
- D. Online aangejaagde ordeverstoringen binnen de gemeentegrenzen



Kenmerken

Verspreiding

Verbinding

Schaal

Tijd

Lokaliteit

Fysiek

Kenmerk

Digitaal

Voornamelijk geografisch

**Verspreiding**

Wijze waarop incidenten en crises opschalen

Ook multi-lokaal, multi-regionaal en multi-provinciaal

Veelal beperkt m.u.v. ketenafhankelijkheden

**Verbinding**

Mate van verbinding naar andere ketens en netwerken

Veel verbonden ketens en netwerken

Verloop biedt duidelijke indicatoren voor schaal

**Schaal**

Mate van voorspelbaarheid potentiële schaal

Minder voorspelbaar door onzichtbare indicatoren

Vaak sequentieel  
Tijd tussen besef en start Incident snel zichtbaar

**Tijd**

Wijze van verloop in de tijd

Ook simultaan  
Vrij plotseling  
Minder snel zichtbaar

Duidelijkheid over locatie assets

**Lokaliteit**

Helderheid over locatie van assets

Onduidelijkheid over locatie assets



voornamelijk fysiek

# Verspreiding

ook multi-lokaal/  
regionaal/  
provinciaal



*Cybersecurityincidenten kunnen grillig  
opschalen en laten zich niet tegenhouden  
door geografische grenzen*



beperkt  
m.u.v.  
ketenafhankelijkheden

# Verbinding

veel verbonden  
ketens en  
netwerken



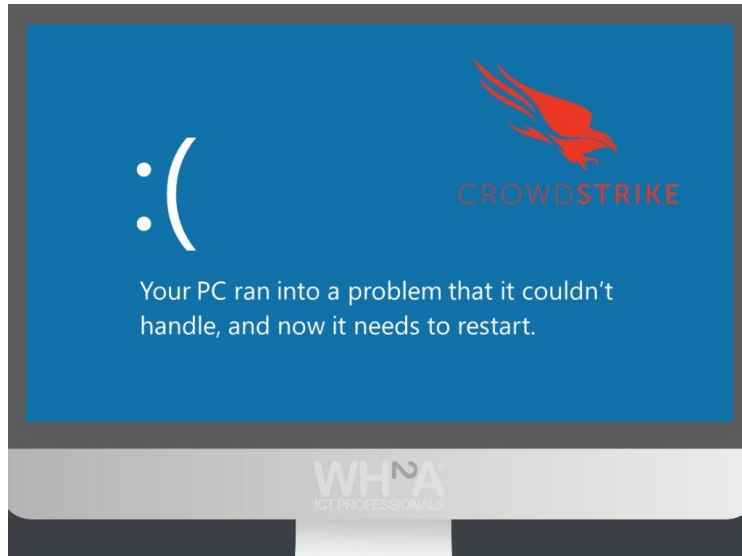
*Een kwetsbaarheid bij één product van een softwarefabrikant kan leiden tot een breed verspreid en langdurig cybersecurityincident*



duidelijke  
indicatoren  
voor schaal

# Schaal

ook multi-lokaal/  
regionaal/  
provinciaal



- *Cybersecurityincidenten kunnen zich kenmerken door onvoorspelbaarheid ten aanzien van de opschaling*
- *De impact van een foutieve automatische update had grote en zichtbare gevolgen*



vaak sequentieel  
tijd tussen besef & incident  
snel zichtbaar

# Tijd

ook simultaan  
vrij plotseling  
minder snel zichtbaar



*Een probleem in de 112-software  
leidt plotseling tot uitval met grote  
impact op de samenleving*



