Samenwerken ten tijde van een landelijke cybercrisis

Een kwalitatief onderzoek naar het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis

N. W. Bomhof
Radboud Universiteit Nijmegen
Faculteit der Managementwetenschappen
Master Bestuurskunde - Specialisatie Besturen van Veiligheid
Masterthesis
31 maart 2025
Begeleiders: Dr. D. P. Schaap & T. C. Brand MSc

Voorwoord

Beste lezer,

Voor u ligt mijn masterthesis *'Samenwerken ten tijde van een landelijke cybercrisis'*. Deze thesis vormt het laatste onderdeel van mijn masteropleiding Bestuurskunde aan de Radboud Universiteit te Nijmegen. Dit onderzoek heb ik in de periode van 11 maart 2024 tot en met 31 maart 2025 mogen uitvoeren in opdracht van Veiligheidsregio IJsselland.

Eerst wil ik graag benoemen dat ik trots ben op de route die ik de afgelopen jaren heb afgelegd. In 2011 ben ik begonnen op het vmbo-tl en in 2017 heb ik mijn havodiploma behaald. Daarna ben ik gestart met de hbo-opleiding Bedrijfskunde in Zwolle. Dit waren vier leerzame jaren, maar toch merkte ik dat het bedrijfsleven mij niet aansprak. Daarom heb ik na het afronden van mijn hbo-opleiding een 'tussenjaar' genomen, om erachter te komen waar mijn interesse wél ligt. Uiteindelijk heb ik mij aangemeld voor de pre-master Bestuurskunde. Na het afronden van deze pre-master ben ik in september 2023 begonnen aan de master Bestuurskunde, met als specialisatie 'Besturen van Veiligheid'.

Het schrijven van mijn thesis heb ik als pittig en leerzaam ervaren. Mede door persoonlijke redenen heb ik er langer over gedaan dan dat ik had gepland, maar gelukkig kon ik rekenen op steun van mijn begeleiders en mensen om mij heen. Daarom wil ik graag een aantal mensen in het bijzonder bedanken. Allereerst wil ik mijn begeleiders dr. D. P. Schaap en T. C. Brand MSc bedanken voor hun fijne begeleiding en feedback. Daarnaast wil ik mijn stagebegeleider H. Schreuders van Veiligheidsregio IJsselland bedanken voor het beschikbaar stellen van deze opdracht, begeleiding en flexibiliteit. Verder wil ik de respondenten bedanken die aan dit onderzoek hebben meegewerkt. Tot slot wil ik mijn familie en vrienden bedanken voor de steun die ze mij hebben gegeven.

Ik wens u veel leesplezier toe met het lezen van mijn masterthesis.

Noor Bomhof

Hardenberg, 31 maart 2025

Samenvatting

Het digitale domein is een dynamisch en onvoorspelbaar terrein, waarin cybercrisissen steeds ingrijpender worden en kunnen leiden tot ontwrichting van de maatschappij. Aangezien een cybercrisis zich niet aan de regiogrenzen houdt, kan deze zich al snel op landelijk niveau gaan afspelen. Een goede samenwerking tussen de veiligheidsregio's en partners vanuit het Rijk is dan noodzakelijk om een cybercrisis effectief te kunnen bestrijden. Om deze samenwerking te kunnen verbeteren, wordt er één keer in de twee jaar een ISIDOOR-oefening georganiseerd. Dit is een grootschalige cyberoefening waarbij de focus ligt op informatie-uitwisseling tussen actoren, het oefenen van de nationale crisisstructuur en het versterken van de samenwerking.

Uit de evaluatie van de laatste ISIDOOR-oefening blijkt dat er onduidelijkheid heerst omtrent het netwerk van informatiedeling en beeldvorming. Dit komt omdat het voor actoren niet duidelijk was hoe het netwerk is samengesteld, wie welke taken en verantwoordelijkheden heeft en wat ze van elkaar konden verwachten (Broeders & Van der Varst, 2024, p. 10). Hierdoor verliep de samenwerking in de praktijk tijdens de ISIDOOR-oefening anders dan in de formele structuur is vastgelegd. Dit wijst op een spanningsveld tussen de formele structuur en de samenwerking in de praktijk. Om deze reden wordt er in dit onderzoek antwoord gegeven op de volgende onderzoeksvraag: *'Hoe is de formele structuur van het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis ingericht, hoe ervaren betrokken actoren de samenwerking in de praktijk en op welke wijze kan de verhouding tussen deze twee concepten begrepen worden?'*

Het antwoord op deze vraag kan helpen om een landelijke cybercrisis in de toekomst effectiever te kunnen bestrijden, wat uiteindelijk kan bijdragen aan een weerbare en veiligere samenleving. Het conceptueel model van dit onderzoek is hoofdzakelijk opgesteld aan de hand van het theoretisch raamwerk van Ansell & Gash (2007) over *collaborative governance*. Vervolgens zijn de kwalitatieve datagegevens verzameld door middel van een documentenanalyse en 23 semigestructureerde interviews.

Allereerst blijkt uit dit onderzoek dat de formele structuur van het netwerk van informatiedeling en beeldvorming eenvoudig en overzichtelijk in samengesteld met duidelijke taken en verantwoordelijkheden. Het netwerk bestaat uit de 25 veiligheidsregio's, het Landelijk Operationeel Coördinatiecentrum (LOCC), het Nationaal Crisiscentrum (NCC), het Nationaal Kernteam Crisiscommunicatie (NKC) en het Nationaal Cyber Security Centrum (NCSC). Formeel gezien vindt er binnen het netwerk communicatie en informatie-uitwisseling plaats via het Landelijk Crisis Management Systeem (LCMS) en via direct contact tussen actoren. Daarnaast worden er binnen het netwerk geen beleidsmatige besluiten genomen over de daadwerkelijke aanpak van een cybercrisis, maar wel over informatiemanagement. Bovendien kan de formele sturingswijze binnen het netwerk, in termen van Kenis & Provan (2008), getypeerd worden als een combinatie van een zelfregulerend netwerk en een leiderorganisatienetwerk (Kenis & Provan, 2008, pp. 301-302).

De ervaren samenwerking in de praktijk laat daarentegen een weerbarstiger en complexer beeld zien. Zo heerst er veel onduidelijkheid onder de respondenten over de daadwerkelijke samenstelling van het netwerk en de rollen, taken en verantwoordelijkheden. Dit geldt ook voor de regels en procedures. Uit dit onderzoek blijkt dat, naast de formeel vastgelegde actoren, het

Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) in de praktijk een belangrijke rol vervult als vertaler. Dit houdt in dat het VR-ISAC de technische informatie over de oorzaak van een cybercrisis vertaalt naar de gevolgen voor de maatschappij. Veel respondenten hebben deze rol als waardevol ervaren, omdat andere actoren niet in staat waren om deze rol te vervullen. De rol van het VR-ISAC is formeel niet vastgelegd, wat leidt tot verwarring onder de respondenten. Verder komt uit dit onderzoek naar voren dat er in de praktijk gecommuniceerd wordt via een Operationeel-Leider call (OL-call). Dit is een belangrijk platform om informatie met elkaar te delen en af te stemmen. De OL-call is, net zoals de rol van het VR-ISAC, niet vastgelegd in de formele structuur van het netwerk.

Wanneer we de formele structuur en de samenwerking in de praktijk naast elkaar leggen, lijkt er sprake te zijn van twee totaal verschillende werelden. Dit heeft voornamelijk met één overkoepelend verschil te maken: het verloop van communicatie- en informatielijnen. Deze lijnen verlopen in de praktijk namelijk anders dan op papier is vastgelegd. De voornaamste verklaring voor het verschil is dat de formele structuur onvolledig is en daardoor onvoldoende houvast biedt aan de actoren. Hierdoor gaan de actoren andere manieren zoeken om het complexe probleem op te kunnen lossen. Een voorbeeld hiervan is de totstandkoming van de OL-call en de rol die het VR-ISAC vervult als vertaler binnen het netwerk. Omdat deze oplossingen tijdens de ISIDOOR-oefening effectief bleken, is het aannemelijk dat deze opnieuw worden toegepast in een volgende oefening of crisissituatie.

Dit wijst op een proces waarin informele oplossingen geleidelijk worden geïnstitutionaliseerd binnen de samenwerking in de praktijk. Er lijkt dan sprake te zijn van een wederkerige relatie tussen de formele structuur en de samenwerking in de praktijk. De formele structuur bepaalt voor een deel hoe men de praktijk ingaat, terwijl de ervaringen uit de praktijk de formele structuur weer veranderen.

Inhoudsopgave

Lijst van afkortingen **7**
H1| Inleiding **8**
1.1 Aanleiding 8
1.2 Probleemstelling 9
1.3 Voorbeschouwing theoretisch kader 9
1.4 Voorbeschouwing methodologisch kader 10
1.5 Wetenschappelijke & maatschappelijke relevantie 11
1.6 Leeswijzer 11
H2| Beleidskader **13**
2.1 Wet veiligheidsregio's 13
2.2 Cybercrisis & cybergevolgbestrijding 13
2.2.1 Definitie cybercrisis 13
2.2.2 Verschil tussen cybercrisis & reguliere crisis 14
2.2.3 Cybercomponenten 14
2.2.4 Cybergevolgbestrijding in de koude & warme fase 15
H3| Theoretisch kader **16**
3.1 Informatiedeling & beeldvorming 16
3.2 Verschuiving van government naar governance 16
3.3 Netwerken & collaborative governance 16
3.3.1 Definitie netwerken 17
3.3.2 Definitie collaborative governance 17
3.3.3 Collaborative governance modellen 18
3.3.4 Collaborative governance model van Ansell & Gash (2007) 18
3.4 Formele structuur van het netwerk 20
3.4.1 Samenstelling & formele werkwijze 20
3.4.2 Sturing & besluitvorming 22
3.5 Samenwerking in de praktijk 23
3.5.1 Startcondities 24
3.5.2 Face-to-face dialoog 25
3.5.3 Vertrouwen 25
3.5.4 Gedeelde betekenisgeving 26
3.5.5 Toewijding aan het proces 26
3.5.6 Tussentijdse resultaten 27
3.5.7 Faciliterend leiderschap 27

3.6 Conceptueel model 27
H4| Methodologisch kader 29
4.1 Onderzoeksmethode & benadering 29
4.2 Onderzoeksstrategie & casusselectie 30
4.3 Dataverzamelingsmethoden 30
4.3.1 Documentenanalyse 30
4.3.2 Semigestructureerde interviews 32
4.3.3 Respondentenselectie 32
4.4 Operationalisatie 34
4.4.1 Operationalisatie van de formele structuur 34
4.4.2 Operationalisatie van de samenwerking in de praktijk 35
4.5 Data-analyse 36
4.6 Kwaliteit van het onderzoek 37
4.6.1 Betrouwbaarheid 37
4.6.2 Validiteit 38
H5| Resultaten 39
5.1 Formele structuur van het netwerk 39
5.1.1 Samenstelling & formele werkwijze 39
5.1.2 Visualisatie van het formele netwerk 44
5.1.3 Sturing & besluitvorming 44
5.2 Samenwerking in de praktijk 46
5.2.1 Startcondities 46
5.2.2 Communicatie 49
5.2.3 Visualisatie van het netwerk in de praktijk 52
5.2.4 Toewijding aan het samenwerkingsproces 52
5.2.5 Leiderschap & vertrouwen 54
5.2.6 Tussentijdse resultaten 57
5.3 Formele structuur versus samenwerking in de praktijk 58
5.3.1 Ervaringen respondenten 59
5.3.2 Belangrijkste verschillen 59
H6| Conclusie, discussie & aanbevelingen 61
6.1 Conclusie 61
6.1.1 Formele structuur van het netwerk 61
6.1.2 Samenwerking in de praktijk 62
6.1.3 Theoretische reflectie op de samenwerking in de praktijk 64

6.1.4 Formele structuur versus samenwerking in de praktijk 65
6.1.5 Incomplete formele structuur & wederkerige relatie 65
6.2 Discussie 66
6.2.1 Theoretische reflectie 66
6.2.2 Methodologische reflectie 67
6.2.3 Implicaties van het onderzoek 68
6.3 Aanbevelingen 69
Literatuurlijst 71
Bijlagen 77
Bijlage A: Topiclijst semigestructureerde interviews 77
Bijlage B: Samenwerkingsstructuur tussen de functionele & algemene keten 79
Bijlage C: Informatielijnen binnen de algemene keten 80
Bijlage D: Gezagslijnen tijdens een landelijke cybercrisis 81
Bijlage E: Hoofdlijnen nationale crisisstructuur 82

Lijst van afkortingen

Afkorting	Omschrijving
AC	Algemeen Commandant
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CoPi	Commando Plaats Incident
GHOR	Geneeskundige Hulpverleningsorganisatie in de Regio
IAO	Interdepartementaal Afstemmingsoverleg
ICCb	Interdepartementale Commissie Crisisbeheersing
IFV	Instituut Fysieke Veiligheid
LCMS	Landelijk Crisis Management Systeem
LCP-Digitaal	Landelijk Crisisplan Digitaal
LDS	Landelijk Dekkend Stelsel
LOB	Landelijk Operationeel Beeld
LOCC	Landelijk Operationeel Coördinatie Centrum
MCCb	Ministeriële Commissie Crisisbeheersing
NAO	Netwerk Administratieve Organisatie
NCC	Nationaal Crisiscentrum
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NIPV	Nederlands Instituut Publieke Veiligheid
NKC	Nationaal Kernteam Crisiscommunicatie
OL-call	Operationeel Leider-call
ROT	Regionaal Operationeel Team
VR-ISAC	Veiligheidsregio Information Sharing and Analysis Centre

Tabel 1: Lijst van afkortingen.

H1| Inleiding

1.1 Aanleiding

Als er één terrein is waarbij de ervaringen uit het verleden geen garantie kunnen bieden voor de toekomst, dan is dat het terrein van digitale veiligheid. Het belang van digitale middelen is tegenwoordig niet meer weg te denken uit onze samenleving, maar dit brengt ook bepaalde risico's met zich mee (NCTV, 2023a, p. 5). Uit het *Cybersecuritybeeld Nederland 2024* blijkt dat digitale risico's dynamisch en complex zijn en kunnen zorgen voor grootschalige uitval. Het risico dat de nationale veiligheid hierdoor in het geding raakt, neemt toe (NCTV, 2024a, p. 5). Voorbeelden uit de praktijk laten zien dat cyberincidenten steeds ingrijpender worden. Denk hierbij aan de ransomware-aanval op Veiligheidsregio Noord- en Oost-Gelderland, de poging van cybercriminelen om in te breken op de Citrix-server van het Medisch Centrum Leeuwarden en de storing bij KPN, waardoor 112 onbereikbaar was. Ondanks dat de gevolgen van deze voorbeelden relatief beperkt zijn gebleven, roept dit de vraag op wat er gebeurt als de gevolgen wél leiden tot ontwrichting van de maatschappij. In dit soort situaties is een snelle en adequate crisisrespons van groot belang (NCTV, 2022a, p. 5).

Organisaties die zich onder meer bezighouden met het bestrijden van de gevolgen van cyberincidenten in de maatschappij zijn de veiligheidsregio's. De veiligheidsregio's zijn in het geval van een crisis verantwoordelijk voor het waarborgen van de continuïteit van de samenleving en het bieden van hulp aan de inwoners en bezoekers van de regio (Hooymans, 2019, p. 7). Om deze taken succesvol uit te kunnen voeren, moeten veiligheidsregio's zich samen met betrokken netwerkpartners zo goed mogelijk voorbereiden op cybercrisissen. Dit doen zij door te investeren in netwerk- en planvorming, informatieveiligheid en door gezamenlijk te oefenen (Heijmen et al., 2021, p. 3).

Aangezien cybercrisissen zich vaak niet aan de regiogrenzen houden, verspreiden deze zich al gauw over meerdere regio's. Dit maakt dat het een complex probleem wordt, omdat de crisis zich op landelijk niveau kan gaan afspelen. Nauwe samenwerking tussen veiligheidsregio's en partners vanuit het Rijk is daarom noodzakelijk. Hierbij is het uitwisselen van informatie en beeldvorming over de crisissituatie belangrijk, om de crisis zo effectief mogelijk aan te kunnen pakken (IFV, 2020, p. 37; Broeders & Van der Varst, 2024, p. 10; Turell et al., 2020, p. 32). Echter blijkt uit een rapport van het Instituut Fysieke Veiligheid (IFV) dat er bij een landelijke cybercrisis vaak onduidelijkheid ontstaat over de informatielijnen en verantwoordelijkheden van actoren (IFV, 2020, p. 37). Daarnaast blijkt uit een rapport van Boin et al. (2020) dat veiligheidsregio's nog weinig ervaring hebben met het bestrijden van landelijke cybercrisissen, waardoor het in de praktijk vaak zoeken is naar de juiste aanpak (Boin et al., 2020, p. 24). Dit kan de samenwerking tussen veiligheidsregio's en partners vanuit het Rijk belemmeren.

Om deze samenwerking te kunnen verbeteren wordt er één keer in de twee jaar een ISIDOOR-oefening georganiseerd. Dit is een grootschalige cyberoefening waarbij de focus ligt op het oefenen van de nationale opschalingsstructuur, informatie-uitwisseling tussen actoren en het verbeteren van de samenwerking tussen het Rijk en betrokken partners (NCSC, z.d.; Broeders & Van der Varst, 2024, p. 4). De meest recente editie van ISIDOOR vond plaats in november 2023 en is na afloop geëvalueerd. Deze evaluatie onderstreept onder andere het belang van informatie-uitwisseling en beeldvorming tussen actoren, omdat dit bijdraagt aan het effectief

bestrijden van een cybercrisis. Dit proces wordt aangeduid als het vormen van een Landelijk Operationeel Beeld (LOB) en wordt gefaciliteerd door het netwerk van informatiedeling en beeldvorming (Broeders & Van der Varst, 2024, pp. 10-11).

Uit de evaluatie blijkt echter dat het opstellen van een LOB niet effectief is verlopen. De oorzaak hiervan is gelegen in het feit dat het voor menig deelnemer onduidelijk was welke actoren betrokken zijn bij het netwerk van informatiedeling en beeldvorming, welke taken en verantwoordelijkheden actoren hebben en wat ze van elkaar kunnen verwachten (Broeders & Van der Varst, 2024, p. 10). Dit probleem wordt ook herkend door Veiligheidsregio IJsselland. Tijdens de ISIDOOR-oefening constateerde de operationeel leider van Veiligheidsregio IJsselland dat de samenwerking in de praktijk afweek van de vastgelegde formele structuur, wat leidde tot verwarring onder de betrokken actoren. Dit wijst op een spanningsveld tussen de formele structuur van het netwerk van informatiedeling en beeldvorming en de samenwerking in de praktijk. Om dit beter te kunnen begrijpen, heeft Veiligheidsregio IJsselland de opdracht gegeven om onderzoek uit te voeren naar het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis.

1.2 Probleemstelling

De probleemstelling van dit onderzoek bestaat uit een doel- en vraagstelling. De doelstelling van dit onderzoek is om inzichtelijk te maken hoe de formele structuur van het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis is ingericht, hoe de samenwerking in de praktijk wordt ervaren door betrokken actoren en hoe deze twee concepten zich tot elkaar verhouden. Dit inzicht draagt uiteindelijk bij aan een effectievere aanpak van een landelijke cybercrisis in de toekomst. De onderzoeksvraag luidt hierbij als volgt:

'Hoe is de formele structuur van het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis ingericht, hoe ervaren betrokken actoren de samenwerking in de praktijk en op welke wijze kan de verhouding tussen deze twee concepten begrepen worden?'

Om deze onderzoeksvraag te kunnen beantwoorden, zijn de volgende deelvragen opgesteld:

1. Hoe kan het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis theoretisch begrepen worden?
2. Hoe is de formele structuur van het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis ingericht?
3. Hoe ervaren de betrokken actoren de samenwerking in de praktijk?
4. Hoe verhoudt de formele structuur zich tot de samenwerking in de praktijk en welke factoren spelen hierbij een rol?

1.3 Voorbeschouwing theoretisch kader

In het theoretisch kader maak ik gebruik van verschillende theoretische inzichten om het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis beter te kunnen begrijpen. Samenwerking rondom een cybercrisis kan worden gezien in de context van een langer lopende bestuurlijke ontwikkeling, namelijk de verschuiving van *government* naar *governance*. Deze verschuiving vormt de basis van het ontstaan van theorieën en concepten rondom netwerken en *collaborative governance*. Deze twee begrippen zijn beiden gedefinieerd, aangezien ze sterk met elkaar samenhangen en verschillende theoretische inzichten bevatten

om de formele structuur van het netwerk en de samenwerking in de praktijk inzichtelijk te kunnen maken.

Het collaborative governance model van Ansell & Gash (2007) vormt de theoretische basis in dit onderzoek. De reden hiervoor is dat het model elementen bevat om de formele structuur van een netwerk en de samenwerking in de praktijk te kunnen onderzoeken. Daarnaast laat dit model zien dat de formele structuur een belangrijke determinant blijkt te zijn voor de samenwerking in de praktijk. Om de formele structuur inzichtelijk te kunnen maken heb ik gebruikgemaakt van de theorie van Ansell & Gash (2007) over het institutioneel ontwerp van een netwerk en de face-to-face dialoog tussen actoren. Daarnaast heb ik verschillende concepten uit de theorie van Koppenjan & Klijn (2004) over de bestuurskundige netwerkanalyse en het conceptueel model van Kenis & Provan (2008) over netwerksturing toegepast. Om de samenwerking in de praktijk beter te kunnen begrijpen heb ik verschillende elementen uit het collaborative governance model van Ansell & Gash (2007) gebruikt. Het gaat hierbij om startcondities, face-to-face dialoog, vertrouwen, gedeelde betekenisgeving, toewijding aan het proces, tussentijdse resultaten en faciliterend leiderschap. Deze elementen zijn verder onderbouwd met theoretische inzichten van andere auteurs, die relevante concepten aandragen. Het hoofdstuk sluit af met een conceptueel model, waarin de elementen van formele structuur en de samenwerking in de praktijk gevisualiseerd zijn. Daarnaast is de verhouding tussen deze twee concepten gevisualiseerd en toegelicht.

1.4 Voorbeschouwing methodologisch kader

Dit onderzoek betreft een kwalitatief onderzoek. Dit type onderzoek richt zich op het verzamelen, analyseren en interpreteren van tekstueel materiaal of verbale gegevens, om op basis daarvan uitspraken te kunnen doen over sociale fenomenen in de werkelijkheid. De kracht van kwalitatief onderzoek is dat het de werking en het bestaan van mechanismen kan blootleggen (Boeije & Bleijenbergh, 2019, p. 18). In dit onderzoek heb ik gekozen voor een interpretatieve benadering, omdat deze benadering de mogelijkheid biedt om de ervaringen van actoren binnen het netwerk van informatiedeling en beeldvorming beter te kunnen begrijpen. Deze benadering legt de nadruk op ervaringen en betekenissen van personen (Boeije & Bleijenbergh, 2019, p. 19). Daarnaast heb ik een abductieve onderzoeksbenadering toegepast, omdat ik continu heen en weer ben gegaan tussen de empirische datagegevens en theoretische inzichten van dit onderzoek (Schwartz-Shea & Yanow, 2012, pp. 27-30).

Verder richt dit onderzoek zich op één specifieke casus: het netwerk van informatiedeling en beeldvorming in de context van een landelijke cybercrisis. Dit netwerk kan bestempeld worden als een enkelvoudige ingebedde *case study*, omdat het meerdere actoren bevat die afzonderlijk onderzocht zijn in dit onderzoek. Daarnaast is de casus een voorbeeld van een extreme case study, aangezien landelijke cybercrisissen een nieuw type crisis zijn en daardoor nog zelden hebben plaatsgevonden (Bryman, 2012, pp. 70-71). Dit betekent dat de manier van samenwerken op dit moment nog niet representatief is voor de algemene manier van samenwerken tijdens reguliere crisissituaties, maar de verwachting is wel dat dit type crisis vaker gaat plaatsvinden in de toekomst.

In dit onderzoek heb ik twee verschillende dataverzamelingsmethoden toegepast. Het gaat hierbij om een documentenanalyse en semigestructureerde interviews. De documentenanalyse

is gebruikt om de formele structuur van het netwerk van informatiedeling en beeldvorming in kaart te brengen. Daarnaast hebben er 23 semigestructureerde interviews plaatsgevonden met respondenten uit het netwerk, om inzicht te krijgen in hun ervaringen met de samenwerking in de praktijk. Na het verzamelen van de gegevens heb ik de interviews getranscribeerd, op een abductieve wijze gecodeerd en uitgewerkt in resultaten.

1.5 Wetenschappelijke & maatschappelijke relevantie

Dit onderzoek levert een wetenschappelijk bijdrage door kennis te vergaren over de manier van samenwerken binnen het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis. Ansell & Gash (2007, p. 563) benadrukken dat netwerksamenwerking steeds meer in opkomst is, waardoor diepgaande kennis over samenwerking binnen een netwerk steeds belangrijker is. Aangezien een landelijke cybercrisis een relatief nieuw type crisis betreft en zelden heeft plaatsgevonden, is hier tot op heden nog weinig onderzoek naar gedaan (Boin et al., 2020, p. 24; Van der Varst et al., 2020, pp. 14-15). Gezien de toenemende impact van cybercrisissen en de verwachting dat deze vaker zullen gaan plaatsvinden, wordt er echter wel steeds meer aandacht besteed aan dit type crisis (NCTV, 2022a, p. 5). De bevindingen van dit onderzoek verrijken de bestaande literatuur over netwerken en collaborative governance en dragen bij aan een beter begrip over samenwerken binnen een netwerk tijdens een nieuwe en complexe crisissituatie. Verder verrijken de bevindingen van dit onderzoek ook de literatuur over crisismanagement en crisisbeheersing, waarin het belang van een samenwerking tussen veiligheidsregio's en het Rijk wordt benadrukt (Hooymans, 2019; Turell et al., 2020; Van der Varst et al., 2020). Dit onderzoek biedt nieuwe inzichten en aanknopingspunten in de samenwerkingsdynamieken tussen de veiligheidsregio's en het Rijk, tijdens een nieuwe en complexe crisissituatie.

Naast de wetenschappelijke relevantie heeft dit onderzoek ook een maatschappelijk relevantie. Aangezien cybercrisissen steeds ingrijpender worden en kunnen leiden tot ontwrichting van de maatschappij, is een snelle crisisrespons van groot belang (NCTV, 2022a, p. 5). Dit onderzoek vergaart inzichten in de formele structuur van het netwerk van informatiedeling tijdens een landelijke cybercrisis, de ervaringen van betrokken actoren met de samenwerking in de praktijk en de verhouding tussen deze twee concepten. Wanneer de betrokken actoren over deze kennis beschikken, kan de samenwerking binnen het netwerk verbeterd worden. Op basis van de bevindingen van dit onderzoek zijn een aantal aanbevelingen geformuleerd, om een landelijke cybercrisis in de toekomst effectiever te kunnen bestrijden. Dit draagt uiteindelijk bij aan een weerbare en veiligere samenleving. Daarnaast zijn de bevindingen van dit onderzoek niet alleen interessant voor de betrokken actoren binnen het netwerk van informatiedeling en beeldvorming, maar kan het in de toekomst ook nuttig zijn voor andere samenwerkingen in crisissituaties. Dit komt omdat de manier van samenwerken binnen het netwerk van informatiedeling en beeldvorming in de toekomst wellicht de manier is om complexe problemen te kunnen aanpakken.

1.6 Leeswijzer

Na de inleiding van dit onderzoek, wordt in Hoofdstuk 2 het beleidskader geschetst. Hoofdstuk 3 richt zich op het theoretisch kader, waarin de concepten van dit onderzoek worden uitgewerkt op basis van wetenschappelijke literatuur. In Hoofdstuk 4 staat het methodologisch kader

centraal en hierin worden de methodologische keuzes toegelicht en verantwoord. In Hoofdstuk 5 worden de resultaten van dit onderzoek gepresenteerd. Tot slot wordt er in Hoofdstuk 6 antwoord gegeven op de onderzoeksvraag, vindt er een discussie plaats over het uitgevoerde onderzoek en worden er enkele aanbevelingen gedaan.

H2| Beleidskader

In dit hoofdstuk beschrijf ik hoe de organisatie van veiligheidsregio's zijn ingericht en wat hun taken en bevoegdheden zijn. Daarna volgt er een uitleg over wat er wordt verstaan onder de begrippen cybercrisis en cybergevolgbestrijding.

2.1 Wet veiligheidsregio's

De Wet veiligheidsregio's is op 1 oktober 2010 ingevoerd en beschrijft de organisatie van een veiligheidsregio (Muller et al., 2020 p. 19). Artikel 8 van de Wet veiligheidsregio's benoemt dat Nederland bestaat uit 25 verschillende veiligheidsregio's die zich inzetten voor de veiligheid van de inwoners en bezoekers van de regio. Conform artikel 10 van de Wet veiligheidsregio's hebben veiligheidsregio's de volgende taken en bevoegdheden:

a. Het inventariseren van risico's van branden, crisissen en rampen;
b. Het adviseren van het bevoegd gezag over risico's van branden, crisissen en rampen in de bij of krachtens de wet aangewezen gevallen alsook in de gevallen die in het beleidsplan zijn vastgelegd;
c. Het adviseren van het college van burgemeester en wethouders over de brandweerzorg;
d. Het voorbereiden op de bestrijding van branden en het organiseren van de crisisbeheersing en rampenbestrijding;
e. Het instellen en in stand houden van een brandweer;
f. Het instellen en in stand houden van een Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR);
g. Het voorzien in de meldkamerfunctie;
h. Het aanschaffen en beheren van gemeenschappelijk materieel;
i. Het inrichten en in stand houden van de informatievoorziening binnen de diensten van de veiligheidsregio en tussen deze diensten en de andere diensten en organisaties die betrokken zijn bij de genoemde taken.

Het algemeen bestuur van veiligheidsregio's bestaat volgens artikel 11, eerste lid, van de Wet Veiligheidsregio's uit de burgemeesters van de betrokken gemeenten. Daarnaast beschrijft artikel 4, eerste lid, van de Wet veiligheidsregio's dat wanneer een brand, ramp of crisis beperkt blijft tot één gemeente, de burgemeester van de getroffen gemeente het gezag heeft. Wanneer meerdere gemeenten tegelijk worden getroffen, is de voorzitter van de veiligheidsregio verantwoordelijk voor de rampenbestrijding en crisisbeheersing binnen de regio. De voorzitter van de veiligheidsregio is in de meeste gevallen de burgemeester van de grootste gemeente binnen de regio (Rijksoverheid, z.d.a).

2.2 Cybercrisis & cybergevolgbestrijding

In deze subparagraaf wordt toegelicht hoe veiligheidsregio's het begrip cybercrisis definiëren, wat de verschillen zijn met een reguliere crisis, op welke cybercomponent dit onderzoek zich richt en wat cybergevolgbestrijding in de koude en warme fase inhoudt.

2.2.1 Definitie cybercrisis

Het begrip cybercrisis kan worden beschouwd als een containerbegrip, waardoor het geen eenduidige definitie kent. Veiligheidsregio's spreken bij een cybercrisis vaak over een 'digitale

verstoring'. In de *Whitepaper Digitale Ontwrichting en Cyber* van het Nederlands Instituut Publieke Veiligheid (NIPV) wordt een cybercrisis als volgt gedefinieerd:

> Iedere verstoring van een digitaal (ICT) systeem (moedwillig of door toeval, bedoeld of door een fout) die de (fysieke) veiligheid of openbare orde in een veiligheidsregio bedreigt. De oorzaak kan zowel in het digitale als fysieke domein liggen. In feite kan iedere verstoring een cybercomponent hebben. Ernstige of langdurige digitale verstoringen kunnen tot maatschappelijke ontwrichting leiden; digitale ontwrichting. (Hooymans, 2019, p. 5)

Deze bovenstaande definitie van een cybercrisis wordt in dit onderzoek gehanteerd.

