NIPV Nederlands Instituut Publieke Veiligheid

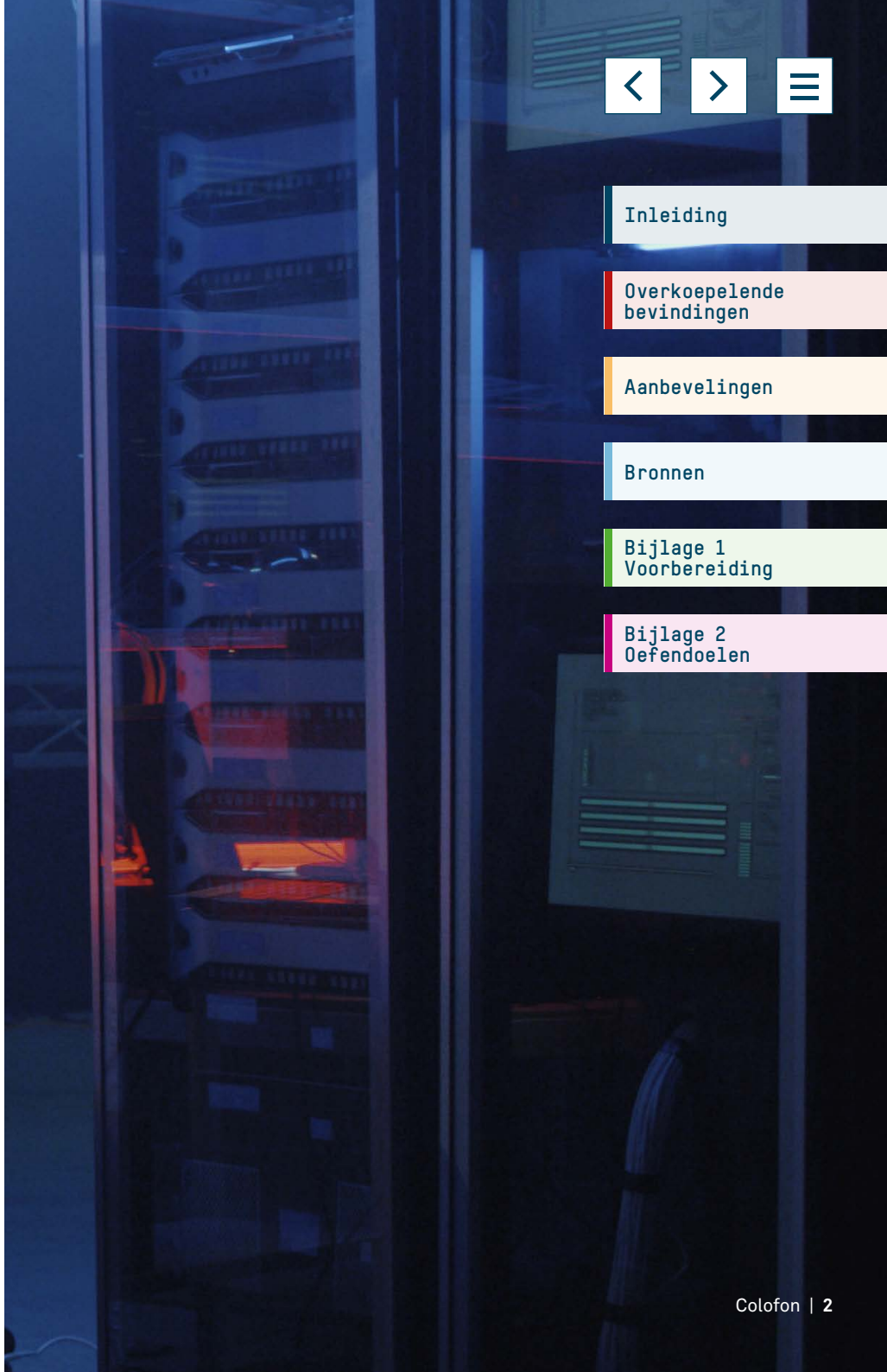
Sectorale evaluatie ISIDOOR-4

Veiligheidsregio's, LOCC en VR-ISAC

Colofon

Auteurs	S. Broeders en L. van der Varst
Met medewerking van	F. Cools
Contactpersoon	L. van der Varst
Opdrachtgever	L. Bril (VRU) en C. de Boer (VRK) Werkgroep Cyber en Digitale Ontwrichting/ RCDV
Datum	1 februari 2024
Foto's	Shutterstock

Het Nederlands Instituut Publieke Veiligheid is bij wet vastgelegd onder de naam Instituut Fysieke Veiligheid.