duidelijkheid  
over locatie assets

# Lokaliteit

onduidelijkheid  
over locatie assets



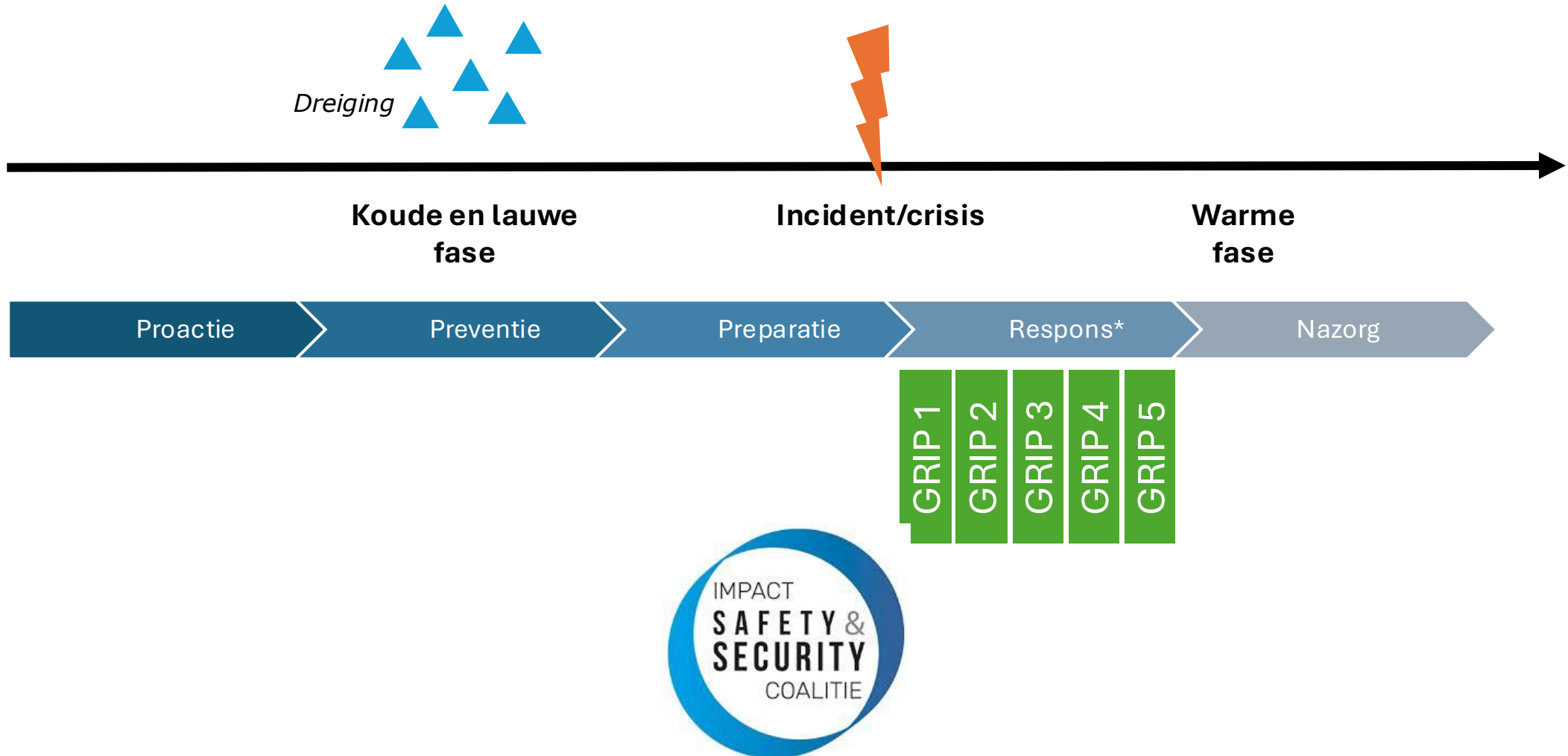
**Gijzelsoftware raakt  
Veiligheidsregio Noord- en Oost-  
Gelderland. 'Essentiële systemen  
werken nog wel'**