2.2.2 Verschil tussen cybercrisis & reguliere crisis

In het rapport *Cybergevolgbestrijding* concluderen Van der Varst et al. (2020, pp. 14-15) dat een cybercrisis een nieuw type crisis is en dat veiligheidsregio's nog weinig ervaring hebben opgedaan met het bestrijden van een cybercrisis. Daarnaast brengt een cybercrisis andere uitdagingen met zich mee en onderscheidt het zich van reguliere crisis, omdat:

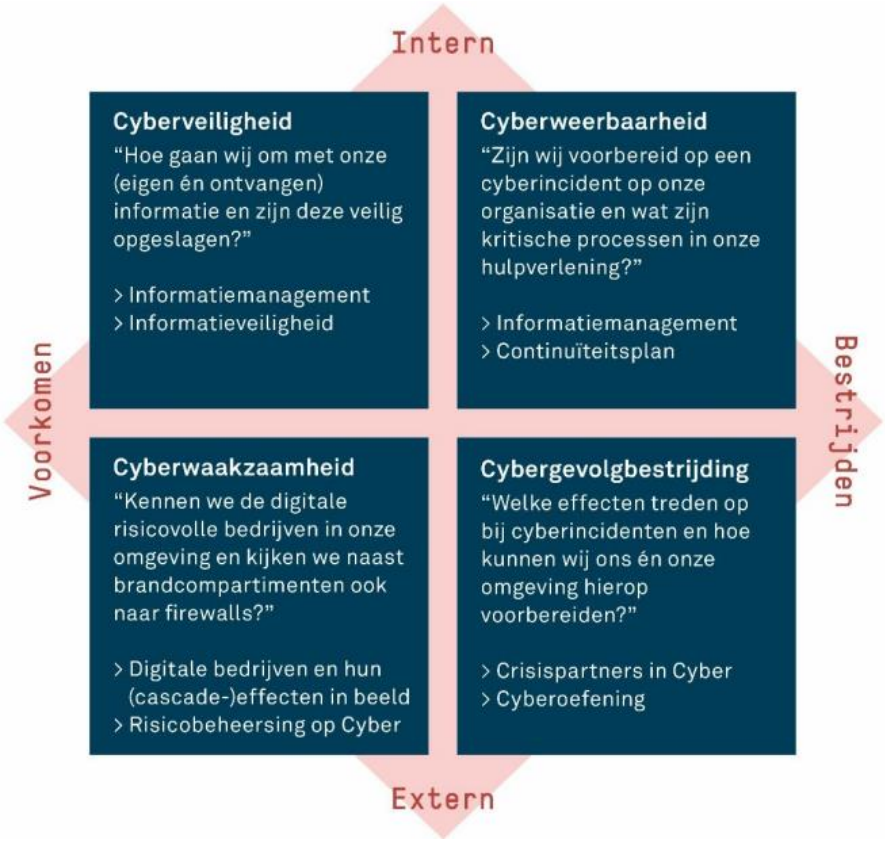
a. Een cybercrisis vaak niet zicht- en tastbaar is. Dit maakt het moeilijker om de bron te identificeren;
b. Het verloop van een cybercrisis in de meeste gevallen onvoorspelbaar is;
c. Een cybercrisis geen grenzen kent en meerdere domeinen tegelijk kan treffen. Dit heeft tot gevolg dat er met andere partners samengewerkt moet worden dan bij een reguliere crisis;
d. Er bij een cybercrisis veelal andere dilemma's spelen. Zo kan het herstel op gespannen voet staan met opsporingsbelangen van de politie. Hierdoor kan het hersteltraject van een cybercrisis langer duren.

Op basis van deze verschillen kan er gesteld worden dat een cybercrisis meer flexibiliteit en improvisatievermogen vereist van de crisisorganisatie dan een reguliere crisis (Van der Varst et al., 2020, p. 14).

2.2.3 Cybercomponenten

Volgens de *Whitepaper Digitale Ontwrichting en Cyber* kent de bestrijding van een cybercrisis vier verschillende componenten: cyberveiligheid, cyberweerbaarheid, cyberwaakzaamheid en cybergevolgbestrijding (Hooymans, 2019, p. 10). Deze componenten zijn door Veiligheidsregio IJsselland ondergebracht in een cyberkwadrant (zie Figuur 1 op de volgende pagina).

Een cybercrisis kan impact hebben op de interne organisatie van een veiligheidsregio, waarbij er bijvoorbeeld belangrijke informatie verloren gaat of digitale systemen uitvallen. In dit geval spelen de interne componenten cyberveiligheid en cyberweerbaarheid een belangrijke rol om uitval of problemen te kunnen voorkomen. Daarnaast kan een cybercrisis ook gevolgen hebben voor de maatschappij, waarbij de componenten cyberwaakzaamheid en cybergevolgbestrijding van belang zijn. In dit onderzoek ligt de focus op het component cybergevolgbestrijding, omdat het netwerk van informatiedeling en beeldvorming zich hierop richt. Cybergevolgbestrijding omvat namelijk alle activiteiten die te maken hebben met het bestrijden van de gevolgen van een cybercrisis in de maatschappij (Hooymans, 2019, p. 10).



Figuur 1: Cyberkwadrant Veiligheidsregio IJsselland (Hooymans, 2019, p. 10).

2.2.4 Cybergevolgbestrijding in de koude & warme fase

Cybergevolgbestrijding kent een koude en warme fase. De koude fase bestaat voornamelijk uit voorbereiding, waarbij de nadruk ligt op het samenwerken met netwerkpartners en de aanpak van de crisis (Hooymans, 2019, p. 16). Aangezien een cybercrisis een nieuw type crisis is, is het belangrijk dat veiligheidsregio's zich goed voorbereiden samen met netwerkpartners om een cybercrisis in de toekomst zo effectief mogelijk te kunnen bestrijden (Boin et al., 2020, p. 24; Turell et al., 2020, p. 32). Zoals eerder besproken is de ISIDOOR-oefening bedoeld om hieraan bij te dragen.

Veiligheidsregio IJsselland heeft met haar Regionaal Operationeel Team (ROT) deelgenomen aan de ISIDOOR-oefening in 2023. Het ROT van Veiligheidsregio IJsselland bestaat uit een operationeel leider, een informatiemanager en een communicatieadviseur. De Algemeen Commandanten (AC's) van de brandweer, Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR), politie en bevolkingszorg kunnen afhankelijk van de crisissituatie ook aansluiten. Taken van het ROT bestaan onder andere uit het ondersteunen van het Commando Plaats Incident (CoPi), het coördineren van de operatie en het adviseren van de burgemeester of de voorzitter van de veiligheidsregio (Veiligheidsregio IJsselland, 2022, pp. 11-12).

De warme fase van cybergevolgbestrijding verwijst naar een cybercrisis die daadwerkelijk plaatsvindt. Dit houdt in dat de veiligheidsregio's en netwerkpartners actie ondernemen om de gevolgen in de maatschappij te bestrijden (Hooymans, 2019, p. 17).

H3| Theoretisch kader

In dit hoofdstuk staat het theoretisch kader centraal. Hierin beschrijf ik verschillende theorieën en modellen die helpen om het netwerk van informatiedeling en beeldvorming beter te kunnen begrijpen. In dit hoofdstuk wordt er dan ook antwoord gegeven op de volgende deelvraag: '*Hoe kan het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis theoretisch begrepen worden?*'

Aan de hand van wetenschappelijke literatuur licht ik eerst toe wat er wordt verstaan onder informatiedeling en beeldvorming. Vervolgens volgt er een theoretische introductie over de verschuiving van *government* naar *governance* en worden de begrippen netwerken en *collaborative governance* gedefinieerd. Daarna komt het theoretisch raamwerk van Ansell & Gash (2007) en andere aanvullende theorieën aan bod, om de formele structuur van het netwerk en de samenwerking in de praktijk inzichtelijk te kunnen maken. Tot slot wordt het conceptueel model van dit onderzoek gepresenteerd, waarin de verschillende elementen die ik in dit onderzoek bestudeer visueel worden weergegeven.

3.1 Informatiedeling & beeldvorming

Het begrip informatiedeling wordt in dit onderzoek gezien als een communicatief proces waarin informatie proactief gedeeld wordt tussen actoren. Dit proces bestaat ook wel uit het informatie verstrekken aan anderen en het ontvangen van informatie vanuit de informatieverstrekker (Sonnenwald, 2006, pp. 1-2). Beeldvorming, ook wel vaak aangeduid als *sense-making*, is een proces waarin crisismanagers proberen te begrijpen wat er gebeurt in de werkelijkheid en wat de gevolgen kunnen zijn van een crisissituatie. Dit proces omvat het verzamelen, analyseren en verspreiden van informatie onder actoren met als doel om een gedeeld begrip te creëren over de crisissituatie (Ansell & Boin, 2019, p. 1082).

3.2 Verschuiving van government naar governance

In de afgelopen decennia heeft er een verschuiving plaatsgevonden van government naar governance. Government kan getypeerd worden als een hiërarchische bestuursvorm waarin de overheid de leiding neemt, regels opstelt en verantwoordelijk is voor het beleid en de uitvoering. Governance is een bestuursvorm waarbij niet alleen de overheid, maar ook andere actoren betrokken zijn en met elkaar samenwerken. Te denken valt aan actoren uit de publieke en private sector, maatschappelijke organisaties en burgers. Dit wordt ook wel als medebestuur of gedeeld bestuur omschreven, aangezien actoren gezamenlijk tot consensus proberen te komen over de doelstellingen die worden nagestreefd en de manier waarop dit gebeurt (Voets et al., 2021, p. 1; Lo, 2017, p. 1; Vreke et al., 2009, p. 9). De verschuiving van government naar governance kan deels worden verklaard door de toenemende complexiteit van maatschappelijke problemen, waardoor de overheid niet langer in staat is om deze zelf op te lossen. Om de complexe problemen effectief te kunnen aanpakken, is samenwerking tussen verschillende actoren noodzakelijk (Voets et al., 2021, p. 3; Sørensen & Torfing, 2005, pp. 197-198).

3.3 Netwerken & collaborative governance

Naast de bovenstaande verklaring vormt de verschuiving van government naar governance ook de basis voor het ontstaan van theorieën rondom netwerken en collaborative governance. De relatie tussen deze twee begrippen wordt benadrukt door Voets et al. (2021), die stellen dat

collaborative governance zich ontvouwt binnen de context van netwerken. Dit betekent dat collaborative governance voortkomt uit de processen die binnen netwerken plaatsvinden (Voets et al., 2021, p. 2). Hierdoor zijn de theorieën over netwerken en collaborative governance met elkaar verbonden en vormen ze samen een nuttige lens om het netwerk van informatiedeling en beeldvorming te kunnen onderzoeken.

3.3.1 Definitie netwerken

Netwerken worden in de wetenschappelijke literatuur vaak als een containerbegrip beschouwd. Ondanks dat auteurs het begrip op verschillende manieren definiëren, verwijzen de meeste definities naar de onderlinge relatie tussen actoren. Zo beschrijven Borgatti & Halgin (2011) dat een netwerk bestaat uit een set actoren en de relaties die hen met elkaar verbindt (Borgatti & Halgin, 2011, p. 1169). Kenis & Provan (2008) definiëren een netwerk als het verbinden of delen van informatie, activiteiten, middelen en competenties van minimaal drie organisaties, om samen een uitkomst te realiseren (Kenis & Provan, 2008, p. 296). Daarbij noemen ze een voorbeeld over een crisisbeheersingsnetwerk, waarin activiteiten van verschillende organisaties gecoördineerd verlopen (Kenis & Provan, 2008, p. 297). Het netwerk van informatiedeling en beeldvorming kan ook getypeerd worden als een crisisbeheersingsnetwerk, aangezien er een landelijke cybercrisis bestreden wordt. In dit onderzoek wordt daarom de definitie van Kenis & Provan (2008) gehanteerd, omdat deze definitie aandacht heeft voor coördinatie, sturing en het delen van hulpbronnen tussen verschillende actoren. Daarmee biedt de definitie van Kenis & Provan (2008) meer empirische aanknopingspunten dan de definitie van Borgatti & Halgin (2011).

3.3.2 Definitie collaborative governance

In het verlengde van governance ligt het begrip collaborative governance. De afgelopen jaren heeft collaborative governance zich steeds verder ontwikkeld als de nieuwe manier van besturen. Deze manier van besturen brengt overheidsinstanties en publieke en private actoren samen in een gemeenschappelijke vergadering, zodat besluitvorming op basis van consensus kan plaatsvinden (Ansell & Gash, 2007, p. 543).

Het begrip collaborative governance bevat verschillende benaderingen van samenwerking die gericht zijn op het bereiken van collectieve acties. De definities van collaborative governance kunnen daarom langs een aantal dimensies variëren. Het gaat hierbij om:

1. Welke actoren er samenwerken;
2. Wie de samenwerking sponsort;
3. Wat de samenwerking betekent;
4. Hoe de samenwerking wordt georganiseerd (Ansell, 2012, p. 499).

Zo definiëren Emerson et al. (2012) collaborative governance als:

> "The processes and structures of public policy decision making and management that engage people constructively across the boundaries of public agencies, levels of government, and/or the public, private and civic spheres in order to carry out a public purpose that could not otherwise be accomplished." (Emerson et al., 2012, p. 2)

Ansell & Gash (2007) definiëren collaborative governance als:

> "A governing arrangement where one or more public agencies directly engage non-state stakeholders in a collective decision-making process that is formal, consensus-oriented, and deliberative and that aims to make or implement public policy or manage public programs or assets." (Ansell & Gash, 2007, p. 544)

In dit onderzoek wordt de definitie van Ansell & Gash (2007) gehanteerd. De reden hiervoor is dat deze definitie een gestructureerde en uitgebreide benadering biedt, door zes belangrijke kenmerken van collaborative governance te benadrukken:

1. Het netwerk wordt geïnitieerd door overheidsinstanties of -instellingen;
2. Zowel publieke als niet-statelijke actoren maken deel uit van het netwerk;
3. Actoren zijn direct betrokken bij de besluitvorming en worden niet alleen geraadpleegd door overheidsinstanties;
4. Het netwerk is formeel georganiseerd en komt collectief bijeen;
5. Besluitvorming is consensusgericht;
6. Het netwerk richt zich op de domeinen public policy of public management (Ansell & Gash, 2007, p. 544).

Aangezien collaborative governance zich focust op de samenwerking tussen actoren binnen een netwerk, biedt de theorie hierover een nuttige lens om te kunnen begrijpen hoe actoren binnen het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis met elkaar samenwerken en op welke manier de samenwerking is gestructureerd.

3.3.3 Collaborative governance modellen

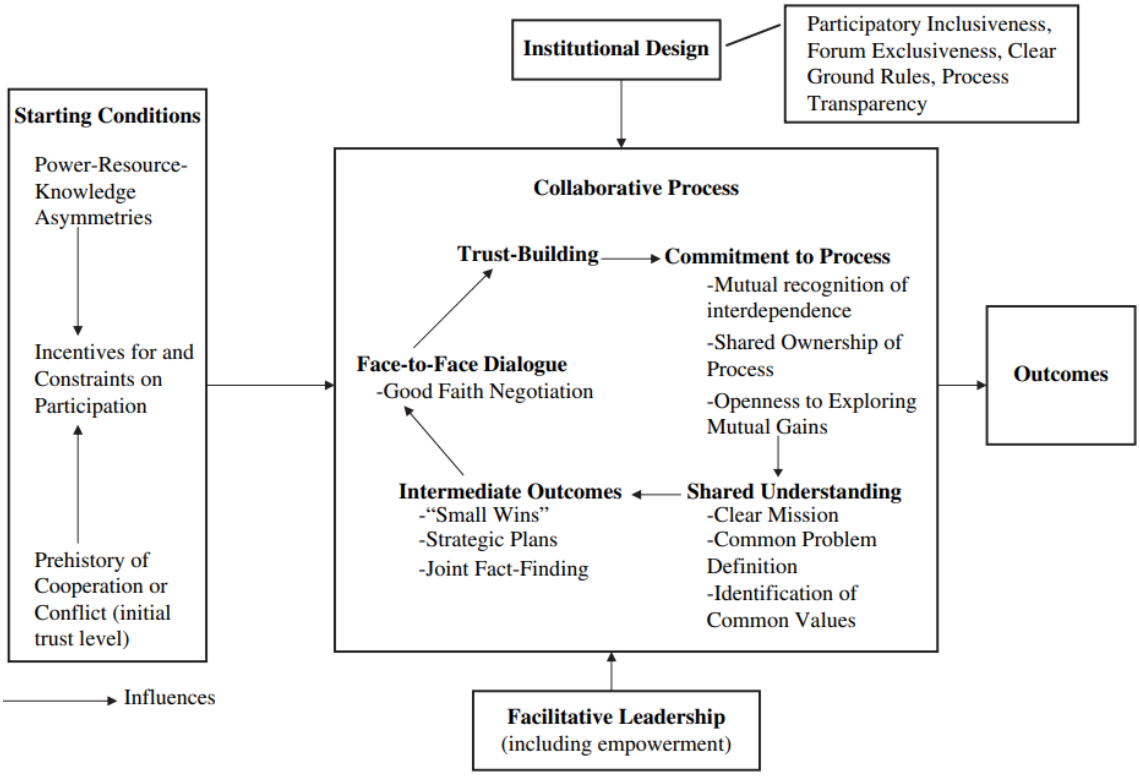
Om de samenwerking tussen actoren binnen een netwerk beter te begrijpen zijn er verschillende collaborative governance modellen ontwikkeld door auteurs. Het model van Ansell & Gash (2007) richt zich onder andere op de startcondities van een samenwerkingsverband en op het feitelijke samenwerkingsproces. Het model besteedt daarnaast ook aandacht aan het faciliterend leiderschap en het institutioneel ontwerp van een netwerk (Voets et al., 2021, pp. 5-7). Het model van Emerson et al. (2012) bespreekt de samenhang tussen de dynamiek binnen een samenwerking en de omgeving. Het model bestaat uit drijfveren die de samenwerking binnen een netwerk op gang brengen en veronderstelt dat een sterke betrokkenheid van actoren leidt tot efficiëntere beslissingen (Voets et al., 2021, pp. 8-9). Tot slot het model van Bryson et al. (2006). Dit model legt de nadruk op sector-overschrijdende samenwerkingen en houdt rekening met de realiteit van macht en autoriteit. Het model focust zich voornamelijk op conflicten, spanningen en verantwoordelijkheden binnen een samenwerking (Voets, 2021, p. 10).

Ondanks dat deze drie modellen deels met elkaar overeenkomen, onderscheiden ze zich ook van elkaar. Dit komt doordat de modellen verschillende elementen en factoren van collaborative governance benadrukken. In dit onderzoek staat het model van Ansell & Gash (2007) centraal, omdat dit model het beste aansluit op de onderzoeksvraag. In de volgende deelparagraaf wordt toegelicht waarom.

3.3.4 Collaborative governance model van Ansell & Gash (2007)

Het collaborative governance model van Ansell & Gash (2007) is een belangrijk instrument om de formele structuur van het netwerk van informatiedeling en beeldvorming te bestuderen en

om inzicht te kunnen krijgen in de samenwerking in de praktijk. Figuur 2 presenteert een visuele weergave van het model.



Figuur 2: Collaborative governance model (Ansell & Gash, 2007, p. 550).

Dit model vormt de basis van het conceptueel model van dit onderzoek, omdat het elementen bevat die zowel de formele structuur van een netwerk als de samenwerking in de praktijk inzichtelijk kunnen maken. Om de formele structuur van het netwerk van informatiedeling en beeldvorming te kunnen onderzoeken wordt voornamelijk het element institutioneel ontwerp uit dit model gebruikt. Verder wordt de face-to-face dialoog ook deels besproken in de theorie dat gaat over de formele structuur van een netwerk, omdat het aanknopingspunten bevat over de formele wijze waarop er wordt gecommuniceerd binnen een netwerk (Ansell & Gash, 2007, p. 550).

Voor het bestuderen van de samenwerking in de praktijk worden de verschillende aspecten uit het samenwerkingsproces gebruikt. Het gaat hierbij om face-to-face dialoog, vertrouwen, gedeelde betekenisgeving, toewijding aan het proces en tussentijdse resultaten. Naast deze aspecten worden ook de elementen startcondities en faciliterend leiderschap bestudeerd. Onder het element startcondities wordt ook deels het element institutioneel ontwerp meegenomen, om een inzicht te kunnen krijgen hoe de betrokken actoren dit in de praktijk ervaren. Het element institutioneel ontwerp wordt ondergebracht onder de startcondities, omdat ik verwacht dat deze in de praktijk met elkaar samenhangen.

Verder laat dit model zien dat het institutioneel ontwerp een belangrijke determinant is voor het samenwerkingsproces. Dit inzicht is van belang om te begrijpen hoe de formele structuur van het netwerk van informatiedeling en beeldvorming en de samenwerking in de praktijk zich tot elkaar verhouden. De bovengenoemde elementen worden verder onderbouwd met andere theoretische concepten van auteurs. Dit wordt verder uitgelegd in paragraaf 3.4 en 3.5.

Tot slot worden de verschillende aspecten van het samenwerkingsproces in het model weergegeven als een cyclus, omdat het samenwerkingsproces volgens Ansell & Gash (2007) een iteratief proces is. In dit onderzoek wordt dit iteratieve proces achterwege gelaten en worden de aspecten los van elkaar bestudeerd. De reden hiervoor is dat het artikel niet duidelijk toelicht hoe deze cyclus verloopt en wat de onderlinge relaties tussen de aspecten binnen het samenwerkingsproces zijn (Ansell & Gash, 2007, p. 550).

3.4 Formele structuur van het netwerk

De formele structuur van een netwerk verwijst naar de vastgelegde regels en afspraken die de werking van een netwerk reguleren. De formele structuur biedt daarmee duidelijke kaders voor de samenwerking tussen actoren (Ansell & Gash, 2007; Koppenjan & Klijn, 2004; Kenis & Provan, 2008). Om inzicht te kunnen krijgen in de formele structuur van het netwerk van informatiedeling en beeldvorming, maak ik in deze paragraaf gebruik van verschillende relevante theorieën die hierop betrekking hebben. Wanneer we kijken naar de literatuur over netwerken en collaborative governance, valt het op dat bij de formele structuur van een netwerk vaak twee elementen onderscheiden worden. Het gaat hierbij om samenstelling en formele werkwijze én sturing en besluitvorming. Deze thema's worden hieronder besproken.

3.4.1 Samenstelling & formele werkwijze

Het element samenstelling en formele werkwijze verdeel ik in deze paragraaf onder in drie aspecten: actoren, formele taken en relaties én de vergader- en communicatiestructuur. De reden hiervoor is dat de literatuur verschillende perspectieven en benaderingen biedt om de samenstelling en formele werkwijze van een netwerk te kunnen onderzoeken. Deze drie aspecten breng ik in dit onderzoek in kaart aan de hand van een aantal concepten uit de bestuurskundige netwerkanalyse van Koppenjan & Klijn (2004) en de elementen institutioneel ontwerp en face-to-face dialoog van Ansell & Gash (2007). Door deze theorieën te combineren ontstaat er een inhoudelijk passend beeld over de samenstelling en formele werkwijze van het netwerk van informatiedeling en beeldvorming.

Actoren

Om de actoren binnen het netwerk van informatiedeling en beeldvorming te bestuderen, maak ik gebruik van concepten uit de bestuurskundige netwerkanalyse van Koppenjan & Klijn (2004). Deze analyse benadrukt drie belangrijke punten. Het eerste punt stelt dat netwerken bestaan door wederzijdse afhankelijkheid tussen actoren. Het tweede punt belicht het feit dat netwerken bestaan uit verschillende actoren, die ieder hun eigen doel hebben. Het derde punt onderstreept dat netwerken worden gekenmerkt door de onderlinge relaties tussen actoren (Koppenjan & Klijn, 2004, p. 135).

Naast deze drie punten onderscheiden Koppenjan & Klijn (2004) drie typen analyses binnen hun bestuurskundige netwerkanalyse. Het gaat hierbij om de actoranalyse, de game-analyse en de netwerkanalyse. Deze analyses bieden een gezamenlijk inzicht in de voorwaarden en omstandigheden waarin besluitvormingsprocessen plaatsvinden binnen een netwerk. In de analyses worden verschillende concepten besproken die gebruikt kunnen worden als leidraad. In dit onderzoek worden slechts een aantal concepten gebruikt om de samenstelling en formele werkwijze van het netwerk te kunnen onderzoeken (Koppenjan & Klijn, 2004, p. 133).

Voor het in kaart brengen van de betrokken actoren binnen het netwerk is de actoranalyse van Koppenjan & Klijn (2004, pp. 135-136) relevant. Zij definiëren een actor als een individu, groep of organisatie die activiteiten onderneemt omtrent een probleemsituatie. De actoranalyse richt zich op het achterhalen wie de betrokken actoren zijn, wat hun probleemdefinities zijn en wat hun rol is binnen het netwerk. Voor het aspect actoren is het enkel relevant om te achterhalen wie de betrokken actoren zijn binnen het netwerk van informatiedeling en beeldvorming en wat hun rollen zijn. Daarbij hebben Koppenjan & Klijn (2004) een aantal kernvragen opgesteld die kunnen helpen bij het identificeren van de actoren en hun rol. Te denken valt aan: welke actoren zijn actief betrokken bij het probleem? Of welke actoren beschikken over kennis en inzicht om bij te dragen aan een oplossing (Koppenjan & Klijn, 2004, pp. 138-139)?

Verder benoemen Ansell & Gash (2007) in hun element over het institutioneel ontwerp dat het belangrijk is dat een netwerk alle actoren moet omvatten die zich bezighouden met het probleem. Dit houdt ook in dat een netwerk open en inclusief moet zijn. Inclusiviteit vormt namelijk de kern van een legitimatieproces waarin actoren gezamenlijk de beleidsresultaten bespreken en tot consensus komen. Wanneer bepaalde actoren niet vertegenwoordigd zijn, kan dit de legitimiteit van de gezamenlijke resultaten belemmeren (Ansell & Gash, 2007, p. 556).

Formele taken & relaties

De formele taken en relaties van het netwerk van informatiedeling en beeldvorming maak ik in dit onderzoek inzichtelijk aan de hand van het institutioneel ontwerp van Ansell & Gash (2007) en concepten uit de bestuurskundige netwerkanalyse van Koppenjan & Klijn (2004).

Ansell & Gash (2007) benadrukken in hun element over het institutioneel ontwerp het belang van een heldere definitie van rollen, taken en verantwoordelijkheden. Volgens hen draagt dit bij aan het opbouwen van vertrouwen tussen actoren. Het formaliseren van rollen, taken en verantwoordelijkheden wordt daarom gezien als een belangrijk factor voor succesvolle samenwerking (Ansell & Gash, 2007, p. 557). Koppenjan & Klijn (2004) verwijzen eveneens naar het belang van een heldere formele structuur binnen een netwerk. De netwerkanalyse van Koppenjan & Klijn (2004) bestaat uit de formele structuur die wordt bepaald door de institutionele context van het netwerk en de informele structuur die wordt gevormd door interactiepatronen en percepties (Koppenjan & Klijn, 2004, p. 151). Voor het aspect formele taken en relaties ligt de focus uitsluitend op de formele structuur van de netwerkanalyse. Koppenjan & Klijn (2004) richten zich daarbij op de rollen, taken en verantwoordelijkheden van actoren binnen een netwerk. Zij formuleren daarbij vragen die kunnen helpen bij de analyse van de formele structuur. Denk hierbij aan: welke rollen, taken en verantwoordelijkheden hebben de verschillende actoren binnen het netwerk (Koppenjan & Klijn, 2004, p. 156)?

Daarnaast beschrijven Ansell & Gash (2007) ook dat de basisregels en procedures de samenwerking binnen een netwerk structureren. Duidelijke regels en procedures dragen namelijk bij aan het vertrouwen binnen het netwerk. Daarnaast zorgt het ervoor dat het samenwerkingsproces eerlijk en open is. Procestransparantie speelt hierin een belangrijke rol. Dit houdt in dat actoren erop kunnen vertrouwen dat publieke onderhandelingen echt zijn en niet dienen als een dekmantel (Ansell & Gash, 2007, pp. 555-556).

Vergader- & communicatiestructuur
Voor het in kaart brengen van de vergader- en communicatiestructuur heb ik gebruikgemaakt van de literatuur van Ansell & Gash (2007) over de face-to-face dialoog. De literatuur over de face-to-face dialoog benadrukt dat het belangrijk is dat er directe interactie plaatsvindt tussen actoren binnen een netwerk, om zo het vertrouwen verder op te bouwen en de communicatie te verbeteren. Binnen dit aspect wordt de face-to-face dialoog van Ansell & Gash (2007) dan ook beschouwd als een formeel kader voor communicatie en interactie, in de vorm van georganiseerde bijeenkomsten of overlegmomenten. Het is namelijk van belang dat actoren binnen een netwerk elkaar regelmatig spreken of overleggen met elkaar, om op deze manier de samenwerking te kunnen verbeteren (Ansell & Gash, 2007, p. 558). Naast dit aspect in de formele structuur vormt de face-to-face dialoog ook een element dat wordt onderzocht in de samenwerking in de praktijk.

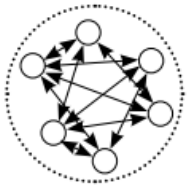
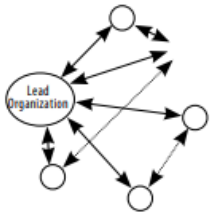
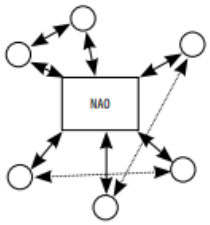
3.4.2 Sturing & besluitvorming
De overkoepelende dimensie sturing en besluitvorming heb ik in deze deelparagraaf opgesplitst in de wijze van sturing en besluitvorming. Deze twee aspecten worden in kaart gebracht aan de hand van het conceptueel model van Kenis & Provan (2008) over netwerksturing en de theorie van Koppenjan & Klijn (2004) over de game-analyse. Op basis van deze theoretische inzichten kan de wijze van sturing en besluitvorming binnen het netwerk van informatiedeling en beeldvorming onderzocht worden.

Wijze van sturing
De wijze van sturing binnen het netwerk van informatiedeling en beeldvorming maak ik in dit onderzoek inzichtelijk aan de hand van het conceptueel model van Kenis & Provan (2008) over netwerksturing. Zij benoemen dat de manier waarop er gestuurd wordt binnen een netwerk belangrijk is om te bepalen wat voor type structuur het netwerk heeft. Hierin worden drie vormen onderscheiden. De eerste vorm is het zelfregulerend netwerk dat bestaat uit verschillende actoren die als een collectief samenwerken, maar geen leider kennen. De sturing ligt bij de actoren in het netwerk zelf en dit houdt in dat alle actoren besluiten nemen en activiteiten managen. Een nadeel van deze vorm is dat het minder efficiënt kan zijn. Dit kan komen doordat er te veel gecommuniceerd wordt over minder belangrijke zaken en dat het moeilijker is om tot een consensus te komen. Hierbij kan een lichte vorm van coördinatie van belang zijn (Kenis & Provan, 2008, p. 301).

De tweede vorm betreft het leiderorganisatienetwerk. Deze vorm is het meest voorkomend en kan getypeerd worden als een sturingsvorm waarbij er verticale relaties zijn tussen de zogenoemde afnemers en aanbieders. Dit houdt in dat alle actoren in het netwerk een gemeenschappelijke doelstelling hebben en dat er sprake is van samenwerking en interactie tussen deze actoren. In dit netwerk worden alle activiteiten gecoördineerd door één van de actoren binnen het netwerk. Deze leider faciliteert de activiteiten van de deelnemende organisaties, zodat de doelstellingen behaald kunnen worden. Een nadeel van deze vorm is dat de leider vanuit eigen belang kan handelen (Kenis & Provan, 2008, pp. 301-302).

De derde vorm is de netwerk administratieve organisatie (NAO). De NAO houdt in dat er een afzonderlijke organisatie is ingesteld die enkel de taak heeft om het netwerk te managen en coördineren. Deze organisatie is niet actief binnen het netwerk zelf. Het gaat hier vaak om

publieke organisaties (Kenis & Provan, 2008, p. 302). In Figuur 3 zijn de verschillende vormen terug te vinden.

Netwerk governance	Zelfregulerend net-werk	Leiderorganisatie-netwerk	Netwerk administra-tieve organisatie (NAO)
Visualisatie			
Principe	Geen administratieve entiteit, participatie in netwerkmanagement door alle partijen	Administratieve entiteit (en netwerk-manager) is een be-langrijke netwerkpartij die ook een rol heeft in het primaire proces	Een toegewezen en aparte entiteit is gecreëerd om het netwerk te managen

Figuur 3: Drie vormen van network governance (Kenis & Provan, 2008, p. 301).

Besluitvorming

Tot slot is het belangrijk om te bestuderen wie er beslissingen mogen maken binnen het netwerk van informatiedeling en beeldvorming. Om dit te kunnen bepalen maak ik gebruik van concepten uit de game-analyse van Koppenjan & Klijn (2004). In de game-analyse wordt de focus gelegd op het identificeren van de zogenoemde arena's waarin actoren beslissingen maken en de stagnaties die zich kunnen voordoen rondom het besluitvormingsproces. Daarbij is het van belang om te onderzoeken welke beslissingen waar worden genomen en wie daarbij betrokken zijn (Koppenjan & Klijn, 2004, p. 147). In dit onderzoek is het enkel relevant om te bestuderen wie de beslissingen mogen maken binnen het netwerk van informatiedeling en beeldvorming. Het tweede deel dat gaat over het identificeren van de stagnaties, wordt niet meegenomen.

3.5 Samenwerking in de praktijk

In tegenstelling tot de formele structuur ligt de focus bij de samenwerking in de praktijk op de ervaringen, sociale relaties, percepties en verwachtingen van actoren. Om de ervaringen van de betrokken actoren binnen het netwerk van informatiedeling en beeldvorming inzichtelijk te kunnen maken, maak ik hoofdzakelijk gebruik van het theoretisch raamwerk van Ansell & Gash (2007) over collaborative governance. De elementen uit dit raamwerk worden verder onderbouwd met andere relevante theoretische concepten van auteurs (Van Delden, 2009; Koppenjan & Klijn, 2004; Emerson et al., 2012; Bryson et al., 2006; Goldsmith & Eggers, 2004; Vangen & Huxham, 2003; Klijn et al., 2010; Emerson & Nabatchi, 2015; Bryson et al., 2015). Door deze verschillende theorieën te combineren, kan de samenwerking in de praktijk beter begrepen worden.