Inleiding

Overkoepelende bevindingen

Aanbevelingen

Bronnen

Bijlage 1 Voorbereiding

Bijlage 2 Oefendoelen

Inhoud

Inleiding 4

1. Overkoepelende bevindingen 6
1.1 Overkoepelende impressie 7
1.2 Crisisorganisatie 7
1.3 Werkwijzen 8
1.4 Mogelijkheden versterken landelijke aanpak cybercrises 12

2. Aanbevelingen 13
2.1 OL-call: leiderschap en regie 14
2.2 Opbouw landelijk operationeel beeld 14
2.3 Planvorming voor landelijke (cyber)crises 14
2.4 Opleiding: wegwijs in de landelijke structuur 15
2.5 Scenariodenken: anticiperen op de middellange termijn 15

Bronnen 16

Bijlage 1 17

Bijlage 2 19

Inleiding

Beschrijving oefening

ISIDOOR is een tweejaarlijkse grootschalige cyberoefening; de vierde editie, ISIDOOR 2023, vond plaats in november 2023. Tevens werd later die maand als onderdeel van de cyberoefening de Interdepartementale Commissie Crisisbeheersing (ICCB) beoefend. De oefening simuleert een cyberincident dat uit meerdere soorten aanvallen bestaat en uiteindelijk een bedreiging vormt voor de nationale stabiliteit en veiligheid.[1]

De oefening wordt georganiseerd door het Nationaal Cyber Security Centrum (NCSC) in samenwerking met de Nationaal Coördinator Terrorisme en Veiligheid (NCTV) en het COT Instituut voor Veiligheids- en Crisismanagement. Aan de oefening namen meer dan honderdtwintig organisaties deel en ruim drieduizend deelnemers uit sectoren als drinkwatervoorziening, telecom en energie.

ISIDOOR beoefent de crisisprocedures zoals beschreven in het LCP Digitaal, de crisishandboeken, Koepelnotitie crisiscommunicatie digitaal domein, het Nationaal Handboek Crisisbesluitvorming en de Wet Beveiliging Netwerk- en Informatiesystemen (WBNI). Op Rijksniveau is geoefend met de volgende doelstellingen:

1. Het beoefenen van informatie-uitwisseling en samenwerking (op alle niveaus) ten tijde van een cybercrisis.
2. Het beoefenen van de nationale opschalingsstructuur volgend op een cybercrisis, tot en met het niveau van een Ministeriële commissie Crisisbeheersing (MCCb).
3. Het versterken van de onderlinge samenwerking tussen de vitale en rijksoverheidsorganisaties.

De accenten liggen op de coördinatie en samenwerking tussen landelijk en sectorale organisaties, en tussen het fysieke en het cyberdomein.

Opdracht

Het NIPV heeft in opdracht van de Werkgroep Digitale ontwrichting en cyber van de RCDV de sectorale evaluatie uitgevoerd van de inzet van de veiligheidsregio's, het Landelijk Operationeel Coördinatiecentrum (LOCC) en VR-ISAC tijdens de cyberoefening ISIDOOR-4. Dit document is daarvan het resultaat. De veiligheidsregio's, het LOCC en VR-ISAC hebben daarnaast eigen evaluaties uitgevoerd.

Deelnemers

Sectorale deelnemers aan ISIDOOR-4 waren:

- Veiligheidsregio Rotterdam-Rijnmond
- Veiligheidsregio IJsselland
- Veiligheidsregio Haaglanden
- Veiligheidsregio Utrecht
- NoordWest-4 (Veiligheidsregio Amsterdam-Amstelland, Kennemerland, Noord-Holland-Noord en Zaanstreek-Waterland)
- LOCC
- VR-ISAC.