*Voor een organisatie is 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*



# Tijdslijn en veiligheidsketen



Koude en lauwe fase

Incident/crisis

Warme fase



Beleid

Uitvoering

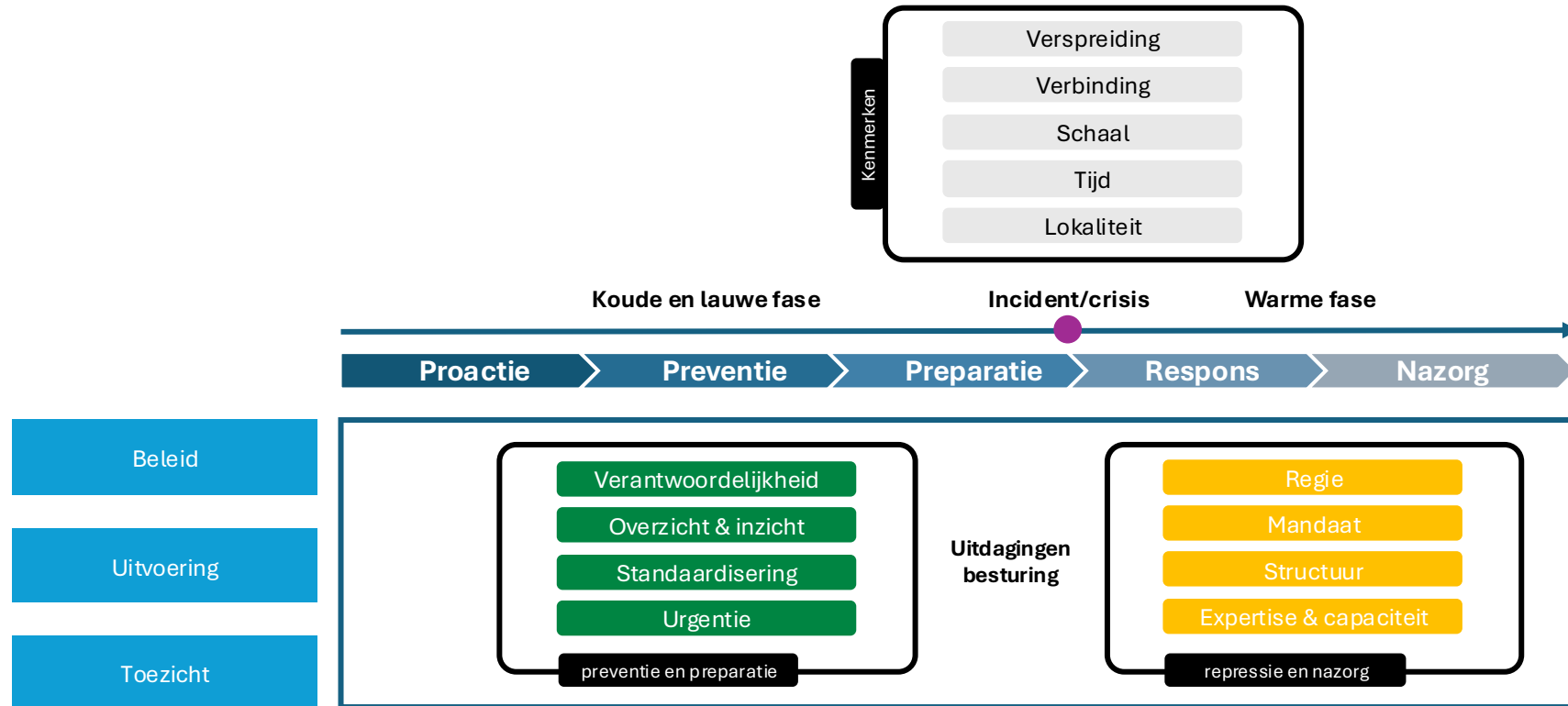
Toezicht

	Proactie	Preventie	Preparatie	Respons*	Nazorg
Beleid	het <b>wegnemen</b> van <b>structurele oorzaken</b> van onveiligheid	het nemen van <b>maatregelen vooraf</b> om de <b>risico's zo klein</b> mogelijk te houden en/of de mogelijke <b>gevolgen te beperken</b> indien deze zich toch voordoen	de <b>voorbereiding en informatie-positie</b> om adequaat te kunnen reageren op een incident of crisis	de daadwerkelijke <b>(gevolg)bestrijding</b> van incidenten en crises	al hetgeen nodig is om zo snel mogelijk naar een <b>'normale' situatie terug te keren</b> , <b>slachtoffers te ondersteunen</b> en te <b>leren</b> van een incident/crisis