Allereerst bespreek ik het element startcondities van Ansell & Gash (2007). Volgens hen hebben de startcondities invloed op de samenwerking in de praktijk en verwijzen ze naar de context

waarin de samenwerking plaatsvindt (Ansell & Gash, 2007, p. 550). Om deze redenen neem ik de startcondities als element op binnen de samenwerking in de praktijk. Het institutioneel ontwerp van Ansell & Gash (2007) is reeds besproken in de theorie dat gaat over de formele structuur van het netwerk, maar in dit onderzoek behandel ik dit element ook deels onder de startcondities. De reden hiervoor is dat ik verwacht dat deze elementen in de praktijk met elkaar samenhangen. Het gaat hierbij voornamelijk over rollen, taken en verantwoordelijkheden en de regels en procedures. Dit moet namelijk helder zijn op het moment dat actoren met elkaar gaan samenwerken en is daarom van belang om te onderzoeken (Ansell & Gash, 2007, p. 555). Vervolgens schrijven Ansell & Gash (2007) dat de elementen face-to-face dialoog, vertrouwen, toewijding aan het proces, gedeelde betekenisgeving en de tussentijdse resultaten ook invloed kunnen hebben op de samenwerking binnen een netwerk (Ansell & Gash, pp. 557-558). Tot slot benoemen Ansell & Gash (2007, p. 554) dat het element faciliterend leiderschap invloed heeft op de samenwerking in de praktijk. In de volgende deelparagrafen bespreek ik de elementen van de samenwerking in de praktijk.

3.5.1 Startcondities

Aan het begin van een samenwerking is het van belang om rekening te houden met een aantal factoren en de context waarin de samenwerking plaatsvindt. Ansell & Gash (2007) noemen dit ook wel de startcondities van een netwerk. Zij schrijven dat deze condities de samenwerking binnen een netwerk kunnen aanmoedigen of belemmeren. Factoren die onder de startcondities vallen zijn: prikkels om samen te werken, voorgeschiedenis van samenwerking tussen actoren, onbalans in macht en middelen en het institutioneel ontwerp (Ansell & Gash, 2007, p. 550).

De eerste factor betreft de prikkels om samen te werken binnen een netwerk. Volgens Ansell & Gash (2007) zijn actoren in een netwerk afhankelijk van elkaar om een doel te kunnen bereiken. Dit betekent dat een actor niet zelfstandig in staat is om een probleem op te lossen. De afhankelijkheid van andere actoren kan worden gezien als een prikkel om deel te nemen aan een samenwerking. Daarnaast kunnen bijvoorbeeld financiële en wettelijke prikkels ook een belangrijke stimulans zijn (Ansell & Gash, 2007, pp. 552-553; Van Delden, 2009, p. 36).

Naast de prikkels om samen te werken is het van belang om te kijken naar de voorgeschiedenis van actoren binnen het netwerk. Het komt vaak voor dat actoren elkaar als eens eerder zijn tegengekomen in andere samenwerkingsverbanden. Dit kan positief of negatief van invloed zijn op de huidige samenwerking. Wanneer er al eerder een succesvolle samenwerking heeft plaatsgevonden, kan dit een hogere mate van vertrouwen opwekken tussen actoren. Wanneer er sprake is geweest van een conflict tussen actoren, kan dit zorgen voor een belemmering in de samenwerking. Dit hangt vaak samen met een minder hoog vertrouwensniveau en slechte communicatie (Ansell & Gash, pp. 553-554; Van Delden, 2009, p. 37). Dit hoeft overigens niet altijd zo te zijn, want een conflict kan ook voor een stimulans zorgen om de samenwerking in de toekomst te verbeteren (Adham, 2023, p. 152).

Tot slot is ongelijkheid in macht en middelen tussen actoren een veelvoorkomend probleem binnen netwerken. Wanneer actoren niet beschikken over capaciteit, status of middelen om deel te nemen, kan dit leiden tot dominantie in het netwerk of manipulatie door ‘sterkere’ actoren (Ansell & Gash, 2007, p 551; Van Delden, 2009, p. 37). Een ander probleem is dat sommige actoren niet de kennis en expertise hebben om deel te nemen aan bepaalde discussies binnen

het netwerk, omdat het bijvoorbeeld over technische problemen gaat. Uiteindelijk stellen Ansell & Gash (2007) dat onbalans in macht en middelen kan leiden tot wantrouwen of beperkte betrokkenheid binnen een netwerk. Om dit op te kunnen lossen is het noodzakelijk dat de zwakkere actoren vertegenwoordigd worden binnen een netwerk (Ansell & Gash, 2007, p. 551).

Institutioneel ontwerp

Zoals al eerder beschreven verwijst het institutionele ontwerp van Ansell & Gash (2007) naar de formele structuur van een netwerk. Dit kan invloed hebben op het samenwerkingsproces. Toegang tot het samenwerkingsproces wordt hierbij gezien als het meest fundamentele ontwerpprobleem. Daarbij geldt de vraag welke actoren er binnen een samenwerking betrokken moeten worden. De literatuur benadrukt dan ook dat het samenwerkingsproces open en inclusief moet zijn en dat het alle actoren moet omvatten die betrokken zijn bij het probleem (Ansell & Gash, 2007, p. 556).

Naast toegang tot de samenwerking zijn duidelijke regels, procedures en definities van rollen ook van belang binnen een samenwerking. Het moet namelijk duidelijk zijn wie waarvoor staat (Van Delden, 2009, p. 104). Het formaliseren van deze bestuursstructuren is dan ook belangrijk, omdat dit een positief effect kan hebben op de samenwerking (Alexander et al., 1998, p. 324; Ansell & Gash, 2007, p. 557; Koppenjan & Klijn, 2004, p. 151).

3.5.2 Face-to-face dialoog

Het tweede element gaat over de face-to-face dialoog, ofwel communicatie. Ansell & Gash (2007) benadrukken dat communicatie tussen actoren de kern van een samenwerking vormt. Volgens hen is communicatie noodzakelijk om de kansen van wederzijds voordeel tussen actoren te kunnen identificeren. Communicatie vormt een belangrijk component voor het doorbreken van stereotyperingen en andere belemmeringen, die het verkennen van wederzijds voordeel tussen actoren in de weg staan. Het draagt bij aan het opbouwen van vertrouwen, wederzijds respect, gedeeld begrip en betrokkenheid bij het proces (Ansell & Gash, 2007, p. 558). Zo stellen Emerson et al. (2012) en Bryson et al. (2006) in hun governance-modellen ook dat face-to-face interacties cruciaal zijn voor het opbouwen van vertrouwen, effectieve communicatie en wederzijds begrip tussen de actoren.

Goldsmith & Eggers (2004, p. 94) onderstrepen daarentegen dat slechte communicatie tussen actoren kan leiden tot het falen van de samenwerking. Slechte communicatie of het niet spreken van dezelfde vaktaal kan het proces van informatie-uitwisseling verstoren. Dit kan uiteindelijk leiden tot verwarring in de verwachtingen en doelen van de samenwerking. Het is dus van belang dat actoren elkaar regelmatig spreken en overleg met elkaar voeren. Geen communicatie tussen actoren maakt dat het bereiken van een succesvolle samenwerking lastig wordt (Ansell & Gash, 2007, p. 558).

3.5.3 Vertrouwen

Het derde element gaat over vertrouwen. Vertrouwen tussen actoren is belangrijk om tot een succesvolle samenwerking te kunnen komen. Van Delden (2009) stelt dat vertrouwen wordt gezien als een conditie die in de samenwerking kan groeien of juist afnemen. Het is hierbij belangrijk dat actoren elkaar vertrouwen in het nakomen van afspraken (Van Delden, 2009, pp. 37-38). Ansell & Gash (2007) bespreken in hun artikel dat het opbouwen van vertrouwen tussen

actoren een belangrijke factor is. Wanneer er sprake is geweest van een conflict, is het van belang dat actoren tijd investeren in het wederopbouwen van vertrouwen. Dit neemt veel tijd in beslag, maar voor een goede samenwerking op de lange termijn is het van belang om hier aandacht aan te besteden (Ansell & Gash, pp. 558-559).

Klijn et al. (2010) beargumenteren ook dat vertrouwen een belangrijke rol speelt binnen een netwerksamenwerking. Zij benadrukken in hun artikel een aantal redenen waarom vertrouwen van belang is binnen een samenwerking. Ten eerste reduceert het de transactiekosten. Ten tweede zullen de actoren hun middelen sneller ter beschikking stellen, wat zorgt voor een sterkere basis van samenwerking. Het derde punt is dat vertrouwen de kennisuitwisseling tussen actoren vergroot. Het laatste punt vertelt ons dat vertrouwen zorgt voor het stimuleren van innovatie (Klijn et al., 2010, pp. 193-198).

3.5.4 Gedeelde betekenisgeving

Het vierde element gaat over gedeelde betekenisgeving van actoren. Om tot een succesvolle samenwerking te komen benadrukken Ansell & Gash (2007) dat er binnen een samenwerking gedeeld begrip moet ontstaan onder de actoren over het probleem. Een erkende missie, gemeenschappelijke probleemdefinitie en waarden zijn daarbij belangrijke elementen. Om dit te bereiken is het van belang de juiste actoren aan tafel te hebben (Ansell & Gash, 2007, p. 560).

Provan & Kenis (2008) spreken bij gedeelde betekenisgeving ook wel over doelconsensus. Dit wil zeggen dat er sprake is van gezamenlijke doelstellingen binnen een samenwerking. Binnen een netwerk is het namelijk niet vanzelfsprekend dat actoren dezelfde doelen hebben. Dit komt doordat actoren vaak verschillende percepties hebben over het probleem (Provan & Kenis, 2008, p. 239). De verschillende achtergronden, belangen en percepties van de actoren kunnen een nadelig effect hebben op de samenwerking (Koppenjan & Klijn, 2004, p. 136). Daarom heerst vooral binnen netwerken het idee dat er consensus moet ontstaan over een gezamenlijke doelstelling, zodat actoren weten wat er van hen verwacht wordt. Wanneer er sprake is van doelconsensus heeft dit een positief effect op het functioneren van het netwerk (Provan & Kenis, 2008, p. 240).

3.5.5 Toewijding aan het proces

Het vijfde element gaat over toewijding aan het proces, ofwel de betrokkenheid. Volgens Ansell & Gash (2007) en Emerson & Nabatchi (2015) is de mate van betrokkenheid van actoren een belangrijke factor voor het verklaren van het succes van de samenwerking of het falen. Betrokkenheid van actoren kan verschillende vormen aannemen, zoals face-to-face betrokkenheid of virtuele bijeenkomsten. Betrokkenheid hangt daarbij nauw samen met de oorspronkelijke motivatie die actoren hebben om deel te nemen aan de samenwerking. Vaak willen actoren hun eigen perspectief niet laten verzwakken, willen ze de legitimiteit waarborgen of participeren ze op basis van een wettelijke taak. Een hoge onderlinge afhankelijkheid tussen actoren vergroot waarschijnlijk de betrokkenheid bij de samenwerking, maar kan ook prikkels vergroten om manipulatief te handelen. Betrokkenheid binnen een netwerk betekent ook wel het ontwikkelen van de overtuiging dat er in goed vertrouwen wordt gehandeld. Bovendien is betrokkenheid de beste manier om beleidsresultaten te bereiken (Ansell & Gash, 2007, p. 559; Emerson & Nabatchi, 2015, p. 59).

Daarnaast is het belangrijk dat actoren een gevoel van gedeeld eigenaarschap ervaren om de gestelde doelen binnen het netwerk te behalen. Dit gevoel wordt versterkt naarmate de betrokkenheid binnen een samenwerking toeneemt. Eigenaarschap houdt tevens in dat actoren gedeelde verantwoordelijkheid dragen voor het samenwerkingsproces. Wanneer er sprake is van een verantwoordelijkheidsgevoel onder de actoren en gedeeld eigenaarschap, heeft dit een positief effect op de samenwerking. Dit komt omdat actoren dan sneller geneigd zijn om hulpbronnen en middelen beschikbaar te stellen aan elkaar (Ansell & Gash, 2007, pp. 559-560).

3.5.6 Tussentijdse resultaten

Het zesde element gaat over de tussentijdse resultaten. Volgens Ansell & Gash (2007) is de kans op een succesvolle samenwerking groter wanneer de doelen en voordelen van samenwerking concreet zijn en wanneer er winst uit de samenwerking kan worden gehaald. Tussentijdse resultaten kunnen een positieve invloed hebben op de samenwerking. Door het delen van tussentijdse resultaten kunnen eventuele opbrengsten van de samenwerking in een vroeg stadium worden vastgesteld (Ansell & Gash, 2007, p. 561). Daarnaast benadrukken Emerson et al. (2012, p. 23) en Bryson et al. (2006, p. 51) dat tussentijdse resultaten kunnen dienen als feedbackmechanismen, waardoor actoren hun strategieën kunnen aanpassen en kunnen leren van eerdere ervaringen. Op deze manier kan de samenwerking verder geoptimaliseerd worden.

3.5.7 Faciliterend leiderschap

Het laatste element gaat over faciliterend leiderschap. Volgens Ansell & Gash (2007) is faciliterend leiderschap een sleutelelement voor succesvolle samenwerking. Faciliterend leiderschap maakt het mogelijk om actoren bij elkaar te brengen en hen door eventuele moeilijke periodes te loodsen. Bovendien is faciliterend leiderschap van belang voor het opbouwen van vertrouwen, het faciliteren van communicatie tussen actoren, het verkennen van wederzijdse voordelen en het vertegenwoordigen van zwakkere actoren (Ansell & Gash, 2007, pp. 554-555; Emerson et al., 2012, p. 15; Vangen & Huxham, 2003, pp. 61-62).

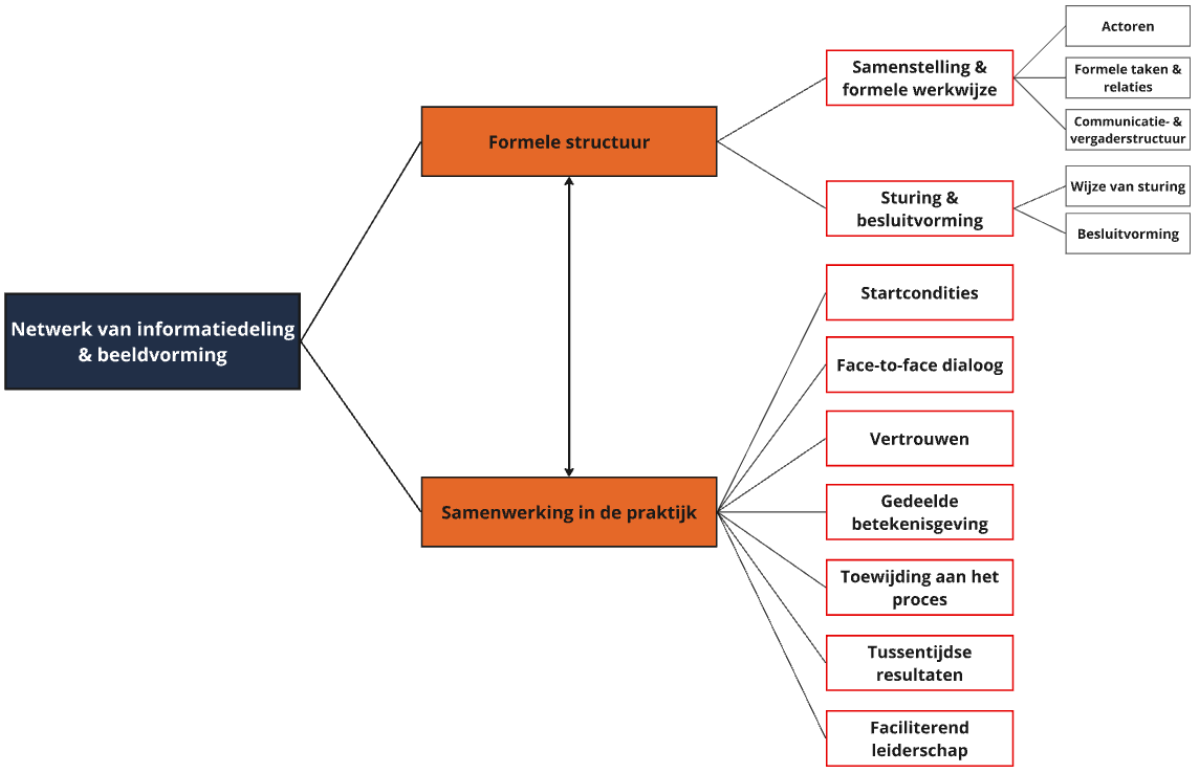
Daarnaast stellen Klijn & Koppenjan (2004) dat een leider onpartijdig moet zijn binnen een netwerk. Partijdigheid kan er namelijk voor zorgen dat andere actoren niet meer de ruimte krijgen om de inhoud van een bepaalde oplossing te bespreken. Leiderschap is belangrijk voor het omarmen, empoweren en betrekken van actoren en hen ertoe aan te zetten om de samenwerking te verbeteren (Koppenjan & Klijn, 2004, p. 203). Tot slot benadrukken Bryson et al. (2015, p. 652) bij leiderschap het belang van '*boundary spanners*'. Dit betekent dat een leider in staat moet zijn om de verschillende vaktalen van actoren binnen een netwerk te begrijpen en deze met elkaar te verbinden.

3.6 Conceptueel model

In Figuur 4 op de volgende pagina is een visuele weergave van het conceptueel model van dit onderzoek gepresenteerd. Dit model bestaat uit de twee centrale concepten: de formele structuur en de samenwerking in de praktijk. De formele structuur onderzoek ik aan de hand van twee overkoepelende elementen: samenstelling en formele werkwijze én sturing en besluitvorming. Bij samenstelling en formele werkwijze kijk ik naar de actoren binnen het netwerk, de formele taken en relaties en de communicatie- en vergaderstructuur. In het kader van sturing en besluitvorming bestudeer ik de wijze van sturing en besluitvorming binnen het netwerk.

Om inzicht te krijgen in de samenwerking in de praktijk onderzoek ik de elementen startcondities, face-to-face dialoog, vertrouwen, gedeelde betekenisgeving, toewijding aan het proces, tussentijdse resultaten en het faciliterend leiderschap. De theorie van Ansell & Gash (2007) maakt duidelijk dat sommige elementen met elkaar verbonden zijn. In dit onderzoek worden de elementen vereenvoudigd en bestudeer ik ze afzonderlijk. De reden hiervoor is dat dit onderzoek zich voornamelijk focust op de verhouding tussen de formele structuur en de samenwerking in de praktijk en hoe de verschillende elementen zich manifesteren in de empirische werkelijkheid. Het is daarom niet relevant om de verbanden tussen de elementen van de samenwerking in de praktijk te onderzoeken.

Verder kan op basis van de wetenschappelijke literatuur van Ansell & Gash (2007), Koppenjan & Klijn (2004), Bryson et al. (2006) en Emerson et al. (2012) verondersteld worden dat de formele structuur van een netwerk zich niet één-op-één verhoudt tot de samenwerking in de praktijk. Hoe de relatie tussen deze twee concepten precies verloopt, is echter nog onduidelijk. Meestal wordt verwacht dat de formele structuur de praktijk beïnvloedt (Ansell & Gash, 2007), hoewel het ook aannemelijk zou zijn dat de praktijk invloed uitoefent op de formele structuur. Deze verhouding is nu nog onduidelijk en ga ik bestuderen binnen dit onderzoek. De verhouding tussen de formele structuur en de samenwerking in de praktijk is in Figuur 4 weergegeven als een pijl.



Figuur 4: Conceptueel model van dit onderzoek.

H4| Methodologisch kader

In dit hoofdstuk worden de methodologische keuzes die ik gemaakt heb binnen dit onderzoek toegelicht en verantwoord. Eerst wordt de onderzoeksmethode beschreven en wordt er ingegaan op de onderzoeksstrategie en de casusselectie van dit onderzoek. Vervolgens wordt toegelicht welke dataverzamelingsmethoden zijn toegepast in dit onderzoek en worden de theoretische concepten uit Hoofdstuk 3 geoperationaliseerd. Daarna wordt beschreven hoe de verzamelde datagegevens zijn geanalyseerd. Tot slot wordt de kwaliteitswaarborging van dit onderzoek onderbouwd.

4.1 Onderzoeksmethode & benadering

Dit onderzoek bevat een kwalitatieve onderzoeksmethode. Volgens Boeije & Bleijenbergh (2019) is een kwalitatieve onderzoeksmethode een strategie voor het verzamelen, analyseren en interpreteren van tekstueel materiaal of verbale gegevens, om uitspraken te kunnen doen over sociale fenomenen in de werkelijkheid. Deze gegevens worden verkregen door interviews, een documentenanalyse of observaties (Boeije & Bleijenbergh, 2019, p. 18).

Om uitspraken te kunnen doen over het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis, heb ik in dit onderzoek gekozen voor de interpretatieve variant van kwalitatief onderzoek. De interpretatieve variant legt de nadruk op de subjectieve ervaringen en betekenissen van personen (Boeije & Bleijenbergh, 2019, p. 19). Deze benadering heb ik binnen dit onderzoek toegepast om het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis diepgaand te bestuderen en te begrijpen, waarbij de focus ligt op de ervaringen van betrokken actoren. Daarnaast vertoont dit onderzoek exploratieve kenmerken, aangezien de verhouding tussen de formele structuur van het netwerk van informatiedeling en beeldvorming en de samenwerking in de praktijk vooralsnog onduidelijk is. Dit onderzoek verschaft inzicht in de verhouding tussen deze twee concepten.

Verder heb ik in dit onderzoek een abductieve onderzoeksbenadering toegepast. Volgens (Rinehart, 2020) beweegt de onderzoeker bij een abductieve onderzoeksbenadering constant heen en weer tussen de verzamelde empirische datagegevens en de theoretische inzichten binnen het onderzoek (Rinehart, 2020, pp. 303-304). Hierbij wordt er gezocht naar de meest begrijpelijke verklaring voor het sociale fenomeen en helpt het proces van heen en weer bewegen bij het verfijnen van begrip en het ontwikkelen van nieuwe inzichten (Schwartz-Shea & Yanow, 2012, pp. 27-30).

Binnen dit onderzoek is er ook heen en weer bewogen tussen de empirische datagegevens en de theoretische inzichten. Van te voren heb ik op een deductieve manier vastgesteld dat de formele structuur en de samenwerking in de praktijk uit een aantal elementen bestaat en dat deze twee concepten zich niet één-op-één tot elkaar verhouden. Maar hoe deze concepten zich wel tot elkaar verhouden, was echter nog onduidelijk. In dit onderzoek heb ik deze verhouding onderzocht. Uiteindelijk is gebleken dat er een wederkerige relatie bestaat tussen de formele structuur en de samenwerking in de praktijk. In paragraaf 4.5 wordt verder uitgelegd hoe ik de abductieve onderzoeksbenadering in de data-analyse heb toegepast.

4.2 Onderzoeksstrategie & casusselectie

Binnen kwalitatief onderzoek zijn er verschillende onderzoeksstrategieën. In dit onderzoek is een *case study* toegepast. Volgens Heale & Twycross (2018, p. 7) en Myers (2013, p. 73) is een case study een empirisch onderzoek waarin een sociaal fenomeen diepgaand onderzocht wordt binnen de context waarin het zich bevindt. Hierbij kan er onderscheid gemaakt worden tussen een enkelvoudige case study of een meervoudige case study (Bleijenbergh, 2013, p. 52).

Dit onderzoek betreft een enkelvoudige case study, omdat het zich richt op één specifieke casus: het netwerk van informatiedeling en beeldvorming in de context van een landelijke cybercrisis. Binnen deze casus zijn er meerdere actoren vertegenwoordigd, waardoor de casus getypeerd kan worden als een ingebedde case study ontwerp (Grenier, 2023, p. 4). Om inzicht te kunnen krijgen in de gehele casus, heb ik de actoren afzonderlijk van elkaar bestudeerd met speciale aandacht voor Veiligheidsregio IJsselland. De reden hiervoor is dat Veiligheidsregio IJsselland de opdrachtgever van dit onderzoek is en om een beter inzicht te kunnen krijgen in de werking voor één veiligheidsregio.

Daarnaast is de casus in dit onderzoek een voorbeeld van een extreme case study, omdat het netwerk van informatiedeling en beeldvorming bestempeld kan worden als een uitzonderlijk geval dat momenteel nog niet representatief is voor de algemene situatie (Bryman, 2012, pp. 70-71). Dit komt doordat landelijke cybercrisissen een nieuw type crisis vormen en nog niet vaak hebben plaatsgevonden. Hierdoor is er nog weinig ervaring opgedaan met het bestrijden van een landelijke cybercrisis. Dit verklaart ook de onduidelijkheid binnen het netwerk en waarom het nog niet goed functioneert. De verwachting is dat landelijke cybercrisissen op de lange termijn steeds vaker gaan plaatsvinden (NCTV, 2024a, p. 5). Op dit moment kan het netwerk van informatiedeling en beeldvorming dus nog getypeerd worden als een extreme case study, maar in de toekomst zal deze casus wel representatief zijn voor de manier van samenwerken in crisissituaties.

4.3 Dataverzamelingsmethoden

Binnen dit onderzoek heb ik de kwalitatieve datagegevens met behulp van twee verschillende dataverzamelingsmethoden verzameld. Het gaat hierbij om een documentenanalyse en semigestructureerde interviews. Beide methoden worden hieronder toegelicht.

4.3.1 Documentenanalyse

Een documentenanalyse kan omschreven worden als het doelgericht verzamelen en analyseren van verschillende documenten, om op deze manier een breder begrip te kunnen krijgen van het sociale fenomeen in de werkelijkheid (Bleijenbergh, 2013, p. 164; Boeije & Bleijenbergh, 2019, p. 80). Door het analyseren van documenten kan de onderzoeker patronen en trends vaststellen die belangrijk zijn voor het onderzoek. Bovendien vergroot een documentenanalyse de betrouwbaarheid en validiteit van het onderzoek, omdat documenten een afspiegeling vormen over wat er daadwerkelijk is vastgelegd (Bleijenbergh, 2013, p. 164). Het is wel van belang om als onderzoeker kritisch te blijven op de documenten die worden onderzocht, aangezien ze door derden zijn opgesteld. Hierdoor kunnen er vertekeningen ontstaan, omdat de documenten bijvoorbeeld vanuit een bepaalde invalshoek zijn gepresenteerd door de auteurs (Bowen, 2009, pp. 31-32).

In dit onderzoek heb ik verschillende documenten onderzocht om de formele structuur van het netwerk van informatiedeling en beeldvorming inzichtelijk te kunnen maken. Het is hierbij relevant om te vermelden dat er tijdens een landelijke cybercrisis veel actoren betrokken zijn uit verschillende domeinen en er daardoor diverse documenten bestaan die wat zeggen over de aanpak van een landelijke cybercrisis. Aangezien dit onderzoek zich richt op het netwerk van informatiedeling en beeldvorming, heb ik de formele structuur van het netwerk geanalyseerd en geconstrueerd vanuit verschillende documenten die relevant zijn voor de veiligheidsregio's en haar netwerkpartners. De reden hiervoor is dat het netwerk nog niet afzonderlijk staat beschreven in de bestaande documentatie.

Een belangrijk document in dit onderzoek is het *Landelijk Crisisplan Digitaal* (LCP-Digitaal). Tijdens een landelijke cybercrisis dient het *LCP-Digitaal* als leidraad voor de actoren die zich bezighouden met het beheersen en bestrijden van de crisis. Het plan schetst de gezamenlijke crisisaanpak op nationaal niveau en brengt de bestaande afspraken en wetgeving in kaart (Veiligheidsberaad, z.d.a; NCTV, 2022a, p. 7). Het *LCP-Digitaal* wordt niet alleen gebruikt als richtlijn tijdens een landelijke cybercrisis, maar dient ook als basis voor de ISIDOOR-oefening.

Naast het *LCP-Digitaal* heb ik nog andere documenten bestudeerd die de formele structuur van het netwerk van informatiedeling en beeldvorming inzichtelijk maken. Zo is de *Koepelnotitie Crisiscommunicatie Digitaal Domein* gebruikt, die dient als aanvulling op het *LCP-Digitaal* wat betreft crisiscommunicatie (NCTV, 2023b). Bovendien is het *Nationale Handboek Crisisbeheersing* geraadpleegd, waarin de nationale crisisstructuur en de besluitvorming wordt uitgelegd (NCTV, 2022b). Daarnaast heb ik gebruikgemaakt van de *Bestuurlijke Netwerkkaarten Crisisbeheersing*, waarin de bestuurlijke verantwoordelijkheden tijdens crisisbeheersing worden beschreven (Brainich & Ten Dam, 2021).

Verder heb ik de *Whitepaper Digitale Ontwrichting en Cyber* van het Nederlands Instituut Publieke Veiligheid (NIPV) geraadpleegd voor dit onderzoek. Dit document dient als vertaalslag van het *LCP-Digitaal* en biedt richtlijnen voor de veiligheidsregio's tijdens een cybercrisis (Hooymans, 2019). Tot slot heb ik gebruikgemaakt van de *Multikaart Digitale Verstoring* van Veiligheidsregio IJsselland (in samenwerking met vier andere veiligheidsregio's) en de *Aandachtskaart Cybergevolgbestrijding/Digitale Ontwrichting* van Veiligheidsregio Utrecht (H. Schreuders, intern document, 11 maart 2024; Veiligheidsregio Utrecht, 2022). Deze documenten zijn ontworpen om de crisisfunctionarissen van de veiligheidsregio's praktische handvatten te bieden tijdens een cybercrisis. De documenten bevatten een beknopte samenvatting en dienen als vertaalslag van de kernprincipes uit het *LCP-Digitaal.* In Tabel 2 is een overzicht te vinden van de documenten die in dit onderzoek zijn gebruikt.

Documenten	Omschrijving
Landelijk Crisisplan Digitaal (LCP-Digitaal)	Schetst de gezamenlijke cybercrisisaanpak op nationaal niveau en brengt de bestaande afspraken en wetgeving in kaart
Koepelnotitie Crisiscommunicatie Digitaal Domein	Dient als verdieping op het gebied van crisiscommunicatie voor het LCP-Digitaal

Nationale Handboek Crisisbeheersing	Handboek met uitleg over de nationale crisisstructuur en besluitvorming
Bestuurlijke Netwerkkaarten Crisisbeheersing	Beschrijft de bestuurlijke verantwoordelijkheden tijdens crisisbeheersing
Whitepaper Digitale Ontwrichting en Cyber	Dient als vertaalslag van het LCP-Digitaal en biedt richtlijnen voor de veiligheidsregio's tijdens een cybercrisis
Multikaart Digitale Verstoring	Biedt praktische handvatten voor crisisfunctionarissen van de veiligheidsregio's en dient als vertaalslag van de kernprincipes uit het LCP-Digitaal
Aandachtskaart Cybergevolgbestrijding/Digitale Ontwrichting	Biedt praktische handvatten voor crisisfunctionarissen van de veiligheidsregio's en dient als vertaalslag van de kernprincipes uit het LCP-Digitaal

Tabel 2: Overzicht van de documenten die gebruikt zijn om de formele structuur helder te krijgen.

4.3.2 Semigestructureerde interviews

Een interview is een gespreksvorm waarin de onderzoeker, ook wel de interviewer, vragen stelt aan de respondent over het fenomeen dat onderzocht wordt. Een interview kan gestructureerd of juist een ongestructureerd format hebben (Van Thiel, 2014, p, 93; Boeije & Bleijenbergh, 2019, p. 74).

In dit onderzoek heb ik semigestructureerde interviews afgenomen om de ervaringen van de respondenten met de samenwerking in de praktijk inzichtelijk te kunnen maken. Een semigestructureerd interview is een vorm van kwalitatief onderzoek en een veelgebruikte methode om percepties, ervaringen en betekenissen van respondenten beter te kunnen onderzoeken en begrijpen (Van Thiel, 2014, p. 94). Bij semigestructureerde interviews wordt meestal een topiclijst gebruikt als richtlijn. Deze lijst bevat bepaalde thema's met vragen die besproken kunnen worden met de respondent. De topiclijst van dit onderzoek is terug te vinden in Bijlage A en is gevormd om inzicht te krijgen in de ervaringen van respondenten met de samenwerking in de praktijk. Naast de topiclijst bieden semigestructureerde interviews ook de mogelijkheid om aanvullende vragen te stellen aan de respondenten. Op deze manier kan er diepgaande informatie verkregen worden en kunnen er nieuwe inzichten ontstaan (Van Thiel, 2014, p. 95).