1 Draaiboek ISIDOOR IV 2023. Veiligheidsregio's, LOCC, VR-ISAC.

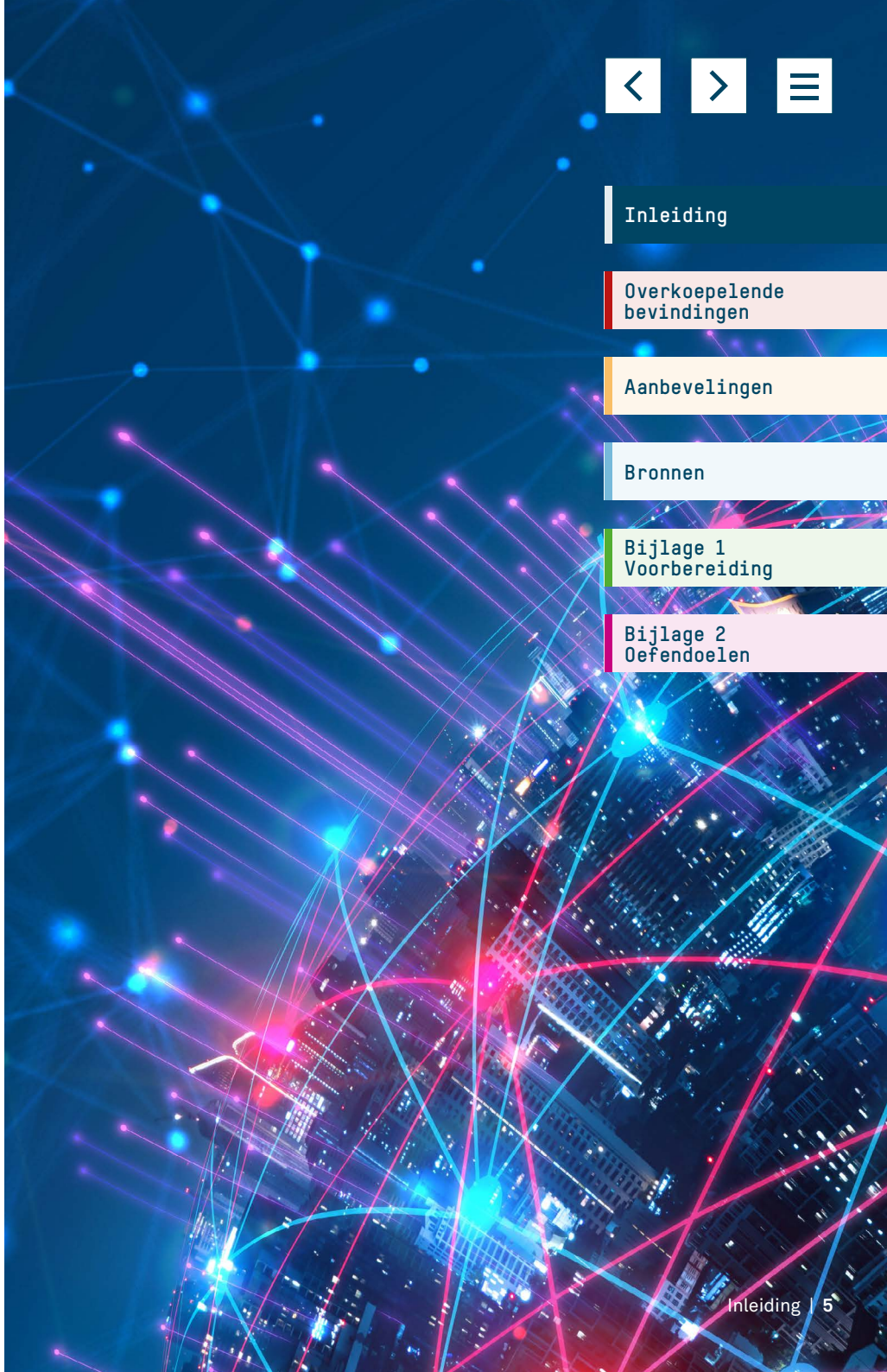
Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

Aanpak evaluatie

In het kader van deze evaluatie is door het NIPV een evaluatieformulier opgesteld. Dit formulier is ter beschikking gesteld aan de evaluatoren en oefenleiders. De evaluatoren hebben het formulier gebruikt voor het vastleggen van leerpunten. Alle acht deelnemende organisaties hebben het formulier ingevuld. Aanvullend hebben de evaluatoren twee leersessies begeleid. Op 16 november vond een leersessie plaats die gericht was op het identificeren van knelpunten en goede praktijken (15 evaluatoren en oefenleiders). Op 22 november vond een tweede leersessie plaats met 26 deelnemers namens veiligheidsregio's, LOCC en VR-ISAC. Tijdens deze bijeenkomst zijn voorlopige leerbevindingen besproken. De onderzoekers hebben tevens als waarnemer deelgenomen aan twee OL-calls (op 14 en 15 november). Op basis van de verzamelde gegevens is dit rapport opgesteld.

Leeswijzer

Hoofdstuk 1 bevat onze bevindingen. In hoofdstuk 2 formuleren we vier adviezen voor het versterken van de landelijke aanpak van (cyber) crises. Bijlage 1 bevat informatie over de wijze waarop de deelnemers zich hebben voorbereid op ISIDOOR-4. In bijlage 2 lichten we de oefendoelen toe en presenteren we de uitkomsten van een peiling onder deelnemers.



Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

1. Overkoepelende bevindingen

Dit hoofdstuk bevat de bevindingen; de focus ligt daarbij op de bovenregionale samenwerking tussen de veiligheidsregio's, het LOCC en VR-ISAC binnen de landelijke crisisstructuur. In algemene zin heeft de oefening bijgedragen aan bewustwording en vakbekwaamheid van deelnemers. Daarnaast zijn binnen de regio's nieuwe inzichten opgedaan, bijvoorbeeld over de meerwaarde van een Interregionaal Operationeel Team (IROT), de rol van cyberburgemeesters bij cybercrises en afstemming met VR-ISAC bij interne cyberincidenten.