De veiligheidsketen-methodiek wordt binnen gemeenten en veiligheidsregio's in het fysieke domein al breder ingezet en is daarom vanuit lokaal perspectief herkenbaar



# Digitale incidenten en impact besturing



Dimensie	Fysieke domein	Digitale domein	Oplosbaar
<b>Verantwoordelijkheid</b>	Taken, verantwoordelijkheden en rollen zijn helder vastgelegd en uitgewerkt (bijv. rol van burgemeester, veiligheidsregio, maar ook de eigen verantwoordelijkheid van burgers en organisaties).	Taken, verantwoordelijkheden en rollen zijn beperkt vastgelegd, veelal wel voor de Rijksoverheid. In het digitale domein ligt een groter deel van de rollen, taken en bevoegdheden bij organisaties zelf, maar ook bij leveranciers en producenten van digitale producten en diensten (bijv. cybersecurity bedrijven, MSSP's, techbedrijven, Internet Service Providers, telecom aanbieders, etc.).	Deels, er blijven veel typen organisaties betrokken
<b>Overzicht &amp; inzicht</b>	Organisaties hebben vaak een goed overzicht van hun belangrijkste fysieke assets en hoe deze beveiligd moeten worden. De (decentrale) overheid heeft tot op zekere hoogte een beeld van wat er in een regio, wijk, buurt of straat speelt en kan maatregelen nemen om de veiligheid te vergroten.	Organisaties hebben nog vaak weinig of beperkt overzicht van hun belangrijkste digitale assets en weinig of beperkt inzicht in de verdeling van verantwoordelijkheden voor hun veiligheid en beveiliging. De (decentrale) overheid heeft beperkt zicht op gedrag van gebruikers van het digitale domein en zeer beperkte mogelijkheden om de veiligheid te vergroten.	Deels, het overzicht blijft altijd minder goed dan in het fysieke domein
<b>Standaardisering</b>	Er zijn veel erkende best practices, voorschriften en standaarden voor preventie (bijv. brandmelders, keurmerken voor sloten, helmen in de bouw, etc.)	Er is nog weinig consensus over wat basismaatregelen zijn in het digitale domein, standaarden zijn nog volop in ontwikkeling en er is veel maatwerk.	Ja
<b>Urgentie</b>	Er is meer gevoelde urgentie rondom het voorkomen van, en voorbereiden op, incidenten en crisis in het fysieke domein, doordat dit type incidenten en crises beter voorstelbaar is, ze vaker zichtbaar zijn voor een breed publiek wanneer ze plaatsvinden, maar ook doordat er wettelijke verplichtingen zijn.	Beslismakers voelen soms minder urgentie bij het nemen van kostbare beslissingen ten aanzien van preventie en preparedness in het digitale domein, omdat we met dergelijke incidenten minder ervaring hebben, er minder wettelijke verplichtingen zijn en als ze plaatsvinden, ze minder zichtbaar zijn en de potentiële schade moeilijk is om in te schatten.	Ja