4.3.3 Respondentenselectie

Een goede respondentenselectie is belangrijk om de juiste datagegevens te kunnen verzamelen. In dit onderzoek heb ik 23 respondenten geselecteerd voor de semigestructureerde interviews. Aangezien een landelijke cybercrisis niet vaak plaatsvindt, is ervoor gekozen om respondenten te interviewen die betrokken zijn geweest bij de ISIDOOR-oefening in november 2023. Omdat dit onderzoek een ingebedde case study structuur bevat, is ernaar gestreefd om zoveel mogelijk verschillende actoren uit het netwerk van informatiedeling en beeldvorming te spreken over hun ervaringen met de samenwerking in de praktijk. Hierbij is er specifiek aandacht voor Veiligheidsregio IJsselland, aangezien zij de opdrachtgever zijn van dit onderzoek en om een beter beeld te kunnen krijgen over de positie die veiligheidsregio's innemen binnen het netwerk.

Tabel 3 op de volgende pagina presenteert een overzicht van de afgenomen semigestructureerde interviews. De interviews hebben plaatsgevonden met respondenten van de veiligheidsregio's

IJsselland, Kennemerland, Utrecht, Rotterdam-Rijnmond, Amsterdam-Amstelland en Noord-Holland Noord. Daarnaast zijn er interviews afgenomen met respondenten van de gemeente Zwolle en Ommen, het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC), het Landelijk Operationeel Coördinatie Centrum (LOCC), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Crisiscentrum (NCC). Tot slot heeft er nog een interview plaatsgevonden met een respondent van het Nederlands Instituut Publieke Veiligheid (NIPV), omdat deze respondent de ISIDOOR-oefening heeft geëvalueerd.

Respondent	Datum & tijd	Organisatie
1	12 juli 2024 om 11:00-12:00	Veiligheidsregio IJsselland
2	24 juli 2024 om 11:00-11:45	Veiligheidsregio IJsselland
3	26 juli 2024 om 11:00-12:30	Veiligheidsregio IJsselland
4	29 juli 2024 om 09:00-10:30	Veiligheidsregio IJsselland
5	29 juli 2024 om 09:00-10:30	Veiligheidsregio IJsselland
6	29 juli 2024 om 14:30-15:30	Veiligheidsregio IJsselland
7	12 augustus 2024 om 09:30-10:30	Gemeente Zwolle
8	12 augustus 2024 om 14:00-15:00	Veiligheidsregio IJsselland
9	14 augustus 2024 om 09:00-10:00	VR-ISAC
10	14 augustus 2024 om 13:00-14:00	VR-ISAC
11	15 augustus 2024 om 13:00-14:00	NCTV
12	15 augustus 2024 om 13:00-14:00	NCC
13	15 augustus 2024 om 15:00-16:00	NIPV
14	19 augustus 2024 om 14:00-16:00	Veiligheidsregio Kennemerland
15	20 augustus 2024 om 10:00-10:30	Gemeente Ommen
16	20 augustus 2024 om 11:30-12:00	Veiligheidsregio Utrecht
17	22 augustus 2024 om 10:00-11:00	Veiligheidsregio Rotterdam-Rijnmond
18	22 augustus 2024 om 13:00-14:00	Veiligheidsregio Utrecht
19	27 augustus 2024 om 10:00-11:00	LOCC
20	27 augustus 2024 om 10:00-11:00	LOCC
21	29 augustus 2024 om 11:00-12:00	Veiligheidsregio Amsterdam-Amstelland
22	30 augustus 2024 om 09:00-10:00	Veiligheidsregio Noord-Holland Noord
23	5 september 2024 om 12:00-13:00	Veiligheidsregio Rotterdam-Rijnmond

Tabel 3: Respondentenlijst voor de semigestructureerde interviews.

Het selecteren van de respondenten heb ik gedaan op basis van de gevoerde gesprekken met mijn stagebegeleider vanuit Veiligheidsregio IJsselland. Deze stagebegeleider is tevens operationeel leider geweest tijdens de ISIDOOR-oefening en aan hem heb ik gevraagd welke respondenten vanuit Veiligheidsregio IJsselland het beste benaderd konden worden. Op basis hiervan heb ik de eerste respondenten geselecteerd en benaderd. Daarnaast heb ik ook gebruikgemaakt van de zogenoemde sneeuwbalmethode. Dit is een methode waarbij de onderzoeker aan het einde van het gesprek aan de respondent vraagt of hij/zij nog aanvullende suggesties heeft voor nieuwe respondenten. Om een zo volledig mogelijk en gebalanceerd beeld te kunnen krijgen van het netwerk van informatiedeling en beeldvorming, heb ik geprobeerd om zoveel mogelijk respondenten te spreken vanuit verschillende organisaties.

De respondenten zijn benaderd via e-mail. Wanneer er geen reactie kwam, heb ik telefonisch contact opgenomen. De 23 semigestructureerde interviews zijn afgenomen in de maanden juli,

augustus en september en vonden fysiek of online plaats. Ondanks dat de voorkeur uitging naar fysieke interviews, hebben de meeste interviews online plaatsgevonden. De voornaamste reden hiervoor was de reisafstand. De interviews hadden een gemiddelde duur van één uur en vooraf aan elk interview is om toestemming gevraagd om het gesprek op te nemen.

4.4 Operationalisatie

Voor de juiste verzameling van datagegevens heb ik de theoretische concepten uit Hoofdstuk 3 geoperationaliseerd naar meetbare indicatoren. De concepten van dit onderzoek bestaan uit de formele structuur en de samenwerking in de praktijk. Deze twee concepten heb ik aan de hand van de wetenschappelijke literatuur uitgewerkt in verschillende dimensies. Uit deze dimensies zijn vervolgens een aantal indicatoren afgeleid, die gemeten zijn in empirie.

4.4.1 Operationalisatie van de formele structuur

Bij het operationaliseren van concepten is het belangrijk om te benoemen hoe je tot bepaalde indicatoren bent gekomen. Op basis van de theorie in Hoofdstuk 3 heb ik de formele structuur onderverdeeld in twee overkoepelende dimensies: de samenstelling en formele werkwijze én sturing en besluitvorming. Deze overkoepelende dimensies zijn verder uitgewerkt in dimensies en indicatoren.

De overkoepelende dimensie samenstelling en formele werkwijze bestaat uit drie dimensies. De eerste dimensie gaat over actoren. Aan de hand van de literatuur van Koppenjan & Klijn (2004) en Ansell & Gash (2007) kan deze dimensie geoperationaliseerd worden naar één meetbare indicator: de formeel betrokken actoren binnen het netwerk. De tweede dimensie gaat over de formele werkwijze en relaties. Deze dimensie is volgens Ansell & Gash (2007) en Koppenjan & Klijn (2004) te herkennen aan de formeel vastgelegde rollen, taken en verantwoordelijkheden van actoren en de regels en procedures binnen een netwerk. De laatste dimensie betreft de vergader- en communicatiestructuur en kan volgens Ansell & Gash (2007) gemeten worden aan de hand van de frequentie van bijeenkomsten en de wijze waarop men communiceert.

De overkoepelende dimensie sturing en besluitvorming bestaat uit twee dimensies: de wijze van sturing en besluitvorming. De wijze van sturing binnen een netwerk kan volgens Kenis & Provan (2008) herkend worden aan het type netwerksturing. Daarnaast heb ik de indicator formele werkwijze van sturing aanvullend toegevoegd, omdat het relevant is om te bestuderen hoe de wijze van sturing formeel is vastgelegd binnen het netwerk van informatiedeling en beeldvorming. Deze toegevoegde indicator is gebaseerd op een aantal verkennende gesprekken met medewerkers van Veiligheidsregio IJsselland. De dimensie besluitvorming wordt volgens Koppenjan & Klijn (2004) bepaalt door de totstandkoming van besluiten tussen actoren en de formele bevoegdheden die specifieke actoren hebben om beslissingen te mogen nemen binnen een netwerk. In Tabel 4 is het operationaliseringsschema van de formele structuur te vinden.

Dimensies	Indicatoren	Meetinstrument
Overkoepelende dimensie: samenstelling & formele werkwijze		
Actoren	Formeel betrokken actoren	Documentenanalyse
Formele taken & relaties	Rollen, taken en verantwoordelijkheden	Documentenanalyse

	Regels en procedures	
Vergader- & communicatiestructuur	Frequentie van bijeenkomsten	Documentenanalyse
	Formele wijze van communicatie	
Overkoepelende dimensie: sturing & besluitvorming		
Wijze van sturing	Type netwerkstructuur	Documentenanalyse
	Formele werkwijze sturing	
Besluitvorming	Totstandkoming van besluitvorming tussen actoren	Documentenanalyse
	Formele bevoegdheden van actoren om beslissingen te mogen nemen	

Tabel 4: Operationaliseringsschema van de formele structuur.

4.4.2 Operationalisatie van de samenwerking in de praktijk

Op basis van het theoretisch raamwerk van Ansell & Gash (2007) bestaat de samenwerking in de praktijk uit zeven dimensies. Het gaat hierbij om startcondities, face-to-face dialoog, vertrouwen, gedeelde betekenisgeving, toewijding aan het proces en faciliterend leiderschap. Deze dimensies zijn verder uitgewerkt in meetbare indicatoren.

Startcondities worden volgens Ansell & Gash (2007) gekenmerkt door prikkels om samen te werken, onbalans van macht en middelen en de voorgeschiedenis van de samenwerking. Daarnaast is het element institutioneel ontwerp van Ansell & Gash (2007) ondergebracht binnen deze dimensie. Hierin worden betrokken actoren en een duidelijke formele structuur als belangrijke meetbare indicatoren genoemd (Ansell & Gash, 2007; Van Delden, 2009; Alexander et al., 1998; Koppenjan & Klijn, 2004).

Dan de dimensie die gaat over de face-to-face dialoog. Ansell & Gash (2007) benoemen in hun literatuur niet expliciet indicatoren waarmee je de face-to-face dialoog in de empirie kan meten. Uit de literatuur kan afgeleid worden dat de face-to-face dialoog gemeten kan worden aan de hand van de wijze van communicatie en informatie-uitwisseling. Goldsmith & Eggers (2004) benadrukken daarnaast dat het spreken van dezelfde vaktaal een belangrijke indicator is.

Volgens Ansell & Gash (2007), Klijn et al. (2010) en Provan & Kenis (2008) is vertrouwen te onderscheiden in vertrouwen in de kwaliteit van actoren en het opbouwen van onderling vertrouwen. Van Delden (2009) voegt hieraan toe dat het vertrouwen in het nakomen van afspraken eveneens een belangrijke indicator vormt.

De vierde dimensie betreft gedeelde betekenisgeving. Volgens Ansell & Gash (2007) kan deze dimensie herkend worden aan de hand van een gemeenschappelijke probleemdefinitie. Provan & Kenis (2008) spreken bij gedeelde betekenisgeving ook wel over het afstemmen van gemeenschappelijke doelen.

Bij toewijding aan het proces wordt de mate van betrokkenheid als belangrijke indicator beschouwd (Ansell & Gash, 2007; Emerson & Nabatchi, 2015). Daarnaast kan toewijding aan het proces ook herkend worden aan het gevoel van gedeeld eigenaarschap onder de actoren en de onderlinge afhankelijkheid die de samenwerking vereist.

Het belang van tussentijdse resultaten wordt beschreven door Ansell & Gash (2007), die stellen dat het delen van tussentijdse resultaten de kans op succesvolle samenwerking vergroot. Bryson

et al. (2006) benadrukken daarnaast dat de samenwerking geoptimaliseerd kan worden door lessen te trekken uit de gedeelde tussentijdse resultaten.

Tot slot de dimensie faciliterend leiderschap. Ansell & Gash (2007) beschrijven in hun literatuur dat het belangrijk is dat de leider de actoren bij elkaar brengt en werkt aan het versterken van het onderling vertrouwen. Daarnaast wordt het faciliteren van communicatie tussen actoren als een belangrijke indicator beschouwd door Ansell & Gash (2007). Bryson et al. (2015) voegen hieraan toe dat een leider in staat moet zijn om verschillende vaktalen te spreken en deze met elkaar te verbinden. Tabel 5 weergeeft het operationaliseringsschema van de samenwerking in de praktijk.

Dimensies	Indicatoren	Meetinstrument
Startcondities	Betrokken actoren	Semigestructureerde interviews
	Duidelijke plannen	
	Prikkels om samen te werken	
	Onbalans van macht en middelen	
	Voorgeschiedenis van de samenwerking	
Face-to-face dialoog	Wijze van communicatie en informatiedeling	Semigestructureerde interviews
	Spreken van dezelfde vaktaal	
Vertrouwen	Vertrouwen in de kwaliteit van actoren	Semigestructureerde interviews
	Vertrouwen in het nakomen van afspraken	
	Opbouwen van onderling vertrouwen tussen actoren	
Gedeelde betekenisgeving	Gemeenschappelijke probleemdefinitie	Semigestructureerde interviews
	Gemeenschappelijke doelen	
Toewijding aan het proces	Betrokkenheid binnen het netwerk	Semigestructureerde interviews
	Onderlinge afhankelijkheid	
	Gevoel van gedeeld eigenaarschap	
Tussentijdse resultaten	Delen van de tussentijdse resultaten	Semigestructureerde interviews
	Leren van de tussentijdse resultaten	
Faciliterend leiderschap	Faciliteren van communicatie tussen actoren	Semigestructureerde interviews
	Versterken van onderling vertrouwen	
	Begrijpen van verschillende vaktalen en deze met elkaar verbinden	

Tabel 5: Operationaliseringsschema van de samenwerking in de praktijk.

4.5 Data-analyse

Na het verzamelen van de datagegevens volgt de data-analyse. Het analyseren van data is een proces waarin de datagegevens worden geordend, gestructureerd en geïnterpreteerd. Volgens Boeije & Bleijenbergh (2019) vergroot een data-analyse het inzicht van de onderzoeker in het onderwerp, waardoor er antwoord kan worden gegeven op de onderzoeksvraag en de resultaten gerapporteerd kunnen worden (Boeije & Bleijenbergh, 2019, p. 75). De datagegevens uit de documentenanalyse heb ik gecodeerd op basis van de indicatoren die tot de formele structuur behoren. Aangezien deze indicatoren voldoende houvast boden heeft de interpretatie hiervan direct plaatsgevonden, zonder analytische tussenstap.

De semigestructureerde interviews heb ik opgenomen via de dictafoon op de telefoon en via Microsoft Teams. Hierbij heb ik vooraf toestemming gevraagd aan de respondenten om het gesprek te mogen opnemen. De geluidsopnamen heb ik vervolgens getranscribeerd in Microsoft Word en opgeslagen binnen een beveiligde omgeving: *RIS for Students*. De semigestructureerde interviews heb ik door middel van een thematische analyse op een abductieve wijze geanalyseerd. Thematisch analyseren is een methode voor het identificeren, rapporteren en analyseren van bepaalde patronen (thema's) binnen de verzamelde datagegevens. Binnen deze methode is er ruimte voor de interpretatie van datagegevens door de onderzoeker. Bij een abductieve analyse worden bestaande theorieën gebruikt om de dataverzamelingsfase in te gaan (deductieve benadering). Vervolgens worden nieuwe inzichten uit de verzamelde datagegevens vergaart (inductieve benadering) (Braun & Clarke, 2006, pp. 79-81).

In dit onderzoek ben ik dataverzameling ingegaan aan de hand van de theoretische inzichten. Gezien de hoeveelheid transcripten heb ik de datagegevens in eerste instantie op een deductieve manier gecodeerd met verschillende kleuren in Microsoft Word. Uiteindelijk bleek deze benadering onvoldoende te zijn om de verzamelde datagegevens volledig te kunnen begrijpen. Dit probleem heb ik opgelost door op een inductieve wijze te gaan werken naar thema's, die uit de data naar voren komen. Een voorbeeld hiervan zijn de dimensies vertrouwen en faciliterend leiderschap. In de praktijk blijken deze dimensies met elkaar samen te hangen, waardoor ik ze heb gebundeld onder één thema: leiderschap en vertrouwen. Gedeelde betekenisgeving heb ik ondergebracht onder de thema's communicatie en toewijding aan het proces.

4.6 Kwaliteit van het onderzoek

Om de kwaliteit van dit onderzoek te waarborgen, is er gekeken naar de betrouwbaarheid en de validiteit van dit onderzoek.

4.6.1 Betrouwbaarheid

De betrouwbaarheid van een onderzoek heeft betrekking op de nauwkeurigheid en consistentie van de metingen in de empirie. Hoe nauwkeuriger en consistenter deze metingen zijn, hoe meer zekerheid er is dat de bevindingen niet op toeval berusten. Nauwkeurigheid verwijst naar het gebruik van betrouwbare meetinstrumenten binnen een onderzoek. Dit moet zo nauwkeurig mogelijk vastgelegd worden (Van Thiel, 2014, p. 48). Consistentie duidt op de herhaalbaarheid van een onderzoek. Een onderzoek wordt als consistent beschouwd wanneer deze onder vergelijkbare omstandigheden herhaald kan worden en tot dezelfde bevindingen leidt. Dit vergroot de betrouwbaarheid van het onderzoek, omdat het aantoont dat de gevonden bevindingen kloppen (Van Thiel, 2014, pp. 48-49).

Binnen dit onderzoek heb ik een aantal activiteiten ondernomen om de betrouwbaarheid van dit onderzoek te vergroten. De nauwkeurigheid van de metingen zijn binnen dit onderzoek gewaarborgd door middel van de operationalisatie van theoretische concepten naar meetbare indicatoren en het opstellen van een topiclijst. Daarnaast heb ik ervoor gekozen om zo veel mogelijk respondenten te interviewen, om de kans op toeval in de bevindingen te verminderen en de betrouwbaarheid en representativiteit van de bevindingen te vergroten. Alle interviews zijn op een systematische wijze afgenomen. Dit betekent dat in elk interview dezelfde topics zijn behandeld, wat zorgt voor minder variabiliteit in de antwoorden. Naast de vooraf opgestelde topiclijst was er ook nog ruimte voor aanvullende vragen tijdens de interviews. De

interviews zijn opgenomen en vervolgens getranscribeerd in Microsoft Word, waardoor de data controleerbaar is.

De consistentie van dit onderzoek heb ik gewaarborgd door de verschillende methodologische keuzes en stappen te documenteren en te verantwoorden. Dit vergroot de transparantie en zorgt ervoor dat toekomstige onderzoekers in staat zijn om het onderzoek te herhalen. Een nadeel hierbij is het gebruik van semigestructureerde interviews in dit onderzoek. De aanvullende vragen kunnen niet worden overgenomen, omdat ze afhankelijk zijn van de context waarin het gesprek plaatsvond. Dit kan bij herhaling van dit onderzoek tot andere resultaten leiden.

4.6.2 Validiteit

Validiteit gaat over de vraag of je meet wat je beoogt te meten. Hierbij wordt onderscheid gemaakt tussen interne validiteit en externe validiteit. Interne validiteit focust zich op de geloofwaardigheid van het onderzoek, waarbij de onderzoeker zich afvraagt of de bevindingen te wijten zijn aan de gemeten variabelen (Bleijenbergh, 2013, p. 110). Externe validiteit gaat over de representativiteit van de bevindingen en de vraag of deze generaliseerbaar zijn voor een grotere populatie (Bleijenbergh, 2013, p. 111; Findley et al., 2021, p. 368).

Om de interne validiteit van dit onderzoek te waarborgen, heb ik de theoretische concepten die gaan over de formele structuur en de samenwerking in de praktijk uitgebreid beschreven in Hoofdstuk 3. Deze concepten heb ik vervolgens in Hoofdstuk 4 geoperationaliseerd naar meetbare indicatoren. Volgens Van Thiel (2014) zorgt het operationaliseren van de theoretische concepten voor een hogere interne validiteit. Vanuit de operationalisatie heb ik in dit onderzoek vragen geformuleerd voor de semigestructureerde interviews. Door het stellen van deze vragen aan de respondenten heb ik gemeten wat er beoogd werd te meten (Van Thiel, 2014, pp. 49-50). Naast de opgestelde interviewvragen was er nog ruimte voor het stellen van open vragen, wat belangrijk was voor het verzamelen van extra informatie en het interpreteren van de subjectieve ervaringen van de respondenten (Bleijenbergh, 2013, p. 110). De interne validiteit van de documentenanalyse heb ik in dit onderzoek gewaarborgd door specifieke documenten en rapporten te selecteren die relevant zijn voor dit onderzoek. Daarnaast heb ik enkel documenten en rapporten vanuit betrouwbare bronnen geraadpleegd, wat de interne validiteit vergroot.

Externe validiteit verwijst naar de generaliseerbaarheid van een onderzoek. In dit onderzoek is er sprake van een enkelvoudige case study met een ingebedde structuur, omdat het netwerk van informatiedeling en beeldvorming bestaat uit verschillende actoren. Aangezien een landelijke cybercrisis vrij uniek is en er nog weinig ervaring is opgedaan met het bestrijden ervan, zijn de bevindingen van dit onderzoek statistisch gezien beperkt generaliseerbaar naar andere samenwerkingen in crisissituaties. De theoretische inzichten en dynamieken uit dit onderzoek zijn daarentegen wel analytisch generaliseerbaar. Het is aannemelijk dat bij vergelijkbare complexe crisissituaties soortgelijke problemen, uitdagingen en dynamieken zullen ontstaan.

H5| Resultaten

In dit hoofdstuk presenteer ik de resultaten van dit onderzoek. Allereerst wordt de formele structuur van het netwerk van informatiedeling en beeldvorming inzichtelijk gemaakt. Vervolgens worden de ervaringen van de respondenten met de samenwerking in de praktijk besproken. Het hoofdstuk sluit af met een analyse van de verhouding tussen de formele structuur en de samenwerking in de praktijk en welke factoren hierbij een rol spelen.

5.1 Formele structuur van het netwerk

In deze paragraaf staat de volgende deelvraag centraal: '*Hoe is de formele structuur van het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis ingericht?*'

5.1.1 Samenstelling & formele werkwijze

Onder de overkoepelende dimensie samenstelling en formele werkwijze vallen drie dimensies. De eerste dimensie beschrijft de actoren die betrokken zijn bij het netwerk van informatiedeling en beeldvorming, de tweede dimensie richt zich op de formele taken & relaties van actoren en de derde dimensie gaat over de vergader- & communicatiestructuur.

Dimensie 1: actoren

Aangezien dit onderzoek wordt uitgevoerd in opdracht van Veiligheidsregio IJsselland, kan er vooraf worden gesteld dat zij een betrokken actor zijn binnen het netwerk. De andere betrokken actoren worden hieronder geanalyseerd aan de hand van de geselecteerde documenten.

<u>Landelijk Crisisplan Digitaal (LCP-Digitaal)</u>

Zoals beschreven in Hoofdstuk 4 dient het *LCP-Digitaal* als leidraad voor actoren die zich bezighouden met het beheersen en bestrijden van een landelijke cybercrisis. Dit crisisplan schetst onder andere de nationale crisisstructuur en biedt richtlijnen voor een gezamenlijke aanpak. Het is hierbij belangrijk om te vermelden dat het *LCP-Digitaal* niet alleen gericht is op de betrokken actoren binnen het netwerk van informatiedeling en beeldvorming, maar ook op andere publieke en private organisaties die verbonden zijn aan de nationale crisisstructuur. Om deze reden worden er in het *LCP-Digitaal* verschillende samenwerkingsstructuren beschreven en gevisualiseerd (NCTV, 2022a, p. 8). Om deze structuren beter te kunnen begrijpen, worden ze hieronder kort toegelicht.

In het *LCP-Digitaal* wordt er onderscheid gemaakt tussen samenwerking binnen de functionele en algemene keten. Actoren binnen de functionele keten richten zich met name op het bestrijden van de oorzaak van de cybercrisis en actoren binnen de algemene keten zijn verantwoordelijk voor de gevolgbestrijding en het handhaven van de openbare orde en veiligheid. Bij opschaling naar de nationale crisisstructuur worden deze twee ketens met elkaar verbonden (NCTV, 2022a, pp. 15-26; Veiligheidsregio IJsselland, 2022, p. 5). Een visualisatie hiervan is opgenomen in Bijlage B (Figuur B1).

Wat opvalt is dat Figuur B1 een complexe samenwerkingsstructuur laat zien tussen de functionele en algemene keten. Deze complexe structuur zorgt ervoor dat het niet duidelijk is welke actoren betrokken zijn bij het netwerk van informatiedeling en beeldvorming, waardoor Figuur B1 niet bruikbaar is voor dit onderzoek. Daarentegen biedt de tekst van het *LCP-Digitaal* wel meer inzicht. Hieruit kan worden opgemaakt dat niet alleen Veiligheidsregio

IJsselland deel uitmaakt van het netwerk van informatiedeling en beeldvorming, maar de andere 24 veiligheidsregio's ook.

Daarnaast wordt uit de tekst van het *LCP-Digitaal* duidelijk dat veiligheidsregio's tijdens een landelijke cybercrisis contact hebben met het Landelijk Operationeel Coördinatiecentrum (LOCC), het Nationaal Crisiscentrum (NCC) en het Nationaal Kernteam Crisiscommunicatie (NKC). Deze actoren zijn allemaal actief binnen de algemene keten en wisselen informatie met elkaar uit om een Landelijk Operationeel Beeld (LOB) van de crisissituatie te kunnen vormen (NCTV, 2022a, pp. 28-29). Verder blijkt uit de tekst dat het Nationaal Cyber Security Centrum (NCSC) vanuit de functionele keten ook een bijdrage levert aan het vormen van een LOB. Dit komt doordat zij valide informatie over de oorzaak van de cybercrisis verstrekken aan het NCC. Daarnaast staat het NCSC in direct contact met het NKC tijdens een landelijke cybercrisis (NCTV, 2022a, p. 17). Om deze redenen wordt het NCSC in dit onderzoek wel beschouwd als een betrokken actor binnen het netwerk van informatiedeling en beeldvorming.

<u>Whitepaper Digitale Ontwrichting en Cyber</u>
Om een duidelijker beeld te kunnen creëren van de betrokken actoren binnen het netwerk van informatiedeling en beeldvorming, is er ook gebruik gemaakt van de *Whitepaper Digitale Ontwrichting en Cyber*. Zoals eerder beschreven geeft dit document een inzicht in het cybernetwerk van veiligheidsregio's en biedt het een houvast aan de crisisfunctionarissen (Hooymans, 2019, p. 7). Een voordeel van dit document is dat het zich specifiek richt op cybergevolgbestrijding, waardoor de samenwerkingsstructuur tussen netwerkpartners minder complex staat afgebeeld dan in het *LCP-Digitaal*. Dit maakt het makkelijker om te bepalen welke actoren betrokken zijn bij het netwerk van informatiedeling en beeldvorming. Een visualisatie van deze samenwerkingsstructuur is opgenomen in Bijlage C (Figuur C1).

Figuur C1 toont aan dat het netwerk van informatiedeling en beeldvorming grotendeels overeenkomt met de beschrijvingen in het *LCP-Digitaal*. Wel valt het op dat veiligheidsregio's in Figuur C1 een directe communicatielijn hebben met de Rijksdiensten, terwijl dit niet staat beschreven in de andere geselecteerde documenten. De Rijksdiensten worden daarom niet gezien als betrokken actor binnen dit onderzoek. Verder valt het op dat Figuur C1 geen directe communicatielijn visualiseert tussen de veiligheidsregio's en het Nationaal Kernteam Crisiscommunicatie (NKC). Deze directe communicatielijn wordt in de tekst van het *LCP-Digitaal* wel duidelijk benadrukt. Aangezien het *LCP-Digitaal* een recentere uitgave is, wordt deze directe communicatielijn wel als uitgangspunt genomen in dit onderzoek.

<u>Multikaart Digitale Verstoring & Aandachtskaart Cybergevolgbestrijding</u>
Naast de bovengenoemde documenten zijn in dit onderzoek ook de *Multikaart Digitale Verstoring* van Veiligheidsregio IJsselland en de *Aandachtskaart Cybergevolgbestrijding* van Veiligheidsregio Utrecht geanalyseerd. Deze documenten dienen als een praktische vertaalslag van het *LCP-Digitaal* en benoemen relevante actoren waarmee veiligheidsregio's samenwerken tijdens een cybercrisis. Ook in deze twee documenten worden het Nationaal Crisiscentrum (NCC), het Landelijk Operationeel Coördinatie Centrum (LOCC), het Nationaal Kernteam Crisiscommunicatie (NKC) en het Nationaal Cyber Security Centrum (NCSC) aangehaald als belangrijke schakels binnen het netwerk van informatiedeling en beeldvorming (H. Schreuders, intern document, 11 maart 2024; Veiligheidsregio Utrecht, 2022, p. 1).

Wat wel opvalt is de vermelding van het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) in beide documenten. Volgens deze documenten richt het VR-ISAC zich voornamelijk op de cyberweerbaarheid van de interne organisatie, maar kan het tijdens een landelijke cybercrisis ook bijdragen aan de informatiepositie van de crisisorganisatie (H. Schreuders, intern document, 11 maart 2024; Veiligheidsregio Utrecht, 2022, p. 3). Deze externe rol van het VR-ISAC wordt niet beschreven in de andere geselecteerde documenten van dit onderzoek. Bovendien hebben de veiligheidsregio's deze externe rol zelf geformuleerd in de documenten, maar dat wil nog niet zeggen dat de andere actoren er ook zo over denken. Om deze redenen wordt het VR-ISAC niet meegenomen als formele betrokken actor binnen het netwerk van informatiedeling en beeldvorming.

Kortom, op basis van de bovenstaande informatie kan geconcludeerd worden dat de **25 veiligheidsregio's**, het **LOCC**, het **NCC**, het **NKC** en het **NCSC** formeel betrokken zijn bij het netwerk van informatiedeling en beeldvorming. Een visuele weergave van dit formele netwerk wordt in subparagraaf 5.1.2 gepresenteerd.

Dimensie 2: formele taken & relaties

Nu we weten welke actoren formeel onderdeel uitmaken van het netwerk van informatiedeling en beeldvorming, is het belangrijk om te achterhalen wat hun formele taken en relaties zijn.

Veiligheidsregio's

In het *LCP-Digitaal* staat beschreven dat veiligheidsregio's tijdens een landelijke cybercrisis de verantwoordelijkheid dragen voor het waarborgen van de continuïteit van de samenleving. Dit omhelst niet alleen het bestrijden van de gevolgen van de crisis in de maatschappij, maar ook het bieden van handelingsperspectief aan de inwoners. Om deze taken uit te kunnen voeren richten veiligheidsregio's zich, samen met actoren uit het netwerk, op het delen van informatie en het vormen van een Landelijk Operationeel Beeld (LOB) van de crisissituatie (NCTV, 2022a, pp. 28-29).

Landelijk Operationeel Coördinatiecentrum (LOCC)

Volgens het *LCP-Digitaal* bestaat het LOCC uit professionals vanuit verschillende organisaties, zoals de veiligheidsregio's, brandweer, politie, Geneeskundige Hulpverleningsorganisatie in de Regio (GHOR) en de gemeenten. Tijdens een landelijke cybercrisis heeft het LOCC een aantal verschillende taken. Zo bieden ze ondersteuning aan crisisorganisaties, zijn ze verantwoordelijk voor het aanleveren van een Landelijk Operationeel Beeld (LOB) en geven ze operationeel advies ten behoeve van besluitvorming op ambtelijk en politiek-bestuurlijk niveau (NCTV, 2022a, p. 28).

Voor het netwerk van informatiedeling en beeldvorming is de taak van het vormen van een Landelijk Operationeel Beeld (LOB) van belang. Om deze taak goed uit te kunnen voeren werkt het LOCC nauw samen met het Nationaal Crisiscentrum (NCC) en de veiligheidsregio's (NCTV, 2022a, p. 49). Het LOCC functioneert binnen het netwerk als verbindende schakel en zorgt ervoor dat iedere actor tijdens een landelijke cybercrisis over dezelfde informatie beschikt (Rijksoverheid, z.d.b).

Nationaal Crisiscentrum (NCC)
Uit het *LCP-Digitaal* blijkt dat het NCC tijdens een landelijke cybercrisis functioneert als een interdepartementaal coördinatiecentrum. Dit houdt in dat het NCC het knooppunt vormt voor bestuurlijke informatievoorziening en crisiscommunicatie. Daarnaast ondersteunt het NCC de crisisbesluitvorming op ambtelijk en politiek-bestuurlijk niveau (NCTV, 2022a, p. 27).

Volgens het *Nationaal Handboek Crisisbeheersing* heeft het NCC tijdens een landelijke cybercrisis twee belangrijke hoofdtaken. De eerste taak is het ondersteunen van de nationale crisisstructuur. Daarbij treedt het NCC op als bewaker voor het proces van coördinatie en besluitvorming op landelijk niveau en zorgen ze voor de koppeling tussen de algemene kolom en de functionele keten (NCTV, 2022b, p. 26). Deze taak is minder relevant voor het netwerk van informatiedeling en beeldvorming.

Daarentegen is de tweede taak van het NCC wel van belang voor het netwerk. Deze taak richt zich op informatievoorziening. Zo is het NCC vanuit het Rijk verantwoordelijk voor de totstandkoming van het Landelijk Operationeel Beeld (LOB) van de crisissituatie (NCTV, 2022b, p. 27). Daarnaast functioneert het NCC volgens het *LCP-Digitaal* als een 24/7 informatieloket en contactpunt vanuit het Rijk en staan zij tijdens een landelijke cybercrisis in rechtstreekse verbinding met de veiligheidsregio's, het Nationaal Cyber Security Centrum (NCSC) en het Landelijk Operationeel Coördinatie Centrum (LOCC) (NCTV, 2022a, p. 27).

Nationaal Cyber Security Centrum (NCSC)
Volgens het *LCP-Digitaal* maakt het NCSC onderdeel uit van de functionele keten en opereert het tijdens een landelijke cybercrisis als het nationale Computer Emergency Response Team (CERT). Dit betekent dat het NCSC technisch onderzoek uitvoert naar de oorzaak van de crisis (NCTV, 2022a, p. 11).

Daarnaast functioneert het NCSC als informatieknooppunt en expertisecentrum. Tijdens een landelijke cybercrisis beschikt het NCSC over valide informatie over de oorzaak van de crisis en verdere ontwikkelingen. Deze informatie wordt enkel verstrekt aan het Rijk en vitale partners. Vitale partners zijn organisaties die diensten leveren waarvan de continuïteit van vitaal belang is voor de maatschappij (NCTV, 2022a, p. 18). Aangezien veiligheidsregio's niet als vitale partners zijn aangemerkt door het Rijk, informeert het NCSC hen niet rechtstreeks en kunnen zij ook geen direct contact opnemen met het NCSC. Belangrijke informatie van het NCSC wordt via het Nationaal Crisiscentrum (NCC) gedeeld met actoren binnen het netwerk van informatiedeling en beeldvorming (Weerwind, 2018, p. 6; NCTV, 2022a, p. 49).

Nationaal Kernteam Crisiscommunicatie (NKC)
In het *LCP-Digitaal* staat beschreven dat zodra er wordt opgeschaald naar de nationale crisisstructuur, het NKC wordt geactiveerd met professionals vanuit het Nationaal Crisiscentrum (NCC) en betrokken departementen. Tijdens een landelijke cybercrisis is het NKC namens het Rijk verantwoordelijk voor de coördinatie en de ontwikkeling van crisiscommunicatie. Dit doen zij op basis van informatie uit het Landelijk Operationeel Beeld (LOB) (NCTV, 2022a, pp. 27-32).

Crisiscommunicatie richt zich op betekenisgeving, schadebeperking en het beantwoorden van de maatschappelijke informatiebehoefte. Hierbij is het vertalen van technische informatie over

de oorzaak van de crisis naar begrijpelijke kernboodschappen belangrijk. Daarom werkt het NKC nauw samen met het Nationaal Cyber Security Centrum (NCSC), omdat zij deze technische informatie kunnen duiden (NCTV, 2022a, pp. 31-32). Vervolgens stemt het NKC de ontwikkelde kernboodschappen af met de veiligheidsregio's (NCTV, 2023b, p. 18).

Dimensie 3: vergader- & communicatiestructuur

Nu het duidelijk is welke actoren betrokken zijn bij het netwerk van informatiedeling en beeldvorming en wat hun respectievelijke taken en relaties zijn, richt deze dimensie zich op de vergader- en communicatiestructuur van het netwerk.

Frequentie & functie van bijeenkomsten

Op basis van *LCP-Digitaal* en de *Whitepaper Digitale Ontwrichting en Cyber* kan worden opgemaakt dat het netwerk van informatiedeling en beeldvorming niet vaak bijeenkomt. Het netwerk komt in de warme fase in actie tijdens een daadwerkelijke landelijke cybercrisis en in de koude fase komen ze bijeen tijdens ISIDOOR-oefening (NCTV, 2022a, p. 8; Hooymans, 2019, p. 7). Aangezien een cybercrisis een nieuw type crisis is en nog niet vaak op landelijk niveau heeft plaatsgevonden, wordt de ISIDOOR-oefening in dit onderzoek gezien als de belangrijkste formele bijeenkomst waarin het netwerk samenkomt (Van der Varst et al., 2020, p. 14).

Zoals eerder vermeld is ISIDOOR een grootschalige cybercrisisoefening dat eens in de twee jaar wordt georganiseerd door het Nationaal Cyber Security Centrum (NCSC), de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Instituut voor Veiligheids- en Crisismanagement (COT). De ISIDOOR-oefening biedt aan het netwerk van informatiedeling en beeldvorming de gelegenheid om de vastgelegde procedures en regels te toetsen en om de samenwerking en informatie-uitwisseling binnen het netwerk te verbeteren (Broeders & Van der Varst, 2024, p. 4). De meest recente editie vond plaats van 13 tot en met 15 november 2023. Na afloop is ISIDOOR-oefening geëvalueerd, met als doel om de landelijke crisisrespons te verbeteren en te leren van de verbeterpunten (COT, 2024, p. 6).

Formele wijze van communicatie

Op basis van het *LCP-Digitaal* en de *Koepelnotitie Crisiscommunicatie Digitaal Domein* kan gesteld worden dat er twee verschillende manieren van communicatie mogelijk zijn tussen actoren binnen het netwerk. Het gaat hierbij om het Landelijk Crisis Management Systeem (LCMS) en directe communicatie tussen actoren (NCTV, 2022a, p. 17; NCTV, 2023b, p. 12).

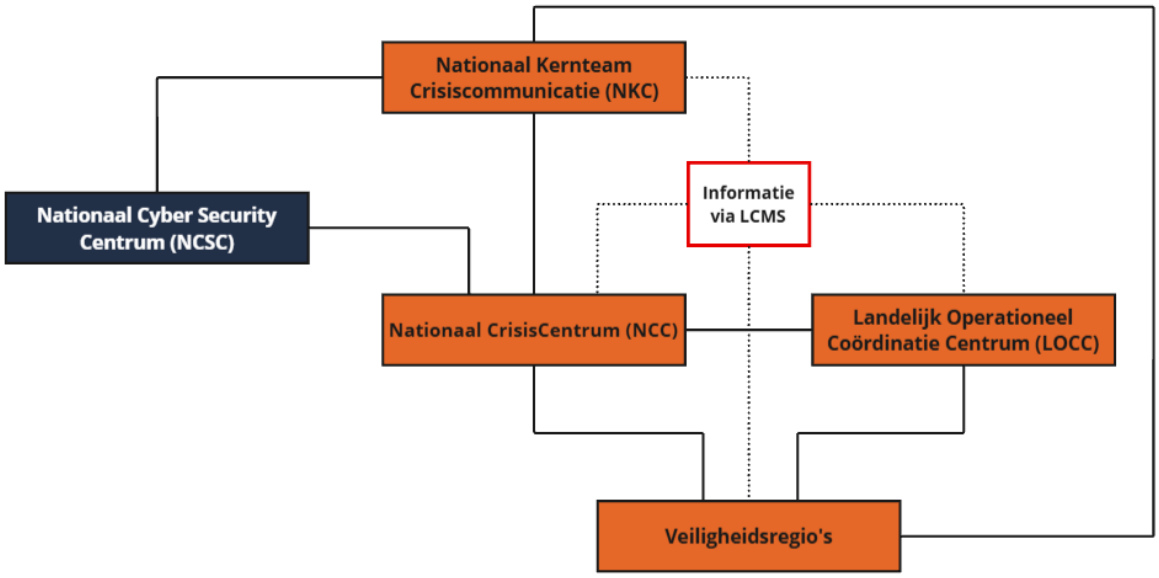
Het LCMS is een digitaal platform dat wordt gebruikt om informatie met elkaar te delen en waarin een Landelijk Operationeel Beeld (LOB) van de crisissituatie kan worden gevormd. Dit platform is 24/7 beschikbaar en zorgt ervoor dat alle actoren beschikken over dezelfde informatie (NCTV, 2023b, p. 12; NIPV, z.d.a). Dit platform wordt dus ook gebruikt binnen het netwerk van informatiedeling en beeldvorming. Echter gebruiken niet alle betrokken actoren dit platform. Zo heeft het Nationaal Cyber Security Centrum (NCSC) geen directe toegang tot het LCMS. Relevante informatie van het NCSC wordt via het Nationaal Crisiscentrum (NCC) aangeleverd in het LCMS (NIPV, z.d.a).

Er vindt ook directe communicatie plaats tussen actoren binnen het netwerk. Op basis van de informatie uit dimensie 1 en 2 kan geconcludeerd worden dat veiligheidsregio's tijdens een

landelijke cybercrisis direct contact kunnen opnemen met LOCC, NCC en het NKC. Verder staat het NCC tijdens een cybercrisis in nauw contact met het LOCC omdat zij gezamenlijk verantwoordelijk zijn voor het vormen van een Landelijk Operationeel Beeld (LOB). Daarnaast staat het NCSC in contact met het NKC voor het afstemmen van kernboodschappen en staan ze in direct contact met het NCC om relevante informatie door te spelen over de oorzaak van de cybercrisis. Tot slot staat het NCC in contact met het NKC, omdat het NKC deels bestaat uit professionals van het NCC.

5.1.2 Visualisatie van het formele netwerk

Figuur 5 toont aan welke actoren formeel betrokken zijn bij het netwerk van informatiedeling en beeldvorming en hoe de communicatielijnen verlopen. De actoren die opereren binnen de algemene keten zijn weergegeven in de oranje kaders. Het Nationaal Cyber Security Centrum (NCSC) opereert binnen de functionele keten en is daarom weergegeven in een blauw kader. De zwarte lijnen geven de directe communicatielijnen tussen de actoren weer en de stippellijnen tonen de informatiestromen aan die verlopen via het Landelijk Crisis Management Systeem (LCMS). Verder is er binnen het netwerk geen sprake van hiërarchie. Zo staat het Nationaal Kernteam Crisiscommunicatie (NKC) niet boven het Nationaal Crisiscentrum (NCC), maar functioneren ze als gelijkwaardige actoren binnen het netwerk. Wel is het belangrijk om te vermelden dat veiligheidsregio's regionaal georganiseerd zijn en de andere actoren nationaal.



Figuur 5: Het formele netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis.

5.1.3 Sturing & besluitvorming

Nu het bekend is hoe de samenstelling en formele werkwijze van het netwerk is ingericht, is het belangrijk om te weten hoe er binnen het netwerk wordt gestuurd en welke actoren bevoegd zijn om besluiten te nemen. Deze overkoepelende dimensie bestaat uit een dimensie die ingaat op de wijze van sturing en een dimensie die de besluitvorming bespreekt.

Dimensie 1: wijze van sturing

Voor het netwerk van informatiedeling en beeldvorming is het van belang om te weten op welke wijze er wordt gestuurd. Dit bepaalt namelijk hoe de samenwerking en coördinatie tussen de betrokken actoren is vormgegeven binnen het netwerk. Volgens Kenis & Provan (2008, p. 301)

is de manier waarop er gestuurd wordt bepalend voor het type netwerkstructuur. Op basis van de geselecteerde documenten in dit onderzoek kan er geconcludeerd worden dat het netwerk van informatiedeling en beeldvorming de meeste kenmerken van een zelfregulerend netwerk vertoont. Dit komt doordat er geen sprake is van een hiërarchische structuur binnen het netwerk en doordat er geen centrale leider aanwezig is. De betrokken actoren werken als een collectief samen en participeren binnen het netwerk op basis van hun rol en expertise.

Toch vertoont het netwerk ook een aantal kenmerken van een leiderorganisatienetwerk, omdat er een aantal actoren zijn die een coördinerende rol op zich nemen. Uit het *Nationaal Handboek Crisisbeheersing* blijkt dat het Nationaal Crisiscentrum (NCC) tijdens een landelijke cybercrisis de informatie vanuit het Rijk coördineert. Daarnaast is het Landelijk Operationeel Coördinatiecentrum (LOCC) verantwoordelijk voor de coördinatie van de informatie vanuit de veiligheidsregio's en het vormen van een Landelijk Operationeel Beeld (LOB) van de crisissituatie (NCTV, 2022b, pp. 26-27). Tot slot blijkt uit de *Koepelnotitie Crisiscommunicatie Digitaal Domein* dat het Nationaal Kernteam Crisiscommunicatie (NKC) een coördinerende rol op zich te neemt wat betreft de crisiscommunicatie (NCTV, 2023b, p. 15).

Dimensie 2: besluitvorming

Naast de wijze van sturing is het van belang om te weten welke actoren binnen het netwerk van informatiedeling en beeldvorming bevoegd zijn om besluiten te nemen tijdens een landelijke cybercrisis. Aan de hand van het *Landelijk Crisisplan Digitaal (LCP-Digitaal)* en het *Nationaal Handboek Crisisbeheersing* kan geconcludeerd worden dat actoren onderling besluiten nemen over informatiemanagement, maar dat er geen beleidsmatige besluiten worden genomen over de aanpak van de cybercrisis. Dit staat niet specifiek in de geselecteerde documenten van dit onderzoek beschreven, maar kan wel als vanzelfsprekend aangenomen worden aangezien de focus van het netwerk vooral ligt op het delen van informatie en het vormen van een Landelijk Operationeel Beeld (LOB) van de crisissituatie. Op basis van het LOB, waar het Landelijk Operationeel Coördinatie Centrum (LOCC) verantwoordelijk voor is, kunnen bevoegde instanties besluiten nemen over de aanpak van de crisis (NCTV, 2022a; NCTV, 2022b).

<u>Bevoegd gezag</u>

Maar welke actoren zijn bevoegd om besluiten te mogen nemen over de aanpak van een landelijke cybercrisis? Volgens de *Bestuurlijke Netwerkkaarten Crisisbeheersing* wordt normaliter de nationale crisisstructuur geactiveerd tijdens een landelijke cybercrisis. Indien dit niet het geval is, zijn de burgemeesters of de voorzitters van de veiligheidsregio's het bevoegd gezag. Dit betekent dat zij dan verantwoordelijk zijn voor de crisisbeheersing en besluiten mogen nemen over de aanpak van de crisis op basis van het gevormde Landelijk Operationeel Beeld (LOB) (Brainich & Ten Dam, 2021, p. 1).

Zodra de nationale crisisstructuur wordt geactiveerd, ontstaan er twee verschillende scenario's. Deze scenario's zijn afhankelijk van de ernst van de crisissituatie. Het eerste scenario is een decentrale aanpak waarbij de minister van Justitie & Veiligheid en de commissaris van de Koning aanwijzingen geven vanuit het Rijk. Dit betekent dat de burgemeesters of de voorzitters van de veiligheidsregio's het bevoegd gezag blijven, maar dat de landelijke aanwijzingen wel opgevolgd moeten worden. Het tweede scenario is een nationale regie. Hierbij wordt het bevoegd gezag overgedragen aan de minister van Justitie & Veiligheid. De minister is dan

verantwoordelijk voor de coördinatie van de crisisbeheersing, de besluitvorming en voor het toezicht op de uitvoering van maatregelen (Brainich & Ten Dam, 2021, p. 6). Een visualisatie van deze bovenstaande gezagslijnen is terug te vinden in Bijlage D (Figuur D1).

Volgens het *Nationaal Handboek Crisisbeheersing* bestaat de nationale crisisstructuur uit drie besluitvormingsorganen. De Ministeriële Commissie Crisisbeheersing (MCCb) komt in actie zodra de nationale veiligheid in het geding is. De MCCb beoordeelt onder andere de beeld- en oordeelsvorming van de crisissituatie, neemt op basis van deze informatie besluiten en stelt een departement-overstijgende strategie op (NCTV. 2022b, p. 21). Naast de MCCb kan de Interdepartementale Commissie Crisisbeheersing (ICCb) tijdens een landelijke cybercrisis worden ingeschakeld. Belangrijke taken van de ICCb zijn het uitwisselen van informatie en het advies geven aan de MCCb over de besluitvorming en coördinatie van maatregelen (NCTV, 2022b, p. 19). De MCCb en ICCb worden ondersteund door het Interdepartementaal Afstemmingsoverleg (IAO). Dit is een tactisch overleg waarin de aanpak van de crisis gecoördineerd wordt (NCTV, 2022b, p. 26). Voor verduidelijking is een visuele weergave van de nationale crisisstructuur opgenomen in Bijlage E (Figuur E1).

Kortom, op basis van de subparagrafen **5.1.1**, **5.1.2** en **5.1.3** kan geconcludeerd worden dat het netwerk van informatiedeling en beeldvorming relatief eenvoudig in elkaar zit met een duidelijke samenstelling, verantwoordelijkheden en taken.

5.2 Samenwerking in de praktijk

Deze paragraaf richt zich op de volgende deelvraag: *'Hoe ervaren de betrokken actoren de samenwerking in de praktijk?'*

Om deze vraag te kunnen beantwoorden heb ik de ervaringen van de respondenten geanalyseerd aan de hand van zeven theoretische dimensies van Ansell & Gash (2007) en de bijbehorende indicatoren. Deze theoretische structuur functioneert goed binnen het theoretisch kader en methodologisch kader van dit onderzoek, maar uit de verzamelde data komt naar voren dat de praktijk een andere structuur kent. Dit komt doordat bepaalde theoretische dimensies in de praktijk met elkaar samenhangen. Een voorbeeld hiervan zijn de dimensies vertrouwen en leiderschap. In deze paragraaf worden daarom de vijf belangrijkste thema's besproken die uit de verzamelde data naar voren zijn gekomen.

5.2.1 Startcondities

In paragraaf 5.1 is de formele structuur van het netwerk van informatiedeling en beeldvorming geanalyseerd. In deze subparagraaf worden de startcondities van dit netwerk besproken. De startcondities kunnen een positieve of negatieve invloed hebben op de samenwerking binnen een netwerk (Ansell & Gash, 2007, p. 550). Het is daarom van belang om de verschillende ervaringen van de respondenten met de startcondities inzichtelijk te maken. Dit wordt gedaan aan de hand van vier elementen.

Samenstelling van het netwerk

Allereerst is het van belang om te achterhalen of de respondenten weten welke actoren betrokken zijn bij het netwerk van informatiedeling en beeldvorming. Zoals beschreven blijkt het netwerk op papier eenvoudig te zijn met een duidelijke samenstelling, maar uit de interviews komt naar voren dat veel respondenten de samenstelling in de praktijk als onduidelijk ervaren.

Daarnaast biedt het *Landelijk Crisisplan Digitaal (LCP-Digitaal)* hierin niet genoeg houvast aan de respondenten.

> "Heel eerlijk, ik vind het een heel onduidelijk netwerk. Dit bleek ook uit de ISIDOOR-oefening. Het is niet duidelijk wie waarvan is. Het was voor ons een grote *black box*." (Respondent 2)

> "Het Landelijk Crisisplan Digitaal, die heb je vast gezien. Daar staan alle landelijke partijen ook in en allemaal ingewikkelde schema's met lijntjes. Ik heb het net doorgenomen, maar je wordt er niet wijzer van." (Respondent 3)

Verder geven geïnterviewden aan dat de actoren uit Figuur 5 in de praktijk ook betrokken zijn, maar wordt het ook duidelijk dat het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) een belangrijke rol speelt in het netwerk van informatiedeling en beeldvorming.

<u>De rol van het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC)</u>
Het VR-ISAC bestaat uit de Chief Information Security Officers (CISO's) van de 25 veiligheidsregio's en richt zich met name op de interne organisatie van de veiligheidsregio's (NIPV, z.d.b). Toch komt uit de interviews naar voren dat ze tijdens de ISIDOOR-oefening een waardevolle bijdrage hebben geleverd aan het netwerk van informatiedeling en beeldvorming. Dit komt doordat ze technische informatie over de oorzaak van de cybercrisis vertaald hebben naar praktische handvatten voor de crisisfunctionarissen. Verschillende respondenten hebben deze externe rol van het VR-ISAC als positief ervaren (respondent 1; 5; 7; 8; 9; 10; 18; 22).

Ondanks deze positieve ervaringen is de rol van het VR-ISAC nog niet officieel vastgelegd in de verschillende documenten. Uit de interviews blijkt dan ook dat dit tot verwarring leidt bij sommige respondenten.

> "Je merkt dat de rol van het VR-ISAC nog niet strak en helder is. Ik weet ook niet of het formeel gaat worden. Ze laten tijdens de ISIDOOR-oefening zien wat ze kunnen en dan is de vraag hoe dat zich verder gaat ontwikkelen." (Respondent 5)

Prikkels om samen te werken
Naast de samenstelling van het netwerk vormen de prikkels om samen te werken een belangrijk element binnen de startcondities. Uit de interviews blijkt dat de actoren binnen het netwerk van informatiedeling en beeldvorming afhankelijk zijn van elkaar, aangezien niemand in staat is om een landelijke cybercrisis zelfstandig op te lossen (respondent 2; 5; 13; 14). Samenwerking en het delen van informatie is daarom nodig om een zo compleet mogelijk Landelijk Operationeel Beeld (LOB) te kunnen vormen van de crisissituatie.

Kennis & inzicht in de formele plannen
Om een landelijke cybercrisis zo effectief mogelijk te bestrijden moeten actoren binnen het netwerk van informatiedeling en beeldvorming beschikken over voldoende kennis en inzicht in de formele plannen. Uit de interviews blijkt dat er een aantal redenen zijn waarin dit niet het geval is.

<u>Onduidelijkheden over de rollen, taken, verantwoordelijkheden & regels en procedures</u>
Het merendeel van de respondenten geeft aan dat de beschrijvingen van de rollen, taken en verantwoordelijkheden van actoren in het *LCP-Digitaal* niet eenduidig genoeg zijn. Respondent 5 legt dit uit aan de hand van een voorbeeld over de taakomschrijving van het Nationaal Cyber

Security Centrum (NCSC): "Als er dan instaat dat het NCSC de operationele coördinatie doet, ja dan nog, wat is dat dan?" Respondent 6 geeft ook aan dat het *LCP-Digitaal* geen duidelijkheid biedt.

> "Er is geen duidelijkheid. Ik heb het landelijk crisisplan wel eens gelezen en dan denk ik van: wat staat hier nou eigenlijk? Ik vind dat het niet helder is en dan moet ik het drie keer lezen voordat ik begrijp wie wat doet. In een daadwerkelijke crisissituatie kan dit niet." (Respondent 6)

Daarnaast blijkt uit de interviews dat de regels en procedures ook onvoldoende helder zijn onder de respondenten. Het is met name onduidelijk hoe de verschillende actoren onderling met elkaar samenwerken binnen het netwerk van informatiedeling en beeldvorming.

> "Hoe dat in de praktijk loopt en hoe het NCSC, NCC en het LOCC met elkaar samenwerken vind ik een lastige. Iedereen heeft iets coördinerend, maar hoe dat in de praktijk verloopt weet ik niet zo goed. Ik vraag me ook af of ze dat zelf helemaal strak hebben. Het NCC, LOCC en NCSC kan ik niet uittekenen." (Respondent 4)

De interviews wijzen uit dat de onduidelijkheden die de respondenten ervaren verklaard kunnen worden door de complexiteit van het *LCP-Digitaal*. Dit komt doordat het document veel pagina's bevat en het netwerk van informatiedeling en beeldvorming er niet duidelijk in beschreven staat. Verschillende respondenten geven dan ook aan dat het document te uitgebreid en onoverzichtelijk is, waardoor het ingewikkelder wordt om de juiste informatie te vinden.

> "Ik weet niet of je er doorheen hebt gebladerd, maar er staat heel veel in. Als er echt stront aan de knikker is kan je daar weinig mee." (Respondent 18)

Deze onduidelijkheden hebben er tijdens de ISIDOOR-oefening ook voor gezorgd dat actoren niet wisten wat ze van elkaar konden verwachten. Respondent 14 van een veiligheidsregio illustreert dit met een voorbeeld:

> "Het was vooral een beetje zoeken voor de actoren van: wie heeft welke informatie nu? Het LOCC zat ons aan te kijken voor een beeld en wij het LOCC. Dus ja, dat zegt wat over de verwachtingen naar elkaar toe." (Respondent 14)

<u>Afkortingen actoren</u>

Naast de bovengenoemde onduidelijkheden over de inhoud van de formele plannen ervaren sommige respondenten ook verwarring over de verschillende afkortingen die worden gebruikt in het *LCP-Digitaal*. Afkortingen zoals het NCC en het NCSC lijken namelijk erg op elkaar, waardoor het soms lastig is om ze van elkaar te onderscheiden. Daarnaast blijkt dat enkele respondenten niet genoeg kennis hebben over de betekenis van de afkortingen (respondent 2; 3; 20; 23). Zo zegt respondent 6: "Als je mij zou overhoren over alle afkortingen, dan zak ik."

<u>Verhouding tussen het LOCC & NCC</u>

Verder blijkt uit de interviews dat de verhouding tussen het Landelijk Operationeel Coördinatie Centrum (LOCC) en het Nationaal Crisiscentrum (NCC) niet eenduidig is omschreven in het *LCP-Digitaal*. Zo weten een aantal respondenten niet wat het onderscheid is tussen deze twee actoren en kunnen ze niet vertellen hoe de onderlinge samenwerking is gestructureerd (respondent 4; 14; 21; 22). Daarentegen vindt een respondent van het LOCC dat de verhouding tussen het LOCC en het NCC wel voldoende is beschreven in het *LCP-Digitaal*.

> "Ik vind de rol van het LOCC en NCC voldoende omschreven in het Landelijk Crisisplan Digitaal. Je moet het een beetje zien als een soort achtje. Wij zijn de onderkant van het achtje en wij hebben contact met de veiligheidsregio's. Het NCC is de bovenkant van het achtje en heeft contact met de departementen. Bij het NCC en het LOCC komt de informatie echt samen." (Respondent 19)

De verschillende ervaringen over de verhouding tussen het LOCC en het NCC suggereren dat er een gebrek is aan afstemming tussen de actoren binnen het netwerk over de inhoud van de formele plannen.

Eerdere samenwerkingen

Het laatste element van de startcondities bespreekt of actoren al eens eerder met elkaar hebben samengewerkt. Eerdere samenwerkingen kunnen van invloed zijn op de huidige samenwerking binnen het netwerk van informatiedeling en beeldvorming (Ansell & Gash, 2007, p. 553). Uit de gesprekken met de respondenten komt naar voren dat de veiligheidsregio's, het Landelijk Coördinatie Centrum (LOCC), het Nationaal Crisiscentrum (NCC) en het Nationaal Kernteam Communicatie (NKC) al eens eerder met elkaar hebben samengewerkt. Denk hierbij aan de corona- en vluchtelingencrisis (respondent 2; 6; 9; 14; 18;). Theoretisch gezien zou dit een positieve invloed moeten hebben op de huidige samenwerking binnen het netwerk, maar toch geven enkele respondenten aan dat dit lastig te beoordelen is (respondent 3; 4; 8; 13; 16; 22). Zij ervaren een landelijke cybercrisis als uniek en geven aan dat het andere uitdagingen met zich meebrengt dan bij een reguliere crisis.

> "Als het woordje cyber erbij komt kijken, dan wordt de mens altijd een beetje zenuwachtig. En ook al hebben ze jarenlang ervaring, dan ineens denken ze dat ze niet meer precies weten wat ze moeten doen." (Respondent 10)

5.2.2 Communicatie

Nu het duidelijk is hoe de startcondities door de verschillende respondenten worden ervaren, richt deze subparagraaf zich op het thema communicatie. Communicatie tussen actoren kan gezien worden als de kern van samenwerking (Ansell & Gash, 2007, p. 558). Daarentegen kan slechte communicatie tussen actoren leiden tot het falen van de samenwerking (Goldsmith & Eggers, 2004, p. 94). Het is daarom van belang om te onderzoeken hoe de respondenten de communicatie binnen het netwerk van informatiedeling en beeldvorming ervaren. Het thema communicatie wordt hieronder aan de hand van twee elementen geanalyseerd.

Manier van communicatie & informatie-uitwisseling tussen actoren

Het eerste element is de manier waarop actoren binnen het netwerk van informatiedeling en beeldvorming met elkaar communiceren en informatie uitwisselen. Uit de interviews blijkt dat er in de praktijk drie verschillende manieren zijn.

<u>Landelijk Crisis Management Systeem (LCMS)</u>

De eerste manier is via het platform LCMS. Zoals eerder beschreven in 5.1.1 delen actoren in het LCMS informatie met elkaar uit over de crisissituatie en wordt er een Landelijk Operationeel Beeld (LOB) gevormd. Volgens de respondenten geeft een LOB een geïntegreerd beeld over de crisissituatie, waarin de informatie van de verschillende actoren met elkaar gebundeld wordt (respondent 5; 9; 12; 15; 19). Op deze manier ontstaat er een gezamenlijk beeld over de situatie en kunnen er verdere besluiten genomen worden op nationaal of regionaal

niveau over de aanpak van de crisis. Uit de interviews blijkt dat respondenten uiteenlopende ervaringen hebben met het delen van informatie en het vormen van een LOB in het LCMS.

> "De informatie die uitgewisseld wordt gaat goed. We gebruiken het LCMS. Voordeel is dat je heel laagdrempelig informatie met elkaar kunt uitwisselen." (Respondent 3)

> "Het LCMS is natuurlijk gevalideerde informatie, hè. Dus wat daarin staat komt echt bij de partijen vandaan en mag je zien als de waarheid. Het is gewoon echt de belangrijkste basis." (Respondent 20)

Naast de positieve ervaringen uiten sommige respondenten kritiek op de manier waarop het Landelijk Operationeel Coördinatie Centrum (LOCC) de aangeleverde informatie in het LCMS verwerkt in een Landelijk Operationeel Beeld (LOB). Er wordt volgens de respondenten te veel gekopieerd en geplakt, waardoor er veel overbodige informatie wordt gepresenteerd in het LOB.

> "Als je terugkijkt in het LCMS zie je dat letterlijk alles gekopieerd is vanuit de andere regio's en vervolgens wordt dat als de waarheid gezien. Je kan er geen chocola van maken zal ik maar zeggen. Als alles gekopieerd en geplakt wordt, ja dan ga je met die hoeveelheid daar niet doorheen werken. Ik heb daar geen tijd voor. Ik wil een korte samenvatting." (Respondent 17)

Opvallend is dat respondenten 19 en 20 van het LOCC in de interviews juist aangeven dat ze de informatie zo goed mogelijk proberen samen te vatten en laten terugkomen in het Landelijk Operationeel Beeld (LOB).

Tot slot blijkt uit de interviews dat het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) geen toegang heeft tot het LCMS. Dit benadrukt nog eens extra de informele positie die het VR-ISAC inneemt binnen het netwerk van informatiedeling en beeldvorming (respondent 8; 9; 10).

<u>Direct contact tussen actoren</u>

Naast communicatie en informatie-uitwisseling via het LCMS vindt er in de praktijk ook direct contact plaats tussen de actoren binnen het netwerk van informatiedeling en beeldvorming. Uit de interviews kan worden opgemaakt dat de formele contactlijnen die gevisualiseerd zijn in subparagraaf 5.1.2, ook in de praktijk zo verlopen. Daarnaast komt naar voren dat het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) tijdens een landelijke cybercrisis in rechtstreeks contact staat met het Nationaal Cyber Security Centrum (NCSC) (respondent 1; 9; 10). Uit de interviews blijkt dat het merendeel van de respondenten het directe contact tussen actoren als prettig ervaart. Toch zijn er ook een aantal respondenten die kritisch zijn. Zo stelt respondent 6: "Ik kan me nog herinneren dat ik een vraag wegzette en dat ik anderhalf uur later pas antwoord kreeg." Dit kan beschouwd worden als een probleem, aangezien het tijdens een crisissituatie belangrijk is dat er snel wordt gereageerd en gehandeld.

<u>Operationeel Leider-call (OL-call)</u>

Naast de bovengenoemde twee manieren blijkt uit de interviews dat er in de praktijk ook gebruik wordt gemaakt van een OL-call. Tijdens de ISIDOOR-oefening werden twee OL-calls georganiseerd door het Landelijk Operationeel Coördinatie Centrum (LOCC). In deze calls kwamen actoren samen om informatie met elkaar uit te wisselen en een gezamenlijk beeld te vormen over de crisissituatie. Dit vond plaats via Microsoft Teams. Uit de interviews komt naar

voren dat verschillende actoren uit het netwerk hieraan deelnamen, waaronder de operationeel leiders van de veiligheidsregio's, het Landelijk Operationeel Coördinatie Centrum (LOCC), het Nationaal Crisiscentrum (NCC), het Nationaal Cyber Security Centrum (NCSC) en het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC). Op basis van de interviews wordt het niet duidelijk of het Nationaal Kernteam Crisiscommunicatie (NKC) ook heeft deelgenomen aan de georganiseerde OL-calls in de ISIDOOR-oefening.

Vaktaal

Het tweede element richt zich op de vaktaal die gesproken wordt binnen het netwerk van informatiedeling en beeldvorming. Het is namelijk van belang dat actoren dezelfde vaktaal spreken, zodat de crisissituatie voor iedere actor helder en begrijpelijk is en er geen misverstanden kunnen ontstaan. Toch blijkt uit de interviews dat dit nog niet zo wordt ervaren.