Dimensie	Fysieke domein	Digitale domein	Oplosbaar
Regie	Regie op incidentafhandeling en crisisbeheersing ligt primair bij de (decentrale) overheid, zoals gemeenten, veiligheidsregio's en hulpdiensten.	Verantwoordelijkheid voor incidentafhandeling en crisisbeheersing ligt deels bij publieke partijen, maar wel andere dan in het fysieke domein (bijv. nationale/sectorale CSIRT's). Private organisaties hebben ook een rol als het gaat om incident response (bijv. organisaties zelf of door hen ingehuurde cybersecuritybedrijven).	Ja
Mandaat	Als het incident/de crisis in de publieke ruimte plaatsvindt en/of onder de wettelijke bevoegdheden van de (decentrale) overheid valt, dan heeft deze een direct mandaat en directe mogelijkheden om te interveniëren.	Vaak kan de (decentrale) overheid niet rechtstreeks interveniëren in incidenten/crises bij bedrijven/burgers, omdat zij geen eigenaar is van de infrastructuur en/of cyberspace geen publieke ruimte is. Ze is dan afhankelijk van (samenwerking met) private partijen (bijv. MSSP's, Internet service providers, cybersecuritybedrijven, techbedrijven, etc.). Ook ontbreken wettelijke kaders en bevoegdheden die dit probleem (deels) kunnen oplossen.	Deels, door aanpassen wettelijk kader
Structuur	Er zijn beproefde structuren en protocollen aanwezig voor incidentafhandeling, informatie-uitwisseling en crisisbeheersing (bijvoorbeeld GRIP) en meldingen komen via een beperkt aantal paden binnen (bijvoorbeeld 112-melding).	Er zijn beperkte structuren en protocollen aanwezig voor incidentafhandeling, informatie-uitwisseling en crisisbeheersing en die richten zich voornamelijk op de Rijksoverheid. Ze zijn anders georganiseerd en er zijn andere actoren bij betrokken, zoals bijv. CISO's, of bedrijven zoals Internet Service Providers. Er zijn minder duidelijk gedefinieerde paden voor meldingen en voor opschaling.	Ja
Expertise & capaciteit	Er is vaak binnen (publiek en private) organisaties voldoende expertise en capaciteit aanwezig en die is meestal in-house beschikbaar, ook bij organisaties met een kleine omvang. Als dat niet het geval is, is de beschikbaarheid van expertise en capaciteit georganiseerd met/via netwerken buiten de eigen organisatie	Er is vaak beperkte expertise en capaciteit binnen organisaties aanwezig en deze is mede afhankelijk van de omvang van de organisatie. Als deze niet in-house beschikbaar en/of beperkt is, is deze vaak ook onvoldoende georganiseerd met/via netwerken buiten de organisatie. In het digitale domein is de afhankelijkheid van externe (private) organisaties en de Rijksoverheid voor de afhandeling van incidenten en crises sowieso veel groter.	Ja

# Meer dan honderd handreikingen, beleidsdocumenten en initiatieven geven zicht op de ontwikkeling van het landschap



↓ Categorieën	Koude en lauwe fase			Warme fase	
	Proactie	Preventie	Preparatie	Respons	Nazorg
<b>A</b> 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>B</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
<b>C</b> 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
<b>D</b> Online aangejaagde ordeverstoringen binnen de gemeentegrenzen	4, 9, 30, 37, 58, 70	12, 13, 72, 73, 74	72, 77	72	72

Er is voornamelijk **veel beleid** ontwikkeld voor de **koude en lauwe fase**



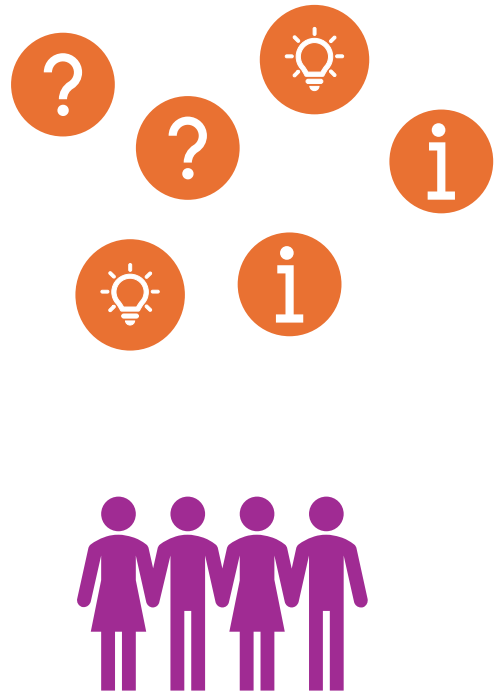
# Gemeenten vervullen taken in alle categorieën, ook in relatie tot de taken van andere stakeholders