Technische informatie

Uit de gesprekken met de respondenten komt naar voren dat niet alle actoren binnen het netwerk van informatiedeling en beeldvorming dezelfde vaktaal spreken. Dit werd zichtbaar tijdens de eerste georganiseerde OL-call in de ISIDOOR-oefening. Hierin deelde het Nationaal Cyber Security Centrum (NCSC) technische informatie over de oorzaak van de cybercrisis. Ondanks dat deze technische informatie begrijpelijk was voor het NCSC, werd deze informatie door andere actoren als onbegrijpelijk ervaren.

> "Als we een OL-call hadden, dan ging het over het technische gedeelte van de crisis. Wij snappen dan niet waarover het gaat. Dat was voor ons abracadabra." (Respondent 2)

Door dit probleem ontstond er tijdens de ISIDOOR-oefening geen eenduidig beeld van de crisissituatie, waardoor het risico op verkeerde aannames groter werd. De behoefte aan vertaling van technische informatie van het NCSC wordt dan ook erkend door meerdere respondenten. Zo zegt respondent 23: "Je hebt een vertaling nodig die tante Truus ook begrijpt."

> "Wij willen geduide informatie krijgen. Je wil mensen hebben in de OL-call die aan de ene kant de technische taal spreken en aan de andere kant de crisisbeheersingstaal. Op basis daarvan kunnen we de effecten in kaart brengen. Die vertaalslag maken lukte niet. Dan ga je het zelf interpreteren en is het gevaar dat je verkeerde aannames doet." (Respondent 3)

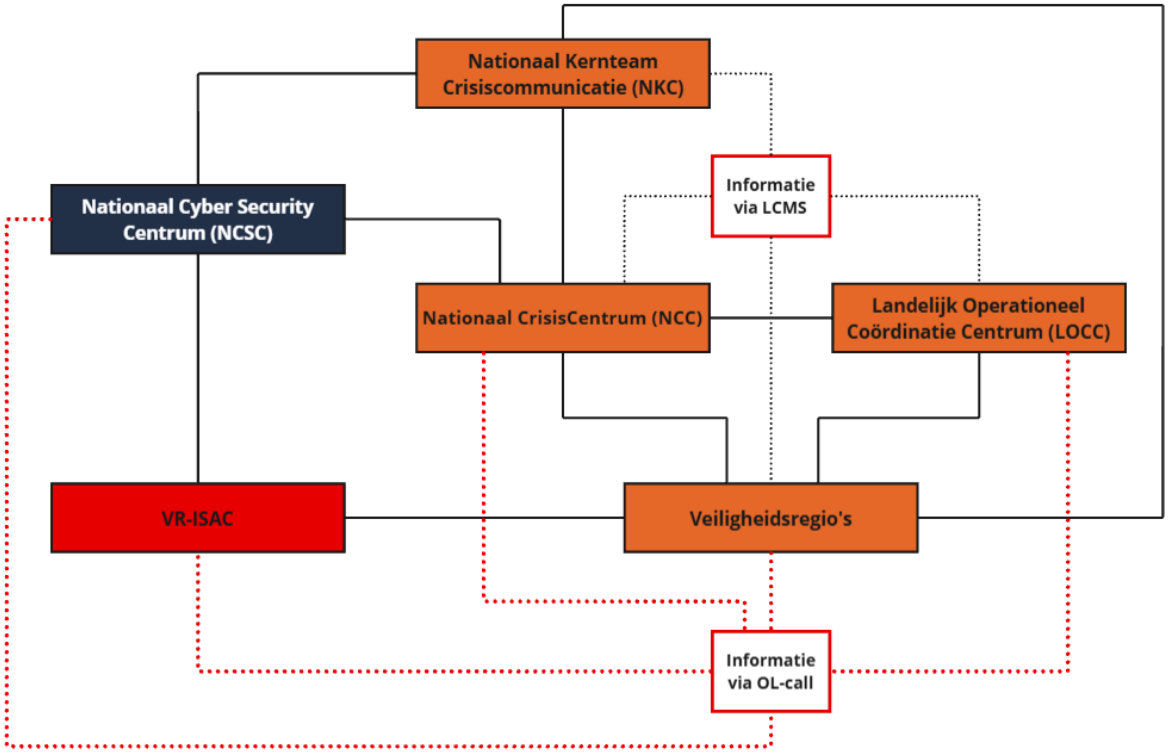
Het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC)

Om dit bovenstaande probleem op te lossen werd tijdens de tweede OL-call in de ISIDOOR-oefening het VR-ISAC betrokken. Deze keuze werd gemaakt vanwege hun expertise op het gebied van informatiebeveiliging en hun ervaring met crisisbeheersing. Zoals eerder beschreven heeft het VR-ISAC tijdens deze tweede OL-call een bijdrage geleverd aan het netwerk van informatiedeling en beeldvorming, doordat ze de technische informatie van het NCSC hebben vertaald naar praktische handvatten voor de crisisfunctionarissen. Dit werd dan ook door de respondenten als waardevol ervaren.

> **"**Toen de eerste OL-call startte en het NCSC begon te vertellen over wat er allemaal technisch aan de hand was, zat iedereen met glazige ogen te kijken. We hadden iemand nodig die het vertaalt voor ons wat al die technische aspecten tot gevolg hebben. Die rol pakte het VR-ISAC op. Ze waren in ieder geval bezig om een soort gat te vullen, want het NCSC kon dat gat niet vullen." (Respondent 18)

5.2.3 Visualisatie van het netwerk in de praktijk

Nu het bekend is hoe de startcondities en communicatie worden ervaren door de respondenten, kan er een visualisatie worden gemaakt van de samenwerking in de praktijk. Deze visualisatie wordt gepresenteerd in Figuur 6. In dit figuur is het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) weergegeven in een rood kader. De reden hiervoor is omdat ze een belangrijke rol in de praktijk innemen, maar officieel nog geen onderdeel zijn van de formele structuur van het netwerk. Daarnaast is het vakje 'informatie via OL-call' toegevoegd, aangezien dit in de praktijk een belangrijk instrument is voor het uitwisselen van informatie en beeldvorming. De rode stippellijnen vertegenwoordigen de actoren die hebben deelgenomen aan de OL-calls in de ISIDOOR-oefening. Tot slot komen de directe contactlijnen tussen actoren in deze visualisatie overeen met de visualisatie van de formele structuur.



Figuur 6: Het netwerk van informatiedeling en beeldvorming in de praktijk.

5.2.4 Toewijding aan het samenwerkingsproces

In deze subparagraaf wordt de toewijding aan het samenwerkingsproces besproken. Het draait hierbij vooral om de verbintenis van actoren met het netwerk. Deze verbintenis kan het succes of het falen van de samenwerking verklaren (Ansell & Gash, 2007, p. 559; Emerson & Nabatchi, 2015, p. 59). Het is daarom belangrijk om te onderzoeken hoe de respondenten de toewijding binnen het netwerk van informatiedeling en beeldvorming ervaren. Dit wordt besproken aan de hand van drie elementen.

Betrokkenheid

Het eerste element betreft de mate van betrokkenheid van actoren binnen het netwerk. Uit de interviews komt naar voren dat de betrokkenheid van actoren binnen het netwerk van informatiedeling en beeldvorming laag is, omdat het netwerk weinig samenkomt. Dit komt doordat een landelijke cybercrisis een nieuw type crisis is en nauwelijks heeft plaatsgevonden. Wel komt het netwerk bijeen tijdens de georganiseerde ISIDOOR-oefeningen. Zoals eerder

besproken vindt dit eens in de twee jaar plaats en dit is relatief weinig. Bovendien heeft niet iedere veiligheidsregio deelgenomen aan de laatste ISIDOOR-oefening, waardoor het netwerk niet compleet was.

> "Niet iedere veiligheidsregio oefende mee in de laatste ISIDOOR-oefening. Dat vind ik wel een belangrijke les voor de volgende keer, hè? Om het zo realistisch mogelijk te oefenen, is dat gewoon belangrijk." (Respondent 9)

Daarnaast blijkt uit de gesprekken met de respondenten dat de beperkte betrokkenheid binnen het netwerk ervoor zorgt dat de formele plannen minder bekend zijn onder de actoren en dat ze daardoor onvoldoende worden getest in de praktijk. Dit zorgt ervoor dat het moeilijk is om te bepalen of de formele plannen ook daadwerkelijk functioneren in de praktijk.

> "Kijk, we beoefenen het ook gewoon niet vaak, hè? Het maakt het dan lastig omdat te kunnen bepalen van: werkt dit ja of nee? Op papier denk je van het staat leuk, maar werkt het dan ook in de praktijk? Iets wat je zelden doet, doe je zelden goed." (Respondent 21)

Een groot deel van de respondenten geeft dan ook aan dat ze vaker willen oefenen (respondent 1; 11; 12; 14; 17; 23). Door vaker te oefenen leer je elkaar beter kennen, wordt de kennis binnen het netwerk vergroot en neemt de betrokkenheid toe. Dit kan een positieve invloed hebben op de samenwerking.

> "Misschien ben ik dan te kort door de bocht, maar ik hoop dat we vaker kunnen oefenen met dit soort landelijke scenario's. Ik denk ook dat het heel goed is voor de actoren om sneller hun rol te pakken." (Respondent 18)

Verantwoordelijkheidsgevoel

Het tweede element draait om het verantwoordelijkheidsgevoel van actoren binnen het netwerk van informatiedeling en beeldvorming. Het gaat hierbij met name om de inzet van actoren om de gezamenlijke netwerkdoelen te behalen. Uit de interviews blijkt echter dat er binnen het netwerk geen gezamenlijk doelen zijn geformuleerd. Dit werd ook duidelijk tijdens de ISIDOOR-oefening. In plaats van het opstellen van gezamenlijke doelen, waren de actoren vooral bezig met het behalen van hun eigen doelen. Dit betekent dat er geen gedeeld verantwoordelijkheidsgevoel bestond onder de actoren om samen de gezamenlijke doelen te behalen.

> "Er wordt te weinig stilgestaan bij gemeenschappelijke doelen. Dat zou wel slim zijn. Iedereen gooit zijn eigen doel op de grote berg en vervolgens wordt het chaos. Dat is dan niet zo gek." (Respondent 6)

> "Het was al moeilijk genoeg om überhaupt partijen bij elkaar te krijgen. Dus laat staan dit soort scherpe afspraken te maken. Nee dit werd niet zo scherp gedaan. Als je dat wel doet kun je natuurlijk veel makkelijker de behoeften op elkaar afstemmen. Dan weet je van jullie doen dit dan doen wij dat. Dat kwam niet van de grond." (Respondent 3)

Verschillende respondenten geven dan ook aan dat ze dit graag meer zouden willen zien in de toekomst. Respondent 7 benadrukt dit: "De les die we daarin kunnen leren is dat we niet allemaal als een gek individueel gaan rennen, maar dat we dat gestructureerd met elkaar gaan doen."

Wederzijdse afhankelijkheid
Naast het verantwoordelijkheidsgevoel is wederzijdse afhankelijkheid een belangrijk element dat terugkomt. Respondenten geven aan in grote mate afhankelijk van elkaar te zijn binnen het netwerk van informatiedeling en beeldvorming. Dit komt doordat actoren elkaar nodig hebben voor informatie en om een zo volledig mogelijk Landelijk Operationeel Beeld (LOB) te kunnen vormen van de crisissituatie. Tijdens de ISIDOOR-oefening werd deze afhankelijkheid door sommige respondenten als onprettig ervaren. Respondent 14 legt dit uit met een voorbeeld:

> "De ervaring is nu dat het best wat tijd kost. Dat is niet kritisch bedoeld, maar wel constaterend dat het tijd kost om een goed landelijk beeld te kunnen vormen. Het LOCC is eerst gewoon tijd kwijt om alle beelden van de veiligheidsregio's bij elkaar te rapen en dan de andere informatie nog. Dat kost gewoon heel veel tijd en we zitten dan te wachten op het landelijke plaatje." (Respondent 14)

Verder blijkt uit de interviews dat actoren sterk afhankelijk zijn van het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) voor de vertaling en duiding van technische informatie van het Nationaal Cyber Security Centrum (NCSC). Dit wijst op ongelijkheid in middelen binnen het netwerk, aangezien niet alle actoren beschikken over expertise en de benodigde kennis over technische informatie. Bovendien komt uit de interviews naar voren dat het VR-ISAC geen toegang heeft tot het Landelijk Crisis Management Systeem (LCMS). Dit wijst ook op een tekort aan hulpbronnen voor het VR-ISAC en bemoeilijkt hun rol als vertaler.

5.2.5 Leiderschap & vertrouwen
In deze subparagraaf worden de thema's leiderschap en vertrouwen binnen het netwerk van informatiedeling en beeldvorming geanalyseerd. In de praktijk blijken deze dimensies sterk met elkaar samen te hangen, omdat de respondenten bij vragen over het thema vertrouwen ook vaak begonnen over coördinatie, afstemming en leiderschap. Om deze reden worden deze twee dimensies samengevoegd. Leiderschap en vertrouwen worden beschouwd als essentiële ingrediënten om actoren binnen een netwerk bij elkaar te brengen. Een gebrek aan leiderschap en vertrouwen kan de samenwerking belemmeren (Ansell & Gash, 2007, p. 554). Het is dan ook van belang om inzichtelijk te maken hoe de respondenten dit ervaren. Dit wordt gedaan aan de hand van twee elementen.

Coördinerend leiderschap
Het eerste element betreft het coördinerende leiderschap binnen het netwerk. In de formele structuur werd duidelijk dat het netwerk van informatiedeling en beeldvorming geen specifieke leider kent. Dit beeld wordt ook bevestigd door de respondenten. Ondanks dat het netwerk geen specifieke leider kent, zijn er wel een aantal actoren die een coördinerende taak op zich nemen. Zo is het Landelijk Operationeel Coördinatie Centrum (LOCC) verantwoordelijk voor de coördinatie van de informatie vanuit de veiligheidsregio's en het Landelijk Operationeel Beeld (LOB), functioneert het Nationaal Crisiscentrum (NCC) als coördinatiecentrum namens het Rijk en zorgt het Nationaal Kernteam Crisiscommunicatie (NKC) voor de coördinatie van de pers- en publiekscommunicatie. Aangezien dit netwerk voornamelijk draait om het uitwisselen van informatie en het vormen van een LOB, wordt het LOCC in dit onderzoek gezien als de actor die het coördinerende leiderschap op zich neemt.

Uit de interviews komt ook naar voren dat de respondenten het LOCC aanzien voor de partij die het coördinerende leiderschap op zich neemt binnen het netwerk. Zij functioneren tijdens

een landelijke cybercrisis als een spin in het web wanneer het gaat om het vormen van een LOB (respondent 1; 4; 14; 16; 19; 22). Zo benoemt respondent 8: "Dat verwacht ik wel van het LOCC, dat ze sturend daarin zijn."

> "De functie van het LOCC is coördineren. Ze moeten ervoor zorgen dat alle actoren hetzelfde beeld hebben. Dus alle OL-calls moeten zij organiseren en een gezamenlijk beeld vormen in het LCMS." (Respondent 5)

<u>Faciliteren van communicatie & informatie-uitwisseling tussen actoren</u>
Het is belangrijk dat de leider de communicatie en informatie-uitwisseling faciliteert tussen de actoren binnen het netwerk van informatiedeling en beeldvorming. Aangezien het LOCC het coördinerende leiderschap op zich neemt, zouden ze ook de verschillende actoren met elkaar moeten verbinden en de communicatie tussen hen moeten faciliteren.

Uit de gesprekken met de respondenten blijkt dat het LOCC een activiteit kan openen in het Landelijk Crisis Management Systeem (LCMS), zodat actoren informatie met elkaar kunnen delen over de crisissituatie. Het LOCC heeft dan als taak om deze informatie samen te brengen en op basis daarvan een Landelijk Operationeel Beeld (LOB) te vormen. Echter blijkt uit de interviews dat dit tijdens de ISIDOOR-oefening niet soepel verliep. Respondenten ervoeren dat het LOCC deze rol niet goed oppakte, waardoor het vormen van het LOB langer duurde.

> "Het LOCC zou eigenlijk de rol moeten pakken om alle beelden bij elkaar te brengen in LCMS en er één beeld van te maken. Dat kwam in deze oefening niet helemaal van de grond." (Respondent 3)

Daarnaast blijkt dat het LOCC ook de OL-calls organiseerde tijdens de ISIDOOR-oefening. Uit de interviews komt naar voren dat sommige respondenten structurele uitdagingen ervoeren tijdens deze calls, omdat het niet duidelijk was of het LOCC de rol van voorzitter op zich zou nemen. Dit kan deels verklaard worden door het feit dat het hoofd van het LOCC niet aanwezig was tijdens de OL-calls, waardoor er een plaatsvervangend hoofd deelnam. Respondent 20 van het LOCC legt dit uit: "Ons hoofd had zich afgemeld, dus ons plaatsvervangend hoofd zat daar. Hij was minder goed gebriefd."

<u>Begrijpen van verschillende vaktalen</u>
Naast het faciliteren van communicatie en informatie-uitwisseling is het ook belangrijk dat de leider de verschillende vaktalen binnen het netwerk begrijpt en deze met elkaar kan verbinden. Uit de interviews blijkt dat het LOCC deze taak niet op zich neemt maar het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC). De reden hiervoor is omdat het VR-ISAC beschikt over meer technische expertise en haar meerwaarde hierin heeft laten zien tijdens de tweede OL-call in de ISIDOOR-oefening. Maar de vraag is wel of het VR-ISAC deze rol op zich moet nemen.

> "Ja, dat is een goeie vraag. Op dit moment kan het LOCC dat niet. De vraag is of het VR-ISAC dat zou moeten doen. Die hebben al helemaal geen formele rol. Die zijn ook niet eens genoemd in het Landelijk Crisisplan Digitaal." (Respondent 18)

Respondent 10 van het VR-ISAC geeft aan dat zij deze rol juist op zich willen nemen, omdat zij de partij zijn die de technische informatie goed kan vertalen naar de gevolgen in de maatschappij: "Ik denk dat dat de plek is waar het VR-ISAC perfect in past, want ja, wij horen

de techniek." Toch geven een aantal respondenten aan dat ze hadden verwacht dat het LOCC deze rol op zich zou nemen. Respondent 17 benadrukt dit: "Ergens moet die duiding goed bij elkaar komen. En je verwacht inderdaad dat dat van het LOCC komt." En respondent 4: "Het LOCC had dat ook kunnen doen." Deze citaten suggereren dat de verwachtingen van de verschillende actoren nog niet met elkaar overeenkomen.

Vertrouwen tussen actoren

Het tweede element focust zich op het vertrouwen tussen de actoren binnen het netwerk van informatiedeling en beeldvorming. Binnen dit element wordt ook het vertrouwen in leiderschap besproken.

Vertrouwen in het coördinerende leiderschap

Binnen het netwerk van informatiedeling en beeldvorming is het van belang dat de actoren vertrouwen hebben in de leider. Uit de interviews blijkt dat de respondenten verschillende ervaringen hebben met het coördinerende leiderschap van het Landelijk Operationeel Coördinatie Centrum (LOCC). Zo hebben een aantal respondenten veel vertrouwen in het LOCC, maar benoemen sommige respondenten ook dat ze nog erg zoekende zijn naar hun rol.

> "Het LOCC heeft de aanbevelingen van de ISIDOOR-oefening ter harte genomen. De geconstateerde lessen werden meteen opgepakt. Dus ja, dat vertrouwen zit er wel. Ik vertrouw er wel op dat daar gewoon ervaren mensen zitten die weten wat ze moeten doen." (Respondent 14)

> "Het LOCC doet in mijn ogen niet wat ze moeten doen, daar zullen ze wel een goede reden voor hebben. Misschien zitten ze klem?" (Respondent 8)

Opbouwen van onderling vertrouwen

Het opbouwen van onderling vertrouwen tussen actoren speelt een belangrijke rol binnen de samenwerking. De ISIDOOR-oefening zou in eerste instantie moeten bijdragen aan het opbouwen van vertrouwen tussen actoren, doordat er gezamenlijk geoefend wordt. Toch blijkt uit de interviews dat de ervaringen hierover gemengd zijn. Zo ervaart een groot deel van de respondenten dat de ISIDOOR-oefening daadwerkelijk bijdraagt aan het opbouwen van het onderling vertrouwen tussen actoren (respondent 1; 11; 14; 17; 19; 23), maar is een klein deel van de respondenten ook kritisch.

> "Wij zeiden tegen elkaar van als dit echt is dan zou ik hier wel zenuwachtig van worden. Het vertrouwen onderling is niet verder gegroeid tijdens de ISIDOOR-oefening. Van tevoren stond ik er neutraal in, daarna waren we niet heel positief hoe het daar liep." (Respondent 2)

Verder benadrukken verschillende respondenten dat het opbouwen van vertrouwen tussen actoren veel tijd kost (respondent 4; 5; 10; 11; 14). Ondanks dat de ISIDOOR-oefening aan de ene kant dus nuttig kan zijn om het vertrouwen tussen actoren verder op te bouwen, blijkt uit de interviews ook dat er nog meer inspanning nodig is om het vertrouwen tussen actoren te kunnen versterken.

Vertrouwen in kwaliteit van actoren

Uit de interviews blijkt dat er onder het merendeel van de respondenten vertrouwen heerst in de kwaliteit van actoren binnen het netwerk van informatiedeling en beeldvorming. Dit vertrouwen wordt met name gebaseerd op expertise, professionaliteit en de intenties van de

betrokken actoren. Respondent 9 benadrukt dit: “Ik heb vertrouwen in de deskundigheid van de partners.” Ondanks dat er dus vertrouwen lijkt te zijn in de kwaliteit van de actoren, geldt dit niet voor de samenhang onderling en de proactiviteit van actoren:

> “Ik heb vertrouwen dat partijen een goede intentie hebben en hun best doen. Ik heb wel vertrouwen in de losse schakels en de expertise, maar niet in de connectie samen.” (Respondent 6)

> “Ik moet wel zeggen dat ik soms wel een beetje schrok van hoe beperkt proactief die landelijke organisaties waren. Dan dacht ik van nou, daar mag wel iets meer pit en iets meer initiatief vandaan komen, maar misschien zie ik dat ook wel verkeerd.” (Respondent 18)

<u>Vertrouwen in nakomen van afspraken</u>
Naast de bovengenoemde ervaringen toont het vertrouwen in het nakomen van afspraken binnen het netwerk ook een wisselend beeld. De meerderheid van de respondenten geeft aan wel vertrouwen te hebben dat actoren hun afspraken nakomen. Zo stelt respondent 1: “Je gaat ervan uit dat iedereen handelt naar hun eigen verantwoordelijkheden.” Maar een klein deel van de respondenten uit ook haar twijfels over de mate waarin bepaalde actoren hun afspraken nakomen en hun rollen vervullen. Respondent 22 illustreert dit met een voorbeeld:

> “Het LOCC en NCC moeten veel beter hun rol gaan pakken, hè? Wat ik dan zie is dat er in LCMS een landelijk beeld geopend wordt. Dan staat er een samenvattend beeld van het LOCC vanaf half zeven in de ochtend. Tot twaalf uur verandert er niks. Terwijl iedereen zit te roepen van wat is er nou precies verder aan de hand? Ik snap niet waarom dat niet lukt.” (Respondent 22)

Kortom, er kan geconcludeerd worden dat er onderling vertrouwen is tussen de actoren in de intenties en de kwaliteit van actoren, maar dat vertrouwen in het leiderschap en in het nakomen van afspraken soms beperkt is.

5.2.6 Tussentijdse resultaten

In deze laatste subparagraaf worden de tussentijdse resultaten geanalyseerd. Tussentijdse resultaten verwijzen ook wel naar de successen die behaald worden en de verbeterpunten binnen een netwerk. Het delen van deze tussentijdse resultaten kan een positieve invloed hebben op de samenwerking, omdat het actoren in staat stelt om de strategie aan te passen en de afstemming te verbeteren (Ansell & Gash, 2007, p. 561). Het is daarom van belang om te onderzoeken in hoeverre er tussentijdse resultaten worden gedeeld binnen het netwerk van informatiedeling en beeldvorming en hoe de respondenten dit ervaren. Dit wordt besproken aan de hand van twee elementen.

Het delen van tussentijdse resultaten
Het eerste element focust zich op het feit of er tussentijdse resultaten worden gedeeld binnen het netwerk van informatiedeling en beeldvorming. Uit de interviews blijkt dat de ISIDOOR-oefening, waaraan de actoren van het netwerk van informatiedeling en beeldvorming ook deelnamen, na afloop is geëvalueerd. Er heeft echter geen specifieke evaluatie plaatsgevonden over het functioneren van het netwerk van informatiedeling en beeldvorming, maar er zijn wel twee andere evaluaties uitgevoerd die voor de actoren uit het netwerk relevant kunnen zijn. Het gaat hier over de sectorale evaluatie en over de algemene evaluatie.

De *Sectorale Evaluatie ISIDOOR-4* is gericht op het functioneren van de veiligheidsregio’s, het Landelijk Operationeel Coördinatie Centrum (LOCC) en het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) (Broeders & Van der Varst, 2024). De *Evaluatie*

ISIDOOR IV heeft een bredere focus en richt zich op het functioneren van de ISIDOOR-oefening en de overkoepelende crisisstructuur (COT, 2024). Aangezien het netwerk van informatiedeling en beeldvorming slechts een klein onderdeel vormde tijdens de ISIDOOR-oefening, zijn niet alle evaluatiepunten even toepasbaar en interessant. Wel zijn er een aantal leerpunten over het vormen van een Landelijk Operationeel Beeld (LOB) beschreven, die wellicht nuttig kunnen zijn voor het netwerk. Uit de interviews blijkt dan ook dat de respondenten deze leerpunten als nuttig ervaren. Wat wel opvalt is dat niet iedere respondent bekend is met de sectorale evaluatie, wat kan duiden op een gebrek aan kennisdeling tussen de actoren.

> "De sectorale evaluatie ken ik helemaal niet. Wanneer is deze gedeeld? [Opent mailbox en zoekt]. Ik heb 22 maart 2024 één mail gehad over een concept, maar niet over de definitieve versie. Dus het antwoord is dat het niet wordt gedeeld met iedereen. Het feit dat het niet gedeeld wordt met iedereen vind ik zorgelijk. We leren dus niet omdat we niet delen." (Respondent 6)

> "Na de hand heb ik ook geen rapportages gehad. We leren gewoon niet. We schrijven allemaal maar wat op en dan wordt het ergens gepubliceerd en that's it. Als je niet eens mensen betrekt, hoe verwacht je dan dat die mensen leren van wat ze hebben gedaan?" (Respondent 8)

Leren van tussentijdse resultaten

De bovenstaande citaten tonen het belang aan of er wordt geleerd van de evaluatiepunten uit de ISIDOOR-oefening. In de zomer van 2024 vond er een wereldwijde computerstoring plaats. Uiteindelijk bleek de oorzaak van deze storing geen cyberaanval, maar een fout in de software-update van het cyberbeveiligingsbedrijf Crowdstrike (NCSC, 2024). Tijdens deze storing kwam het netwerk van informatiedeling en beeldvorming deels bijeen om een Landelijk Operationeel Beeld (LOB) te vormen, aangezien het niet bestempeld werd als een landelijke crisis en niet iedere veiligheidsregio te maken had met dit probleem binnen de regio. Toch blijkt uit een aantal interviews dat de leerpunten met betrekking tot het vormen van een LOB ook tijdens de CrowdStrike-storing naar voren kwamen. Dit wijst erop dat er nog onvoldoende is geleerd van de evaluatiepunten die uit de ISIDOOR-oefening naar voren kwamen.

> "Er moest een beeld gevormd worden en je merkte wel dat de wijze waarop ISIDOOR verliep als oefening, dat dat op dezelfde manier nu terugkwam tijdens CrowdStrike. We zagen een herhaling daarvan." (Respondent 9)

Kortom, op basis van de bovenstaande thema's kan er gesteld worden dat de samenwerking in de praktijk een stuk complexer en weerbarstig lijkt te zijn dan op papier is vastgelegd.

5.3 Formele structuur versus samenwerking in de praktijk

In deze paragraaf staat de volgende deelvraag centraal: *'Hoe verhoudt de formele structuur zich tot de samenwerking in de praktijk en welke factoren spelen hierbij een rol?'*

Zoals besproken in Hoofdstuk 3, verhoudt de formele structuur van een netwerk zich niet één-op-één tot de samenwerking in de praktijk. Maar hoe deze twee concepten zich dan wel tot elkaar verhouden, is nog onduidelijk (Ansell & Gash, 2007; Koppenjan & Klijn, 2004; Bryson et al. 2006; Emerson et al. 2012). Wanneer we de bevindingen van de formele structuur van het netwerk van informatiedeling en beeldvorming en de samenwerking in de praktijk naast elkaar leggen, kan er geconstateerd worden dat deze twee concepten zich inderdaad niet één-op-één tot elkaar verhouden. Er lijkt sprake te zijn van twee totaal verschillende werelden, omdat de

praktijk anders verloopt dan op papier is vastgelegd. In deze paragraaf worden de belangrijkste verschillen tussen de formele structuur en de samenwerking in de praktijk toegelicht.

5.3.1 Ervaringen respondenten

Voordat we de verschillen bespreken, is het relevant om te vermelden dat alle respondenten in dit onderzoek ook de ervaring delen dat de samenwerking in de praktijk anders verloopt dan op papier is vastgelegd.

> "Je kunt een plan maken maar dat is waarschijnlijk het eerste dat sneuvelt. Het zou anders gaan verlopen dan dat je van tevoren hebt bedacht. Goed dat het is uitgewerkt, maar ik denk dat er in de praktijk veel wordt afgeweken van het plan." (Respondent 4)

> "Als je het Landelijk Crisisplan Digitaal als uitgangspunt neemt voor hoe we moeten samenwerken, dan zie ik in de praktijk dat dat anders verloopt dan dat het op papier staat." (Respondent 9)

Daarnaast merkt een respondent op dat er wel degelijk een verband bestaat tussen de formele structuur en de samenwerking in de praktijk. Dit verband wordt ook deels besproken in Hoofdstuk 3, waarin verwacht wordt dat de formele structuur invloed kan uitoefenen op de samenwerking in de praktijk (Ansell & Gash, 2007).

> "De formele structuur is de motor en de techniek en de samenwerking is de olie. En samen maakt het dat het werkt. De onduidelijkheid heeft wel invloed op de samenwerking en we zijn dus nog niet goed in staat om goed op elkaar aan te sluiten. Er zit dus wel degelijk een verband tussen denk ik." (Respondent 6)

5.3.2 Belangrijkste verschillen

Het eerste verschil betreft de rol van het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) in de praktijk. Hoewel deze actor geen plek inneemt binnen de formele structuur van het netwerk van informatiedeling en beeldvorming, blijkt uit de praktijk dat ze een waardevolle bijdrage leveren aan het netwerk. Het VR-ISAC kan namelijk technische informatie vanuit het Nationaal Cyber Security Centrum (NCSC) vertalen naar praktische handvatten voor de crisisfunctionarissen. Deze rol hebben zij vervult tijdens de tweede georganiseerde Operationeel Leider-call (OL-call) in de ISIDOOR-oefening. Veel respondenten hebben deze rol als zeer positief ervaren. Dit komt doordat andere actoren niet in staat waren deze rol op zich te nemen, omdat ze niet over de juiste expertise beschikken. Wel is het opvallend dat het VR-ISAC geen toegang heeft tot het Landelijk Crisis Management Systeem (LCMS). Dit suggereert een tekort aan hulpbronnen voor het VR-ISAC en kan hun rol als vertaler belemmeren. Kortom, het VR-ISAC is in de praktijk één van de belangrijkste actoren binnen het netwerk, maar op papier blijken ze niet te bestaan.

Een ander belangrijk verschil tussen de formele structuur en de samenwerking in de praktijk is de totstandkoming van de OL-call. De OL-call is niet opgenomen in de formele structuur van het netwerk, terwijl het in de praktijk als een van de belangrijkste platformen voor communicatie en informatie-uitwisseling wordt gezien. Dit komt doordat een OL-call de mogelijkheid biedt aan actoren om informatie snel met elkaar af te stemmen en om een gezamenlijk beeld te kunnen vormen van de crisissituatie.

Het laatste verschil betreft de wijze waarop de contactlijn tussen de veiligheidsregio's en het NCSC verloopt. Deze contactlijn verloopt namelijk anders dan op papier is vastgelegd. In de

formele structuur is beschreven dat het NCSC gevalideerde informatie over de oorzaak van de crisis doorstuurt naar het Rijk en vitale partners. Vitale partners zijn organisaties die diensten leveren waarvan de continuïteit van vitaal belang is voor de maatschappij (NCTV, 2022a, p. 18). Veiligheidsregio's zijn door het Rijk nog niet erkend als vitale partners.

Uit dit onderzoek blijkt echter dat het NCSC aansluit bij een OL-call, waarin ze technische informatie delen over de oorzaak van de crisis. Dit impliceert dat de veiligheidsregio's in de praktijk een directe contactlijn hebben met het NCSC, aangezien ze via een OL-call met elkaar contact hebben. Deze contactlijn is niet vastgelegd in de formele structuur, aangezien de veiligheidsregio's niet zijn aangemerkt als vitale partners. Gezien het feit dat het NCSC en de veiligheidsregio's in de praktijk wel contact met elkaar hebben via een OL-call, kunnen zij feitelijk worden beschouwd als vitale partners.

Wanneer we de verschillen overkoepelend bekijken, hebben deze voornamelijk te maken met het daadwerkelijke verloop van communicatie- en informatielijnen in de praktijk. Deze lijnen verlopen namelijk anders dan op papier is vastgelegd. Dit overkoepelende mechanisme maakt dat de formele structuur en samenwerking in de praktijk van elkaar verschillen.

H6| Conclusie, discussie & aanbevelingen

In dit laatste hoofdstuk staat de beantwoording van de onderzoeksvraag centraal. Daarna wordt er gereflecteerd op de theoretische inzichten en de methodologische keuzes die ik gemaakt heb binnen dit onderzoek. Tot slot volgen er op basis van de bevindingen een aantal aanbevelingen.

6.1 Conclusie

In deze paragraaf wordt de onderzoeksvraag van dit onderzoek beantwoord: *'Hoe is de formele structuur van het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis ingericht, hoe ervaren betrokken actoren de samenwerking in de praktijk en op welke wijze kan de verhouding tussen deze twee concepten begrepen worden?'*

De aanleiding van dit onderzoek is dat de *Sectorale Evaluatie ISIDOOR-4* onduidelijkheid suggereert rondom het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis. Hierdoor verliep de samenwerking in de praktijk anders dan op papier is vastgelegd (Broeders & Van der Varst, 2024, pp. 10-11). Dit probleem wordt ook herkend door Veiligheidsregio IJsselland. Om inzicht te kunnen geven in dit probleem is dit onderzoek uitgevoerd.

6.1.1 Formele structuur van het netwerk

In dit onderzoek is er antwoord gegeven op de volgende deelvraag: '*Hoe is de formele structuur van het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis ingericht?'*

Samenstelling & formele werkwijze

Op basis van de geselecteerde documenten in dit onderzoek blijkt het netwerk formeel te bestaan uit de 25 veiligheidsregio's, het Landelijk Operationeel Coördinatie Centrum (LOCC), het Nationaal Crisiscentrum (NCC), het Nationaal Kernteam Crisiscommunicatie (NKC) en het Nationaal Cyber Security Centrum (NCSC).

Vervolgens zijn de formele taken en relaties van de actoren in beeld gebracht. Uit dit onderzoek blijkt dat de veiligheidsregio's tijdens een landelijke cybercrisis verantwoordelijk zijn voor het bestrijden van de gevolgen in de maatschappij en het delen van informatie. Het LOCC is verantwoordelijk voor het coördineren van de informatie vanuit de veiligheidsregio's en het Landelijk Operationeel Beeld (LOB). Het NCC is verantwoordelijk voor het aanleveren en coördineren van de informatie vanuit het Rijk. Verder voert het NCSC technisch onderzoek uit naar de oorzaak van de cybercrisis en leveren ze gevalideerde informatie hierover aan het Rijk en vitale partners. Tot slot is het NKC verantwoordelijk voor het ontwikkelen van de pers- en publiekscommunicatie.

Als laatste is de vergader- en communicatiestructuur onderzocht. Uit de documentatie blijkt dat het netwerk niet vaak bijeenkomt. De reden hiervoor is dat cybercrisissen een nieuw fenomeen zijn en zelden op landelijke schaal hebben plaatsgevonden. De ISIDOOR-oefening is daarom de belangrijkste bijeenkomst waarin het netwerk samenkomt. Deze oefening wordt om de twee jaar georganiseerd en biedt het netwerk de mogelijkheid om met elkaar te oefenen en de samenwerking te verbeteren. Daarnaast blijkt dat er binnen het netwerk op twee verschillende

manieren wordt gecommuniceerd. Het gaat hier om communicatie en informatie-uitwisseling via het Landelijk Crisis Management Systeem (LCMS) en directe communicatie tussen actoren.

Sturing & besluitvorming
Er kan geconcludeerd worden dat het netwerk van informatiedeling en beeldvorming de meeste kenmerken vertoont van een zelfregulerend netwerk. Dit komt doordat er geen centrale leider aanwezig is en er geen sprake is van hiërarchie. Toch vertoont het netwerk van informatiedeling en beeldvorming ook kenmerken van een leiderorganisatienetwerk (Kenis & Provan, 2008, pp. 301-302. De reden hiervoor is dat een aantal actoren een coördinerende rol op zich nemen. Zoals eerder beschreven coördineert het LOCC de informatie van de veiligheidsregio's en het Landelijk Operationeel Beeld (LOB), is het NCC verantwoordelijk voor de coördinatie van informatie vanuit het Rijk en neemt het NKC een coördinerende rol in ten aanzien van de pers- en publiekscommunicatie. Dit betekent dat het netwerk van informatiedeling en beeldvorming in termen van Kenis & Provan (2008) een mengvorm is van een zelfregulerend netwerk en een leiderorganisatienetwerk. Daarnaast blijkt dat er binnen het netwerk geen beleidsmatige besluiten worden genomen over de daadwerkelijke aanpak van een landelijke cybercrisis. Wel worden er besluiten genomen over informatiemanagement.

Kortom, op basis van de bovenstaande bevindingen kan geconcludeerd worden dat het netwerk van informatiedeling en beeldvorming relatief eenvoudig en overzichtelijk in elkaar zit, met duidelijke taken en verantwoordelijkheden.

6.1.2 Samenwerking in de praktijk
Naast de formele structuur is er in dit onderzoek ook antwoord gegeven op de deelvraag: *'Hoe ervaren de betrokken actoren de samenwerking in de praktijk?'*

Startcondities
Uit dit onderzoek blijkt dat de startcondities over het algemeen als onduidelijk worden ervaren. Zo is het voor veel respondenten niet helder hoe de samenstelling georganiseerd is en blijkt dat het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) een belangrijke rol inneemt in de praktijk. Respondenten geven dan ook aan hierover verwarring te ervaren, omdat de rol van het VR-ISAC formeel nog niet is vastgelegd. Daarnaast komt naar voren dat actoren afhankelijk van elkaar zijn om een Landelijk Operationeel Beeld (LOB) te kunnen vormen van de crisissituatie. Dit zet hen ertoe aan om samen te werken binnen het netwerk. Verder blijkt dat het merendeel van de respondenten onduidelijkheden ervaart over de rollen, taken en verantwoordelijkheden binnen het netwerk. Dit geldt ook voor de regels en procedures. Deze onduidelijkheden hebben tijdens de ISIDOOR-oefening ervoor gezorgd dat actoren geen goed beeld hadden wat ze van elkaar konden verwachten.

Bovendien wordt het duidelijk dat de veiligheidsregio's, het Landelijk Operationeel Coördinatie Centrum (LOCC) en het Nationaal Crisiscentrum (NCC) als eens eerder met elkaar hebben samengewerkt. Respondenten vinden het echter wel lastig om te beoordelen of deze eerdere samenwerking invloed hebben op de huidige samenwerking. Dit komt doordat zij een landelijke cybercrisis als uniek ervaren.

Communicatie
Dit onderzoek toont aan dat de respondenten de communicatie en informatie-uitwisseling via het Landelijk Crisis Management Systeem (LCMS) als verschillend ervaren. De één vindt dat het goed verloopt, terwijl de ander kritiek uit. Daarnaast wordt het direct contact tussen actoren als positief ervaren. Verder blijkt dat er in de praktijk ook gebruik wordt gemaakt van een Operationeel Leider-call (OL-call), om informatie met elkaar te delen en af te stemmen. Tijdens de georganiseerde OL-calls in de ISIDOOR-oefening deelde het Nationaal Cyber Security Centrum (NCSC) vooral technische informatie, waardoor andere actoren moeite hadden met het begrijpen van deze informatie. Dit suggereert dat niet alle actoren dezelfde vaktaal spreken binnen het netwerk. De behoefte aan vertaling van de technische informatie wordt dan ook erkend door meerdere respondenten. Het VR-ISAC heeft de rol van vertaler op zich genomen en veel respondenten hebben dit als prettig ervaren.

Toewijding aan het samenwerkingsproces
Uit dit onderzoek komt naar voren dat de betrokkenheid binnen het netwerk beperkt is. Dit komt doordat de actoren weinig samenkomen. Het netwerk komt wel bijeen tijdens de tweejaarlijkse ISIDOOR-oefening, maar veel respondenten vinden deze frequentie te weinig. Bovendien hebben niet alle veiligheidsregio's deelgenomen aan de laatste editie, waardoor het netwerk incompleet was. Daarnaast blijkt dat een aantal respondenten het jammer vindt dat er geen gezamenlijke doelen worden opgesteld binnen het netwerk. Verder blijkt dat de actoren sterk afhankelijk zijn van het VR-ISAC voor de vertaling van technische informatie. Dit wijst op ongelijkheid in middelen binnen het netwerk omdat niet iedereen over dezelfde expertise en kennis beschikt. Tot slot komt uit dit onderzoek naar voren dat het VR-ISAC geen toegang heeft tot het LCMS. Dit suggereert een tekort aan hulpbronnen voor het VR-ISAC. Dit is opvallend, aangezien het VR-ISAC een van de belangrijkste actoren is binnen het netwerk.

Leiderschap & vertrouwen
Uit dit onderzoek blijkt dat het Landelijk Operationeel Coördinatie Centrum (LOCC) door de actoren wordt beschouwd als de coördinerende leider binnen het netwerk. Echter blijken de ervaringen van de respondenten verschillend te zijn. Sommige respondenten vinden dat het LOCC haar coördinerende functie niet goed oppakt, terwijl een ander deel van de respondenten juist vertrouwen uit in het LOCC. Daarnaast zou de ISIDOOR-oefening moeten bijdragen aan het opbouwen van onderling vertrouwen tussen actoren, maar uit dit onderzoek komt naar voren dat respondenten hier verschillend over denken. Zo ervaren de meeste respondenten de oefening als zeer positief, maar zijn er ook een aantal kritisch. Verder hebben respondenten vertrouwen in de kwaliteit van actoren, maar is er minder vertrouwen in de samenhang onderling. Tot slot geeft de meerderheid van de respondenten aan vertrouwen te hebben dat actoren hun afspraken nakomen, maar een klein deel ook niet.

Tussentijdse resultaten
Tot slot komt naar voren dat de *Sectorale Evaluatie ISIDOOR-4* en de *Evaluatie ISIDOOR IV* als nuttig worden ervaren door de respondenten. Opvallend is dat niet iedere respondent bekend is met de sectorale evaluatie, wat duidt op een gebrek aan kennisdeling binnen het netwerk. Daarnaast vond er een herhaling plaats van een aantal leerpunten uit de ISIDOOR-oefening

gedurende de wereldwijde CrowdStrike-storing. Dit suggereert dat er nog onvoldoende is geleerd van de evaluatiepunten uit de ISIDOOR-oefening.

Kortom, de bevindingen laten zien dat de samenwerking in de praktijk weerbarstiger is dan op papier is vastgelegd. Dit zorgt ervoor dat de samenwerking binnen het netwerk niet effectief verloopt. In de volgende deelparagraaf wordt toegelicht waarom.

6.1.3 Theoretische reflectie op de samenwerking in de praktijk

Nu het duidelijk is hoe respondenten de samenwerking in de praktijk ervaren, is het van belang om te verklaren waarom de samenwerking niet effectief verloopt. Een van de belangrijkste verklaringen hiervoor is de beperkte betrokkenheid binnen het netwerk. Volgens Ansell & Gash (2007) en Emerson & Nabatchi (2015) is de mate van betrokkenheid belangrijk voor het bepalen van het succes of het falen van de samenwerking (Ansell & Gash, 2007, p. 559; Emerson & Nabatchi, 2015, p. 59). Binnen het netwerk van informatiedeling en beeldvorming is de betrokkenheid dus beperkt. Dit komt doordat een landelijke cybercrisis een nieuw type crisis is en nog zelden heeft plaatsgevonden. Bovendien komt het netwerk alleen samen tijdens de tweejaarlijkse ISIDOOR-oefening. Dit verklaart ook de complexiteit die respondenten ervaren, aangezien ze nog onvoldoende samen hebben geoefend en daardoor nog weinig ervaring hebben opgedaan.

Het niet effectief functioneren van de samenwerking kan ook verklaard worden door de onduidelijkheid die er heerst onder de respondenten over de formele plannen. Het formaliseren van duidelijke basisregels, procedures, taken en verantwoordelijkheden is belangrijk voor een effectieve samenwerking (Alexander et al., 1998, p. 324; Ansell & Gash, 2007, p. 557; Koppenjan & Klijn, 2004, p. 151). De formele plannen bieden volgens de respondenten te weinig houvast. Dit heeft te maken met de omvang en complexiteit van het *Landelijk Crisisplan Digitaal (LCP-Digitaal)* en doordat de rollen, taken, verantwoordelijkheden en de regels en procedures niet eenduidig gedefinieerd zijn. Daarnaast kan de onduidelijkheid ook verklaard worden door onvoldoende kennis en inzicht die actoren hebben in de formele plannen.

Een andere verklaring is de toegang tot het samenwerkingsproces. Een belangrijke voorwaarde voor een succesvolle samenwerking is dat het netwerk alle actoren moet omvatten die betrokken zijn bij het probleem (Ansell & Gash, 2007, p. 556). Uit de praktijk komt naar voren dat het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) een belangrijke rol inneemt binnen het netwerk, maar formeel blijken ze nog niet te bestaan. Dit betekent dat het netwerk formeel gezien niet alle actoren omvat. Dit verklaart ook waarom er in de praktijk verwarring ontstaat onder de respondenten over de rol van het VR-ISAC binnen het netwerk.

Verder kan het ineffectief functioneren van de samenwerking verklaard worden doordat er geen gemeenschappelijke doelen worden opgesteld binnen het netwerk. Ansell & Gash (2007, p. 560) en Provan & Kenis (2008, p. 240) benadrukken dat het opstellen en afstemmen van gemeenschappelijke doelen een positief effect heeft op de samenwerking. Aangezien er geen gemeenschappelijke doelen worden opgesteld, is iedere actor vooral bezig met het behalen van haar eigen doelen. Op deze manier ontbreekt de afstemming tussen de actoren, waardoor ze niet weten wat ze van elkaar kunnen verwachten. Dit verklaart ook het gebrek aan een gevoel van eigenaarschap binnen het netwerk.

Tot slot is er geen gedeeld begrip onder de actoren binnen het netwerk. Om tot een succesvolle samenwerking te komen, benadrukken Ansell & Gash (2007, p. 560) dat er gedeeld begrip moet ontstaan onder de actoren over het probleem. Binnen het netwerk van informatiedeling en beeldvorming is hier nog geen sprake van, omdat actoren niet dezelfde vaktaal spreken. Het niet spreken van dezelfde vaktaal kan het proces van communicatie en informatie-uitwisseling verstoren (Goldsmith & Eggers, 2004, p. 94).

6.1.4 Formele structuur versus samenwerking in de praktijk

Als laatste is de deelvraag: *'Hoe verhoudt de formele structuur zich tot de samenwerking in de praktijk en welke factoren spelen hierbij een rol?'* beantwoord.

Wanneer we de bevindingen van dit onderzoek naast elkaar leggen, zien we dat de formele structuur zich niet één-op-één verhoudt met de samenwerking in de praktijk. Zoals eerder beschreven blijkt de formele structuur van het netwerk van informatiedeling en beeldvorming relatief eenvoudig en overzichtelijk te zijn, maar in de praktijk zien we dat de samenwerking een stuk complexer is. Er lijkt dus sprake te zijn van twee totaal verschillende werelden. Dit komt doordat er een aantal belangrijke verschillen te zien zijn tussen de formele structuur en de samenwerking in de praktijk.

Het eerste verschil betreft de rol van het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) in de praktijk. Hoewel het VR-ISAC formeel gezien niet bestaat binnen het netwerk van informatiedeling en beeldvorming, blijkt uit de praktijk dat ze een van de belangrijkste actoren zijn binnen het netwerk. Dit komt doordat zij de rol als vertaler op zich nemen en technische informatie duiden. Hierdoor verbinden ze actoren met elkaar, waardoor er gedeeld begrip ontstaat. Een ander opvallend verschil is het gebruik van de Operationeel-Leider call (OL-call) in de praktijk. Binnen de formele structuur is de OL-call niet vastgelegd, maar in de praktijk blijkt het een belangrijk platform te zijn waar informatie met elkaar gedeeld en afgestemd wordt. Het laatste verschil is het directe contact tussen de veiligheidsregio's en het Nationaal Cyber Security Centrum (NCSC). Volgens de formele structuur van het netwerk hebben de veiligheidsregio's geen rechtstreeks contact met het NCSC, omdat zij door het Rijk niet zijn aangemerkt als vitale partners. Aangezien ze in de praktijk wel direct contact met elkaar hebben via een OL-call, kunnen de veiligheidsregio's feitelijk worden beschouwd als vitale partners van het NCSC.

Kortom, wanneer we de bovenstaande drie verschillen overkoepelend bekijken kan er gesteld worden dat deze voornamelijk het verloop van communicatie- en informatielijnen betreffen. Deze lijnen verlopen in de praktijk namelijk anders dan op papier is vastgelegd. Dit maakt dat de formele structuur en de samenwerking in de praktijk van elkaar verschillen.

6.1.5 Incomplete formele structuur & wederkerige relatie

Nu het duidelijk is geworden dat de formele structuur van het netwerk van informatiedeling en beeldvorming en de samenwerking in de praktijk verschillend van elkaar zijn, is het belangrijk om te begrijpen en verklaren waar dit verschil vandaan komt.

De voornaamste verklaring voor het verschil is dat de formele structuur incompleet is en daardoor te weinig houvast biedt aan de actoren binnen het netwerk. Dit komt doordat de formele structuur nog niet voldoende is verrijkt met ervaringen, inzichten en uitdagingen uit de

praktijk. Een mogelijk oorzaak hiervan is dat een landelijke cybercrisis een nieuw type crisis betreft, waardoor er nog beperkte ervaring is opgedaan met het bestrijden ervan.

Doordat de formele structuur onvoldoende houvast biedt, zoeken actoren andere manieren om het complexe probleem in de praktijk op te kunnen lossen. Zo toont dit onderzoek aan dat actoren andere communicatie- en informatielijnen gaan improviseren, die afwijken van de formele structuur. Een voorbeeld hiervan is de totstandkoming van de Operationeel-Leider call (OL-call). Dit platform stelt actoren in staan om in de praktijk sneller informatie met elkaar af te stemmen. Een ander voorbeeld is de rol die het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) vervult als vertaler binnen het netwerk. Aangezien deze oplossingen tijdens de ISIDOOR-oefening effectief bleken, is het aannemelijk dat ze opnieuw worden toegepast in een toekomstige oefening of crisissituatie.

Dit wijst op een proces waarin informele oplossingen geleidelijk worden geïnstitutionaliseerd binnen de samenwerking in de praktijk. Dit impliceert dat men uit de praktijkfase stapt en dat de informele oplossingen langzamerhand formeel worden vastgelegd. Wat we dan zien is een soort wederkerige relatie tussen de formele structuur en de samenwerking in de praktijk. De formele structuur bepaalt voor een deel hoe men de praktijk ingaat, terwijl de ervaringen uit de praktijk de formele structuur weer doen veranderen.

6.2 Discussie

In deze paragraaf reflecteer ik op de theoretische inzichten en de methodologische keuzes die ik heb gemaakt binnen dit onderzoek. Vervolgens bespreek ik de implicaties van dit onderzoek.

6.2.1 Theoretische reflectie

In het theoretisch kader heb ik hoofdzakelijk gebruikgemaakt van het collaborative governance raamwerk van Ansell & Gash (2007) om het conceptueel model van dit onderzoek te kunnen vormen. Dit conceptuele model helpt ons om het netwerk van informatiedeling en beeldvorming te kunnen onderzoeken en te begrijpen. De formele structuur heb ik dan ook in kaart gebracht aan de hand van de theorieën van Ansell & Gash (2007) over het institutioneel ontwerp van een netwerk en het element dat gaat over de face-to-face dialoog tussen actoren. Daarnaast heb ik een aantal concepten uit de bestuurskundige netwerkanalyse van Koppenjan & Klijn (2004) gebruikt en het conceptueel model van Kenis & Provan (2008) over netwerksturing. De samenwerking in de praktijk heb ik onderzocht aan de hand van de verschillende elementen uit het model van Ansell & Gash (2007). Het gaat hier om startcondities, face-to-face dialoog, vertrouwen, gedeelde betekenisgeving, toewijding aan het proces, tussentijdse resultaten en faciliterend leiderschap. Het element institutioneel heb ik in de praktijk ook onderzocht, om te kijken hoe de respondenten dit ervaren. Dit element heb ik ondergebracht onder de startcondities, omdat ik verwachtte dat deze in de praktijk met elkaar zouden samenhangen. Dit blijkt ook zo te zijn. Verder heb ik de elementen onderbouwd met relevante theoretische concepten van andere auteurs, om op deze manier de samenwerking beter te begrijpen (Van Delden, 2009; Koppenjan & Klijn, 2004; Emerson et al., 2012; Bryson et al., 2006; Goldsmith & Eggers, 2004; Vangen & Huxham, 2003; Klijn et al., 2010; Provan & Kenis, 2008; Emerson & Nabatchi, 2015; Bryson et al., 2015).

Een beperking van het theoretisch kader is dat het niets zegt over een belangrijk element van samenwerking, namelijk platforms. Aan het begin van dit onderzoek verwachtte ik niet dat

binnen het netwerk verschillende platforms werden toegepast. Uit dit onderzoek komt echter naar voren dat actoren met elkaar communiceren via het Landelijk Crisis Management Systeem (LCMS) en via de Operationeel Leider-call (OL-call). Deze twee instrumenten worden door Ansell & Gash (2017) aangeduid als *collaborative platforms*. Zij definiëren een collaborative platform als volgt:

> "A collaborative platform is an organization or program with dedicated competences, institutions and resources for facilitating the creation, adaptation and success of multiple or ongoing collaborative projects or networks. (Ansell & Gash, 2017, p. 20)

Daarnaast beschrijven Ansell & Gash (2017) ook de voordelen en de verschillende uitdagingen die collaborative platforms met zich meebrengen. Zo blijkt uit de resultaten van dit onderzoek dat informatie-uitwisselen en communiceren via het LCMS en de OL-call ook uitdagingen met zich meebrengt. Te denken valt aan het feit dat niet iedere actor toegang heeft tot het LCMS of dat communiceren via een OL-call nog niet effectief verloopt. De theorie over collaborative platforms biedt dan een breder perspectief om het daadwerkelijk functioneren van de platforms binnen het netwerk van informatiedeling en beeldvorming te kunnen onderzoeken. Dit is een mooie suggestie voor een vervolgonderzoek. Een andere suggestie voor vervolgonderzoek zou kunnen zijn om te onderzoeken hoe collaborative governance en collaborative platforms zich tot elkaar verhouden.

Verder blijkt dat het conceptueel model van Kenis & Provan (2008) over netwerksturing ontoereikend is voor het netwerk van informatiedeling en beeldvorming. Uit dit onderzoek blijkt dat het netwerk in de praktijk complex is en kenmerken vertoont van een zelfregulerend netwerk en een leiderorganisatienetwerk (Kenis & Provan, 2008, pp. 301-302). Bij nader inzien past de theorie van Cumming (2016) over een heterarchie wellicht beter bij het netwerk van informatiedeling en beeldvorming, omdat het verschillende perspectieven van een hiërarchie en netwerken verenigt in één kader. Een heterarchie betekent dat de structuur een combinatie bevat van horizontale en verticale lijnen. Dit is ook het geval binnen het netwerk van informatiedeling en beeldvorming, omdat er sprake is van coördinerend leiderschap (Cumming, 2016, p. 622).

Voor toekomstig onderzoek is het dus belangrijk om de theorieën over collaborative platforms (Ansell & Gash, 2017) en heterarchie (Cumming, 2016) te integreren, zodat de samenwerking binnen het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis in zijn geheel begrepen kan worden.

6.2.2 Methodologische reflectie

In dit onderzoek heb ik twee onderzoeksmethoden toegepast. Het gaat hierbij om een documentenanalyse en semigestructureerde interviews. Deze methoden hebben gezamenlijk bijgedragen aan een diepgaand inzicht in het netwerk van informatiedeling en beeldvorming, maar brengen ook een aantal beperkingen met zich mee.

De documentenanalyse heeft in dit onderzoek ertoe bijgedragen dat er doelgericht informatie verzameld kon worden over de formele structuur van het netwerk. Bovendien vergroot een documentenanalyse de betrouwbaarheid en validiteit van het onderzoek, omdat het een afspiegeling vormt over wat er is vastgelegd (Bleijenbergh, 2013, p. 164). Een beperking binnen

dit onderzoek is dat de geselecteerde documenten een vertekend beeld van de werkelijkheid kunnen opleveren, omdat de documenten vanuit een bepaalde invalshoek zijn gepresenteerd. Daarnaast speelt de subjectieve interpretatie van de onderzoeker ook een rol. Dit houdt in dat de geselecteerde documenten door andere onderzoekers op een andere manier geïnterpreteerd kunnen worden (Bowen, 2009, pp. 31-32).

Naast de documentenanalyse hebben er ook semigestructureerde interviews plaatsgevonden. Door deze interviews is er diepgaande informatie verkregen over de samenwerking in de praktijk, omdat respondenten hun ervaringen, percepties en betekenissen konden delen. Daarentegen kunnen de semigestructureerde interviews ook een beperking opleveren, omdat er een *social desirability bias* kan ontstaan bij de respondenten. Dit houdt in dat respondenten geneigd zijn om sociaal wenselijke antwoorden te geven. Hierdoor kan er een verschil optreden tussen de werkelijkheid en wat respondenten zeggen (Nederhof, 1985, pp. 263-264). Om dit te verhelpen kunnen er in het vervolgonderzoek ook observaties uitgevoerd worden, waarin de respondenten worden gevolgd in hun natuurlijke context. Dit kan bijvoorbeeld uitgevoerd worden tijdens een ISIDOOR-oefening.

Een andere beperking richt zich op de selectiemethode binnen dit onderzoek. Door middel van de sneeuwbalmethode heb ik aan respondenten gevraagd of zij andere respondenten kenden die konden bijdragen aan dit onderzoek. Er bestaat echter wel een kans dat niet alle relevante actoren voor dit onderzoek zijn geïnterviewd, aangezien veel respondenten geen duidelijk beeld hadden over de samenstelling van het netwerk. Om toch een zo diepgaand mogelijk inzicht te verkrijgen heb ik 23 semigestructureerde interviews afgenomen met respondenten. Helaas hebben er geen interviews plaatsgevonden met respondenten van het Nationaal Cyber Security Centrum (NCSC) en het Nationaal Kernteam Crisiscommunicatie (NKC), waardoor hun perspectieven ontbreken binnen dit onderzoek. Daarnaast zijn niet alle veiligheidsregio's geïnterviewd vanwege de beperkte tijd. Het kan dus voor vervolgonderzoek wenselijk zijn om de ervaringen van andere veiligheidsregio's, het NCSC en het NKC te onderzoeken.

Tot slot is het netwerk van informatiedeling en beeldvorming te typeren als een extreme case study, aangezien een landelijke cybercrisis een nieuw type crisis is en nog zelden heeft plaatsgevonden. Dit betekent dat de resultaten van dit onderzoek statistisch gezien op dit moment beperkt generaliseerbaar zijn naar samenwerkingen in andere crisissituaties. Echter wordt er wel verwacht dat landelijke cybercrisissen op de lange termijn steeds vaker gaan plaatsvinden (NCTV, 2024a, p. 5). In de toekomst is het dus aannemelijk dat deze casus wel representatief zal zijn voor de manier van samenwerken in crisissituaties.

6.2.3 Implicaties van het onderzoek

De bevindingen van dit onderzoek dragen bij aan een duidelijk beeld over het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis. Op basis hiervan kan de samenwerking tussen actoren verbeterd worden, waardoor een landelijke cybercrisis in de toekomst effectiever kan worden aangepakt. Bovendien kunnen de bevindingen beleidsmakers helpen bij het aanpassen van de bestaande formele structuren, zodat deze beter aansluiten op de praktijk.

Daarnaast bieden de bevindingen waardevolle inzichten in de manier van samenwerken tijdens een nieuw type crisis. Een landelijke cybercrisis is namelijk relatief uniek, aangezien het zelden voorkomt en het van een andere orde is dan een reguliere crisis. Dit is dan ook terug te zien in de formele structuur van het netwerk en de samenwerking in de praktijk. Zoals beschreven biedt de formele structuur onvoldoende houvast aan de actoren, waardoor er in de praktijk gezocht moeten worden naar andere oplossingen. We zien dus dat er een aantal mechanismen gaande zijn binnen het netwerk. Voorbeelden hiervan zijn de Operationeel Leider-call (OL-call), de rol van het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) en het feit dat het netwerk kenmerken vertoont van een heterarchische netwerkstructuur. Deze manier van samenwerken zullen we naar verwachting in de toekomst steeds vaker gaan zien, aangezien landelijke cybercrisissen in de komende decennia vaker zullen voorkomen en dit wellicht de manier is om complexe problemen in de toekomst te kunnen bestrijden.

6.3 Aanbevelingen

Op basis van de bevindingen heb ik enkele aanbevelingen geformuleerd. Deze aanbevelingen zijn gericht aan alle betrokken actoren binnen het netwerk van informatiedeling en beeldvorming.

Aanbeveling 1: Nieuwe planvorming opstellen

De belangrijkste aanbeveling is om gezamenlijk een nieuwe planvorming op te stellen dat beter aansluit op de samenwerking in de praktijk. In dit kader is het wenselijk een nieuw document te ontwikkelen dat specifiek gericht is op het netwerk van informatiedeling en beeldvorming. Uit dit onderzoek is gebleken dat de formele structuur van het netwerk onvoldoende houvast biedt aan de actoren, waardoor de samenwerking in de praktijk niet volgens de formele structuur verloopt. Het is daarom van belang om in de nieuwe planvorming de volgende punten mee te nemen:

a. Het formuleren van duidelijke rollen, taken en verantwoordelijkheden van actoren en het formuleren van eenduidige regels en procedures. Uit dit onderzoek blijkt dat hier veel onduidelijkheid over bestaat. Het is daarom belangrijk om deze aspecten gezamenlijk met elkaar af te stemmen en te formuleren, zodat er gedeeld begrip ontstaat onder de actoren.

b. Het formeel vastleggen van de rol van het Veiligheidsregio Information Sharing and Analysis Centre (VR-ISAC) als vertaler. Dit onderzoek wijst uit dat het VR-ISAC in de praktijk een waardevolle bijdrage levert aan het netwerk van informatiedeling en beeldvorming. Dit komt doordat het VR-ISAC de technische informatie van het Nationaal Cyber Security Centrum (NCSC) over de oorzaak van een cybercrisis kan vertalen naar de gevolgen voor de maatschappij. Tijdens de Operationeel-Leider call (OL-call) in de ISIDOOR-oefening ontstond er onder de actoren veel verwarring, aangezien zij niet in staat waren om de technische informatie op de juiste manier te vertalen en te duiden. Door de rol van het VR-ISAC als vertaler formeel vast te leggen, wordt het gedeelde begrip tussen de actoren binnen het netwerk van informatiedeling en beeldvorming aanzienlijk versterkt.

c. Het formeel vastleggen van de OL-call als belangrijk platform voor communicatie en informatie-uitwisseling tussen actoren. Uit dit onderzoek blijkt dat actoren in de praktijk

gebruik maken van de OL-call om met elkaar te communiceren en informatie te delen. Het vastleggen van de OL-call in de nieuwe planvorming zorgt ervoor dat alle betrokken actoren een duidelijk begrip hebben van de werking van de OL-call en het moment waarop deze call moet plaatsvinden. Dit voorkomt misverstanden in de toekomst en kan bijdragen aan het opbouwen van het onderling vertrouwen tussen actoren.

d. Het verduidelijken van de contactlijn tussen de veiligheidsregio's en het NCSC. Uit dit onderzoek blijkt dat de veiligheidsregio's in de huidige formele documenten niet worden erkend als vitale partners van het NCSC. In de praktijk blijkt daarentegen dat deze twee actoren contact met elkaar hebben. Hierdoor kunnen de veiligheidsregio's feitelijk worden beschouwd als vitale partners van het NCSC. Het is dan ook raadzaam om dit vast te leggen in de nieuwe planvorming.

Aanbeveling 2: Regelmatig met elkaar oefenen
De tweede aanbeveling is om frequenter netwerkbijeenkomsten te organiseren, waarin de betrokken actoren uit het netwerk van informatiedeling en beeldvorming samenkomen. Uit dit onderzoek blijkt dat het netwerk slechts bijeenkomt tijdens de ISIDOOR-oefening in de koude fase of tijdens een daadwerkelijke cybercrisis in de warme fase. Aangezien de ISIDOOR-oefening eens per twee jaar wordt georganiseerd en een daadwerkelijke landelijke cybercrisis relatief uniek is, is het wenselijk om meer met elkaar te gaan oefenen. Door regelmatig met elkaar te oefenen wordt de betrokkenheid binnen het netwerk vergoot, leren actoren elkaar beter kennen, wordt er meer ervaring opgedaan en kan het onderling vertrouwen tussen actoren versterkt worden.