Categorieën	Koude en lauwe fase			Warme fase	
	Proactie	Preventie	Preparatie	Respons	Nazorg
Interne digitale veiligheid gemeenten	A Strategische keuzes over aanpak	Taken krijgen met de NIS2 een wettelijk kader, maar worden op dit moment uitgevoerd o.b.v. de AVG en afgesproken beleid, namelijk de Baseline Informatiebeveiliging Overheid (BIO) <sup>24,32</sup>			
Ontwrichting binnen de gemeentegrenzen door een cyberincident	B Bevorderende rol t.a.v. cybeveiligheid		Gezamenlijk oefenen	Gevolgbestrijding indien de openbare orde en veiligheid ernstig in het geding is	Herstel en nazorg
Cybercrime en gedigitaliseerde criminaliteit die zich binnen de gemeentegrenzen manifesteert	C Voorlichting om awareness onder (kwetsbare) doelgroepen te vergroten	Beschikbaar stellen van tools, trainingen en/of ondersteuning om de cyberweerbaarheid van (kwetsbare) doelgroepen te bevorderen	Beschikbaar stellen van handreikingen hoe te handelen bij slachtofferschap van cybercrime of gedigitaliseerde criminaliteit	Gevolgbestrijding indien de openbare orde en veiligheid ernstig in het geding is	Verwijzen naar organisaties die kunnen ondersteunen bij slachtofferschap van cybercrime of gedigitaliseerde criminaliteit
D Online aangejaagde ordeverstoringen binnen de gemeentegrenzen	Voorlichting om awareness onder burgers te vergroten	Online aanwezigheid van lokaal gezag	Vorbereiden op mogelijke ongeregeldeheden	Treffen van maatregelen om de openbare orde te handhaven en herstel van de openbare orde	Ondersteuning aan slachtoffers

-  Taken die voortvloeien uit andere wettelijke taken
-  Rechtstreekse wettelijke taken



# De ontwikkeling van digitale veiligheid op de vier incidentcategorieën vraagt nadere uitwerking



A. Interne digitale veiligheid

B. Ontwrichting

C. Cybercrime & gedigitaliseerde criminaliteit

D. Online aangejaagde openbare-ordeverstoringen

**Breed herkend/erkend?  
Haalbaar?  
Realistisch?  
Wie invulling geven?**

In rapport:  
geïnterviewde **uitdagingen**  
voor besturing



# Conclusies en aanbevelingen landschap

## Conclusies

1. Op een gestructureerde manier in kaart brengen van het landschap is van belang is voor de bij dit onderwerp betrokken stakeholders.
2. Een nadere uitwerking is nodig 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.

## Aanbevelingen

1. Het landschap regelmatig (bijvoorbeeld tweejaarlijks) updaten.
2. In kaart te brengen welke concrete casuïstiek ten grondslag ligt aan de in kaart gebrachte behoeften zodat de achterliggende vraag concreet kan worden gemaakt en kan worden bepaald wat nodig, haalbaar en realistisch is om op te pakken.



# Verloop incidenten fysiek/digitaal

## Conclusies

1. De analyse van de verschillen tussen het fysieke en digitale domein is van toegevoegde waarde voor het begrip van de problematiek en wat er nodig is voor een betere besturing van incidenten en crises.
2. Bij B, C en D de expliciete liggen wettelijke taken en verantwoordelijkheden voornamelijk in de warme fase van incidenten en crises terwijl beleid voornamelijk voor de koude en lauwe fase is geformuleerd.

## Aanbevelingen

1. Deze analyse als ijkpunt gebruiken bij beleidsvormende initiatieven op dit gebied én deze regelmatig (bijvoorbeeld tweejaarlijks) actualiseren.
2. 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.
3. Bij de uitwerking van de uitdagingen extra aandacht besteden aan taken en verantwoordelijkheden en regie en mandaat.



# Vervolgstappen

Vanuit het bestuurlijk covenant wordt bepaald op welke van de vele conclusies en aanbevelingen concreet zal worden ingezet vanuit BZK, J&V, VNG en G4

Rapport breed delen om lokaal met de conclusies en aanbevelingen verder aan de slag te gaan