Aanbeveling 3: Gezamenlijke doelen formuleren
De laatste aanbeveling betreft het formuleren van gezamenlijke doelen. Dit onderzoek heeft aangetoond dat er binnen het netwerk van informatiedeling en beeldvorming geen gezamenlijke doelen worden geformuleerd. Dit werd duidelijk tijdens de ISIDOOR-oefening, omdat actoren niet wisten wat ze van elkaar konden verwachten en ieder van hen voornamelijk bezig was met het behalen van zijn of haar eigen doelen. Het is dan ook wenselijk om gezamenlijke doelen met elkaar vast te stellen, zodat actoren duidelijk weten wat ze van elkaar kunnen verwachten in een crisissituatie en dezelfde richting opgaan. Dit bevordert het gevoel van eigenaarschap binnen de samenwerking, aangezien actoren zich dan meer verantwoordelijk zullen voelen voor het behalen van de gestelde doelen. Uiteindelijk zal dit het vertrouwen tussen actoren versterken en de motivatie binnen het netwerk verhogen.

Kortom, voor het effectief bestrijden van een landelijke cybercrisis in de toekomst is het belangrijk dat de bevindingen en aanbevelingen van dit onderzoek in acht worden genomen. Dit zal uiteindelijk gaan bijdragen aan een weerbare en veiligere samenleving.

Literatuurlijst

Adham, T. K. I. (2023). Conflict resolution in team: Analyzing the cause of conflicts and best skills for conflict resolution. *Scholars Journal of Engineering and Technology, 11*(8), 152-163. DOI:10.36347/sjet.2023.v11i08.001

Alexander, J. A., Comfort, M. E., & Weiner, B. J. (1998). Governance in public-private community health partnerships: A survey of the community care network℠ demonstration sites. *Nonprofit Management & Leadership, 8*(4), 311-332. https://doi.org/10.1002/nml.8402

Ansell, C. (2012). *Collaborative governance*. Oxford University Press.

Ansell, C., & Boin, A. (2019). Taming deep uncertainty: The potential of pragmatist principles for understanding and improving strategic crisis management. *Administration & Society, 51*(7), 1079-1112. https://doi.org/10.1177/0095399717747655

Ansell, C., & Gash, A. (2007). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory, 18*(4), 543-571. https://doi.org/10.1093/jopart/mum032

Ansell, C., & Gash, A. (2017). Collaborative platforms as a governance strategy. *Journal of Public Administration Research and Theory, 28*(1), 16-32. https://doi.org/10.1093/jopart/mux030

Bleijenbergh, I. (2013). *Kwalitatief onderzoek in organisaties.* Boom Uitgevers.

Boeije, H. R., & Bleijenbergh, I. (2019). *Analyseren in kwalitatief onderzoek: Denken en doen.* Boom Uitgevers.

Boin, A., Linck, R., Duin, M. van, Hendriks, J., Berger, E., & Varst, L. van der (2020). *Versterken van veerkracht: Naar een gezamenlijke aanpak van ongekende crises.* Instituut Fysieke Veiligheid. https://nipv.nl/wp-content/uploads/2022/02/20200317-IFV-Versterken-van-veerkracht.pdf

Borgatti, S. P., & Halgin, D. S. (2011). On network theory. *Organization Science, 22*(5), 1168-1181. https://doi.org/10.1287/orsc.1100.0641

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27-40. https://doi.org/10.3316/QRJ0902027

Brainich, E., & Dam, M. ten (2021). *Bestuurlijke netwerkkaarten crisisbeheersing: Rampenbestrijding algemeen & handhaving openbare orde.* Instituut Fysieke Veiligheid. https://archief.nipv.nl/wp-content/uploads/sites/2/2022/03/20210215-IFV-BNK-1-Rampenbestrijding-en-handhaving-openbare-orde.pdf

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Broeders, S., & Varst, L. van der (2024). *Sectorale evaluatie ISIDOOR-4.* Nederlands Instituut Publieke Veiligheid. https://nipv.nl/wp-content/uploads/2024/05/20240201-NIPV-Sectorale-evaluatie-ISIDOOR-4.pdf

Bryman, A. (2012). *Social research methods.* Oxford University Press.

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2006). The design and implementation of cross-sector collaborations: Propositions from the literature. *Public Administration Review, 66*(1), 44-55. https://doi.org/10.1111/j.1540-6210.2006.00665.x

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2015). Designing and implementing cross-sector collaborations: Needed and challenging. *Public Administration Review, 75*(5), 647-663. https://doi.org/10.1111/puar.12432

COT (2024). *Evaluatie ISIDOOR IV.* COT Instituut voor Veiligheids- en Crisismanagement. https://www.nctv.nl/documenten/publicaties/2024/08/23/evaluatie-isidoor-iv

Cumming, G. S. (2016). Heterarchies: Reconciling networks and hierarchies. *Trends in Ecology & Evolution, 31*(8), 622-632. https://doi.org/10.1016/j.tree.2016.04.009

Delden, P. van (2009). *Samenwerking in de publieke dienstverlening: Ontwikkelingsverloop en resultaten.* Uitgeverij Eburon.

Domrose, J., & Varst, L. van der (2020). *Cyberrisico's en veiligheidsregio's: Hoe beoordelen veiligheidsregio's cyberrisico's?* Instituut Fysieke Veiligheid. https://nipv.nl/wp-content/uploads/2022/02/20200228-IFV-Cyberrisicos-en-veiligheidsregios.pdf

Domrose, J., & Varst, L. van der (2021). *Evaluatie veiligheidsregio's ISIDOOR 2021*. Instituut Fysieke Veiligheid. https://nipv.nl/wp-content/uploads/2022/03/20210927-IFV-Evaluatie-veiligheidsregios-ISIDOOR-2021.pdf

Duin, M. van (2019). *KPN-storing: Hoe bestuurlijk omgaan met gebiedsontbonden crises?* Instituut Fysieke Veiligheid. https://archief.nipv.nl/wp-content/uploads/sites/2/2022/03/20200220-IFV-KPN-storing-hoe-bestuurlijk-omgaan-gebiedsontbonden-crises.pdf

Emerson, K., & Nabatchi, T. (2015). *Collaborative governance regimes.* Georgetown University Press.

Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of Public Administration Research and Theory, 22*(1), 1-29. https://doi.org/10.1093/jopart/mur011

Findley, M. G., Kikuta, K., & Denly, M. (2021). External validity. *Annual Review of Political Science, 24*(1), 365-393. https://doi.org/10.1146/annurev-polisci-041719-102556

Goldsmith, S., & Eggers, W. D. (2004). *Governing by network: The new shape of the public sector.* Brookings Institution Press.

Grenier, A. (2023). The qualitative embedded case study method: Exploring and refining gerontological concepts via qualitative research with older people. *Journal of Aging Studies, 65*(1), 1-10. https://doi.org/10.1016/j.jaging.2023.101138

Heale, R., & Twycross, A. (2018). What is a case study? *BMJ Journals, 21*(1), 7-9. https://doi.org/10.1136/eb-2017-102845

Heijmen, D., Varst, L. van der, & Groenendaal, J. (2021). *Cyberscenario's voor veiligheidsregio's.* Instituut Fysieke Veiligheid & Haagse Hogeschool. https://nipv.nl/wp-content/uploads/2022/03/20210616-IFV-Cyberscenarios-voor-veiligheidsregios.pdf

Hooymans, S. (2019). *Whitepaper digitale ontwrichting en cyber.* Instituut Fysieke Veiligheid. https://nipv.nl/wp-content/uploads/2022/05/20190912-IFV-Whitepaper-digitale-ontwrichting-en-cyber.pdf

Kenis, P. N., & Provan, K. G. (2008). Het network-governance-perspectief. In T. Wentink (Red.), *Business performance management: Sturen op prestatie en resultaat*, 296-312. Boom Academic.

Klijn, E. H., Edelenbos, J., & Steijn, B. (2010). Trust in governance networks: Its impacts on outcomes. *Administration & Society, 42*(2), 193-221. https://doi.org/10.1177/0095399710362716

Klijn, E. H., & Koppenjan, J. (2016). *Governance networks in the public sector.* Routledge.

Koppenjan, J., & Klijn, E. H. (2004). *Managing uncertainties in networks: A network approach to problem solving and decision making.* Routledge.

Littooij, A., & Eck, M. van (2015). *Handreiking: De veiligheidsregio bij dreigende verstoring of uitval van vitale voorzieningen.* Veiligheidsberaad & ministerie van Justitie en Veiligheid. https://nipv.nl/wp-content/uploads/2022/06/20151204-VB-VenJ-Handreiking-De-veiligheidsregio-bij-dreiging-verstoring-uitval-vitale-voorzieningen.pdf

Lo, C. (2017). Between government and governance: Opening the black box of the transformation thesis. *International Journal of Public Administration, 41*(8), 650-656. https://doi.org/10.1080/01900692.2017.1295261

Muller, E., Berndsen, M., Graaf, B. de, Kramers, N., Schnelders, B., & Verlaan, P. (2020). *Evaluatie Wet veiligheidsregio's: Naar de toekomstbestendige crisisbeheersing en brandweerzorg.* Evaluatiecommissie Wet veiligheidsregio's. https://open.overheid.nl/documenten/ronl-ba7df199-91c7-4f4b-8469-5e775b4fc4aa/pdf

Myers, M. D. (2013). *Qualitative research in business and management.* SAGE Publications.

NCSC (z.d.). *ISIDOOR.* Nationaal Cyber Security Centrum. Geraadpleegd op 13 maart 2024 van https://www.ncsc.nl/wat-doet-het-ncsc-voor-jou/isidoor

NCSC (2024). *Update wereldwijde storing Crowdstrike.* Nationaal Cyber Security Centrum. Geraadpleegd op 9 maart 2025 van https://www.ncsc.nl/actueel/nieuws/2024/juli/19/wereldwijde-storing

NCTV (2022a). *Landelijk Crisisplan Digitaal*. Nationaal Coördinator Terrorismebestrijding en Veiligheid. https://open.overheid.nl/documenten/ronl-43856896b0650c82103312680f9c830c09b5f485/pdf

NCTV (2022b). *Nationaal Handboek Crisisbeheersing.* Nationaal Coördinator Terrorismebestrijding en Veiligheid. https://www.nctv.nl/documenten/publicaties/2022/12/06/nationaal-handboek-crisisbeheersing

NCTV (2023a). *Cybersecuritybeeld Nederland 2023*. Nationaal Coördinator Terrorismebestrijding en Veiligheid. https://www.nctv.nl/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023

NCTV (2023b). *Crisiscommunicatie in het digitale domein.* Nationaal Coördinator Terrorismebestrijding en Veiligheid. https://www.nctv.nl/documenten/publicaties/2023/01/31/koepelnotitie-communicatie-bij-digitale-incidenten

NCTV (2024). *Cybersecuritybeeld Nederland 2024*. Nationaal Coördinator Terrorismebestrijding en Veiligheid. https://www.nctv.nl/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024

Nederhof, A. J. (1985). Methods of coping with social desirability bias: A review. *European Journal of Social Psychology, 15*(3), 263-280. https://doi.org/10.1002/ejsp.2420150303

NIPV (z.d.a). *Landelijk Crisis Management Systeem (LCMS).* Nederlands Instituut Publieke Veiligheid. Geraadpleegd op 10 december 2024 van https://nipv.nl/informatievoorziening/voorzieningen/landelijk-crisis-management-systeem/

NIPV (z.d.b). *Digitale weerbaarheid.* Nederlands Instituut Publieke Veiligheid. Geraadpleegd op 27 januari 2025 van https://nipv.nl/onderwerp/digitale-weerbaarheid/

Provan, K. G., & Kenis, P. N. (2008). Modes of network governance: Structure, management, and effectiveness. *Journal of Public Administration Research and Theory, 18*(2), 229-252. https://doi.org/10.1093/jopart/mum015

Rijksoverheid (z.d.a). *Veiligheidsregio's.* Geraadpleegd op 20 maart 2024 van https://www.rijksoverheid.nl/onderwerpen/veiligheidsregios-en-crisisbeheersing/veiligheidsregios

Rijksoverheid (z.d.b). *Landelijk Operationeel Coördinatiecentrum (LOCC).* Geraadpleegd op 10 december 2024 van https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid/organisatie/organogram/directoraat-generaal-politie-en-veiligheidsregio%E2%80%99s-dgpenv/landelijk-operationeel-coordinatiecentrum-locc

Rinehart, K. E. (2020). Abductive analysis in qualitative inquiry. *Qualitative Inquiry, 27*(2), 303-311. https://doi.org/10.1177/1077800420935912

Schwartz-Shea, P., & Yanow, D. (2012). *Interpretive research design: Concepts and processes.* Routledge.

Sonnenwald, D. H. (2006). Challenges in sharing information effectively: Examples from command and control. *Information Research, 11*(4), 251-270. https://files.eric.ed.gov/fulltext/EJ1104659.pdf

Sørensen, E., & Torfing, J. (2005). The democratic anchorage of governance networks. *Scandinavian Political Studies, 28*(3), 195-218. https://doi.org/10.1111/j.1467-9477.2005.00129.x

Thiel, S. van (2014). *Research methods in public administration and public management: An introduction.* Routledge.

Thiel, S. van (2015). *Bestuurskundig onderzoek: Een methodologische inleiding.* Uitgeverij Coutinho.

Turell, J., Su, F., & Boulanin, V. (2020). Lessons from past cyber incidents and country studies. In J. Turell, F. Su & V. Boulanin (Reds.), *Cyber-incident management: Identifying and dealing with the risk of escalation,* 32-42. Stockholm International Peace Research Institute. http://www.jstor.org/stable/resrep26199.11

Vangen, S., & Huxham, C. (2003). Enacting leadership for collaborative advantage: Dilemmas of ideology and pragmatism in the activities of partnership managers. *British Journal of Management, 14*(1), 61-76. https://doi.org/10.1111/j.1467-8551.2003.00393.x

Varst, L. van der, Groenendaal, J., Bantema, W., & Cools, F. (2022). *Bestuurlijke bevoegdheden cyber: Bevoegdheden en interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio bij (dreigende) digitale incidenten.* Nederlands Instituut Publieke Veiligheid. https://nipv.nl/wp-content/uploads/2023/01/20220930-NIPV-Bestuurlijke-bevoegdheden-cyber.pdf

Varst, J. van der, Heijmen, D., Berger, E., Sleen, T. van der, & Bosman, E. (2020). *Cybergevolgbestrijding: Lessen uit cyberverstoringen in Nederland.* Instituut Fysieke Veiligheid. https://nipv.nl/wp-content/uploads/2022/02/20201202-IFV-Cybergevolgbestrijding.pdf

Veiligheidsberaad (z.d.a). *Landelijk Crisisplan Digitaal omarmd.* Geraadpleegd op 6 december 2024 van https://www.veiligheidsberaad.nl/2022/12/21/landelijk-crisisplan-digitaal-omarmd/

Veiligheidsberaad (z.d.b). *Het Veiligheidsberaad*. Geraadpleegd op 8 december 2024 van https://www.veiligheidsberaad.nl/

Veiligheidsregio IJsselland (2022). *Crisisplan 2023-2026: Samen veiligheid versterken.* https://www.vrijsselland.nl/wpcontent/uploads/2023/01/Crisisplan-2023-2026.pdf

Veiligheidsregio Utrecht (2022). *Aandachtskaart cybergevolgbestrijding/digitale ontwrichting.* https://vru-prd-minio.fourdigits.nl//media/documents/AB20220328-07-3_Bijlage_B_-_Aandachtskaart_Cybergevolgbestrijding_VRU_0.pdf

Voets, J., Brandsen, T., Koliba, C., & Verschuere, B. (2021). Collaborative governance. In G. Peters & I. Thynne (Reds.), *The Oxford encyclopedia of politics*, 1-21. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1419

Vreke, J., Gerritsen, A. L., Kranendonk, R. P., Pleijte, M., Kersten, P. H., & Bosch, F. J. P. van den (2009). *Maatlat government-governance.* Wettelijke Onderzoekstaken Natuur & Milieu. https://edepot.wur.nl/8170

Weerwind, F. (2018). *De rol van de veiligheidsregio's bij digitale ontwrichting*. Veiligheidsberaad. file:///C:/Users/noorb/Downloads/De-rol-van-de-veiligheidsregios-bij-digitale-ontwrichting%20(7).pdf

Bijlagen

Bijlage A: Topiclijst semigestructureerde interviews

Inleiding

- Voorstellen en toestemming vragen aan de respondent om het interview op te nemen en te transcriberen;
- Uitleggen over wat het onderzoek inhoudt en wat het doel is;
- Introductie respondent:
  - Wie bent u en wat is uw functie?

Startcondities

1. Welke actoren zijn betrokken bij het netwerk van informatiedeling en beeldvorming tijdens een landelijke cybercrisis?

2. Wat vindt u van de formele plannen die zijn vastgelegd?
  - Wat vindt u van de rollen, taken en verantwoordelijkheden?
  - En hoe zit het met de regels en procedures?

3. Kunt u vertellen welke prikkels er zijn om samen te werken binnen dit netwerk?

4. Hoe ervaart u de verdeling van macht en middelen van actoren binnen het netwerk?

5. Hebben er al eerdere samenwerkingen plaatsgevonden met actoren uit dit netwerk? Zo ja, heeft dit invloed op de huidige samenwerking binnen het netwerk?

Communicatie & vertrouwen

6. Kunt u wat vertellen over de wijze van communicatie en informatie-uitwisseling binnen het netwerk?

7. Wat is uw ervaring met de vaktaal die wordt gesproken?

8. Kunt u vertellen hoe het zit met het vertrouwen in actoren binnen het netwerk?
  - Heeft u vertrouwen in de expertise van actoren?
  - Heeft u er vertrouwen in dat actoren afspraken nakomen?

9. Vindt u dat er binnen het netwerk genoeg aandacht wordt besteed aan het versterken van onderling vertrouwen tussen actoren?

Gedeelde betekenisgeving

10. Kunt u wat vertellen over hoe actoren het probleem binnen het netwerk definiëren?

11. Kunt u wat vertellen over de gezamenlijke doelen binnen het netwerk?

Toewijding aan het proces & tussentijdse resultaten

12. Wat vindt u van de betrokkenheid binnen het netwerk? Hoe vaak vindt er overleg plaats?

13. Je hebt andere actoren vaak nodig binnen een netwerk, wat is uw ervaring daarmee?

14. Heerst er een gevoel van gedeeld eigenaarschap binnen het netwerk?

15. Wordt er binnen het netwerk ook stilgestaan bij tussentijdse resultaten? Zo ja, hoe ervaart u dit en worden hier lessen uit getrokken?

Leiderschap

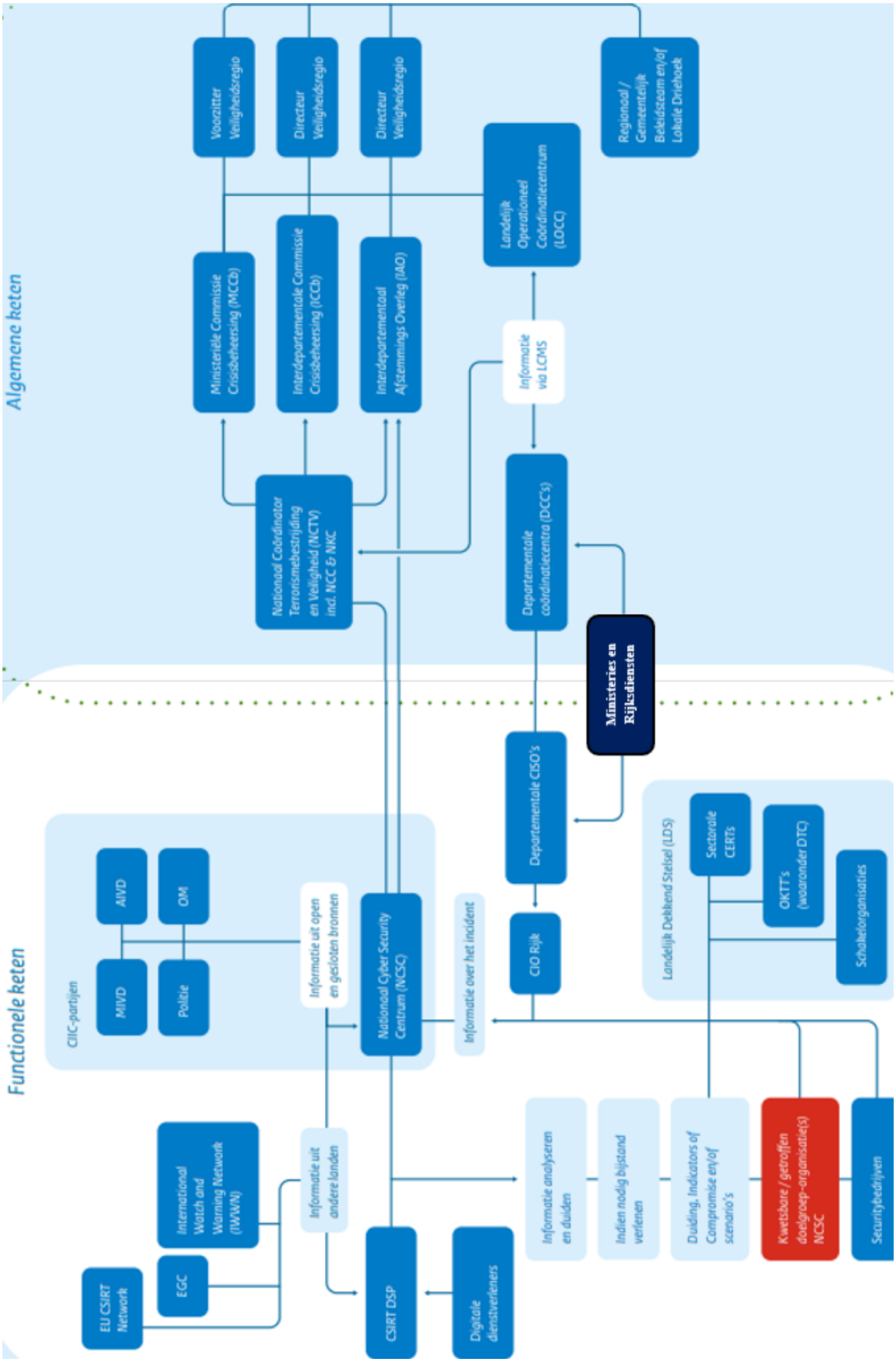
16. Wie stuurt het netwerk aan en wat is uw ervaring hiermee?
  - Draagt de leider bij aan het opbouwen van vertrouwen?
  - En het faciliteren van communicatie tussen actoren?

- Is de leider in staat om de verschillende vaktalen binnen het netwerk te begrijpen en met elkaar te verbinden?

Afsluiting

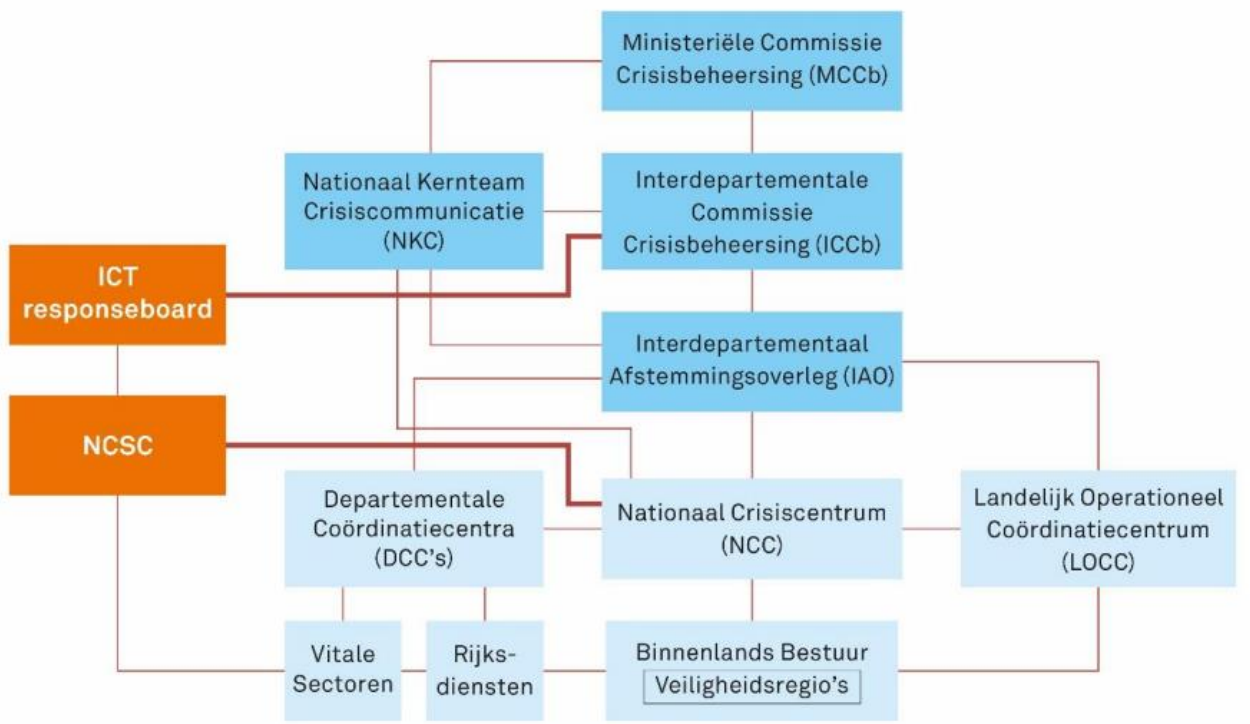
- Zijn er nog eventuele aanbevelingen of dingen die u kwijt wil?
- Bedanken.

Bijlage B: Samenwerkingsstructuur tussen de functionele & algemene keten



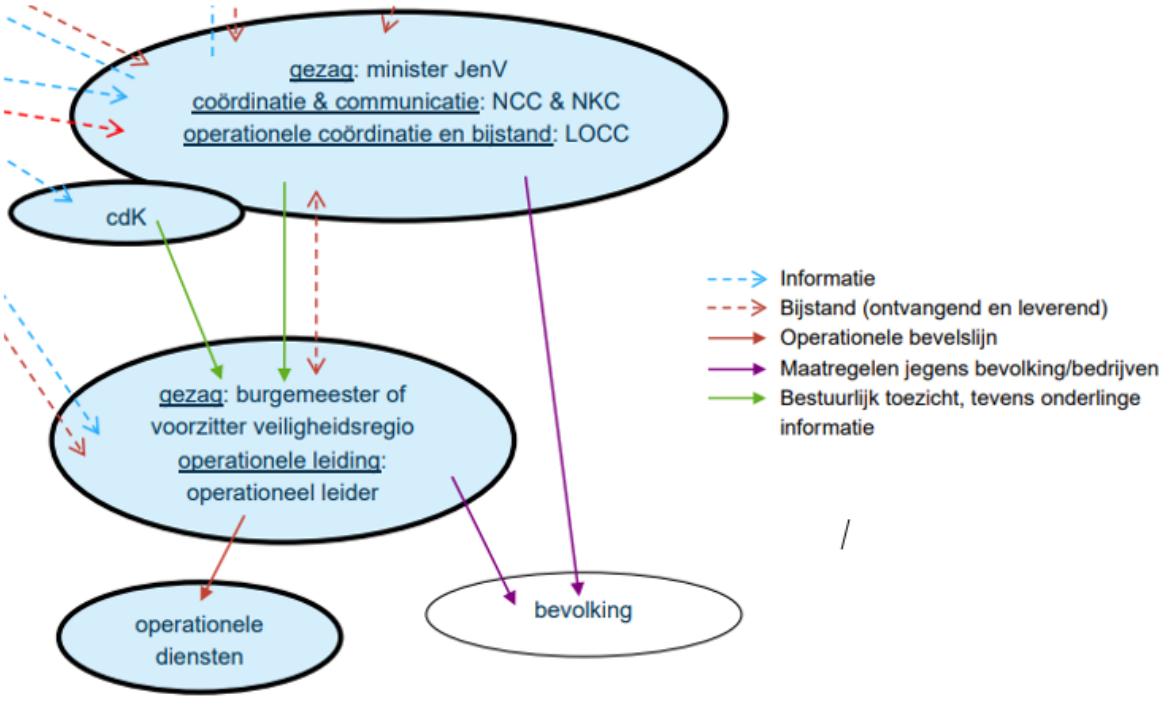
Figuur B1: Informatielijnen tussen de functionele en algemene keten (NCTV, 2022a, pp. 16-17).

Bijlage C: Informatielijnen binnen de algemene keten



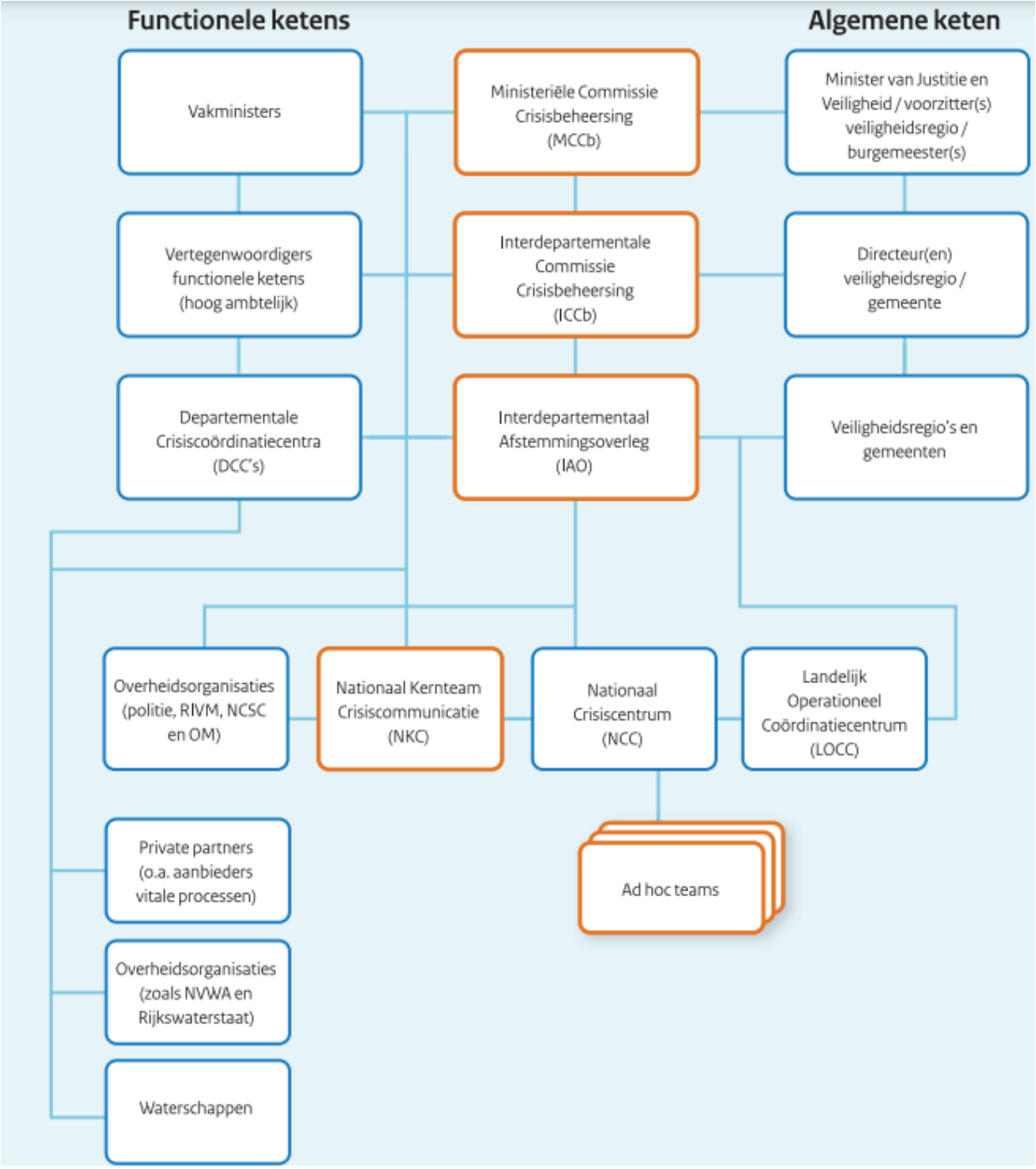
Figuur C1: Informatielijnen binnen de algemene keten (Hooymans, 2019, p. 19).

Bijlage D: Gezagslijnen tijdens een landelijke cybercrisis



Figuur D1: Gezagslijnen tijdens een landelijke cybercrisis (Brainich & Ten Dam, 2021, p. 10).

Bijlage E: Hoofdlijnen nationale crisisstructuur



Figuur E1: Hoofdlijnen nationale crisisstructuur (NCTV, 2022b, p. 34).