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

1.1 Overkoepelende impressie

Over het algemeen is door de deelnemers een rustige, maar ook serieuze sfeer ervaren tijdens de oefendagen. Zowel binnen, als tussen de teams was de sfeer goed. Toch voelden een aantal teams spanning, doordat zij niet goed aan de voorkant van het scenario wisten te komen.

De start van de oefening werd gekenmerkt als wat chaotisch en onduidelijk. Dat kan verband houden met het feit dat de crisisteams van de veiligheids-regio's halverwege de oefening 'instapten in een rijdende trein' en daardoor wat onwennig waren en tijd nodig hadden om zich in het scenario in te leven. Overkoepelend geven evaluatoren aan dat de oefening heeft bijgedragen aan bewustwording, aan kennismaking en gevoel krijgen bij de cybercontext en het formuleren van actiepunten binnen de teams.

1.2 Crisisorganisatie

1.2.1 Onbekendheid landelijke crisisstructuur

Uit de evaluatie komt onbekendheid met het functioneren van de landelijke crisisstructuur naar voren: hoe lopen informatielijnen, wie doet wat, welke overleggen en activiteiten vinden op welk moment in de tijd plaats? Die onbekendheid is opmerkelijk, vanwege de inspanningen aan de voorkant om een gebruiksvriendelijk LCP-D op te stellen en de kennis over het plan onder deelnemers te vergroten, onder meer door het verzorgen van webinars. Anderzijds is de landelijke crisisstructuur niet eenvoudig én was het de eerste keer dat deelnemers oefenden met het LCP-D. Bovendien is de ervaring met de aanpak van landelijke (cyber)crises bij veiligheidsregio's beperkt.

De oefening heeft daarnaast een aantal zaken blootgelegd, die volgens betrokkenen in bestaande planvorming nog onvoldoende zijn uitgekristalliseerd. Hierbij gaat het onder andere om vragen als:

- Wie neemt er namens de veiligheidsregio's deel aan het Interdepartementaal Afstemmingsoverleg (IAO) en ICCB?
- Wat is de rol van het Veiligheidsberaad bij bovenregionale (cyber) crises en hoe en door wie wordt het Veiligheidsberaad in positie gebracht en van informatie voorzien?
- Hoe wordt informatie en (bestuurlijke) duiding uit het IAO teruggegeven naar de veiligheidsregio's en het LOCC?
- Waar ligt de verantwoordelijkheid voor afstemming over de duur, prognoses en maatschappelijke impact met vitale partners: is dat een regionale of juist landelijke verantwoordelijkheid?
- Wat mogen de deelnemende organisaties binnen de landelijke crisisstructuur van elkaar verwachten?
- Wat is de rol en scope van het landelijke scenarioteam (en wie participeren namens de veiligheidsregio's in het scenarioteam: IT-experts, adviseurs crisisbeheersing of beiden)?

Tevens merkt een evaluator op dat in de oefening 'de veiligheidsregio' als één entiteit wordt gezien, waardoor het onderscheid tussen de interne bedrijfsvoering ('het team cybersecurity & incidentrespons')[2] en cybergevolgbestrijding ('team crisisbeheersing')[3] verloren gaat. In het LCP-D zouden om die reden de taken, rollen en informatielijnen van een VR-ISAC, SOC en CERT als onderdeel van de zogenaamde functionele keten binnen de cyberspecifieke crisisstructuur opgenomen kunnen worden.

De deelname van een directeur aan de OL-call (die eerder namens de veiligheidsregio's deelnam aan het IAO) zien we daarbij als een goede praktijk. De directeur kon een terugkoppeling uit het IAO geven en daarmee bijdragen aan de eerste duiding van de ontstane situatie. Bovendien kon hij in het overleg meedenken over bestuurlijke opschaling en informatievoorziening. Dat voorzag in een duidelijke behoefte.

1.2.2 Bestuurlijke afstemming en informatievoorziening

In de tweede OL-call kwam 'bestuurlijke opschaling' aan de orde. Meerdere regio's waren op dat moment opgeschaald naar GRIP2. Met bestuurlijke opschaling leek in het overleg te worden bedoeld: het bijeenroepen van het Veiligheidsberaad (VB).[4] Uiteindelijk is daarvan afgezien, maar werd in de call wel besloten tot het informeren van het Veiligheidsberaad.

In relatie tot opschaling spelen enkele thema's die relevant zijn om verder te verkennen, namelijk:

- Tijdens crisisoverleg zorgen voor concretisering van het begrip ' opschaling', zodat voor iedereen helder is wat ermee wordt bedoeld:
  - Wat wordt hieronder concreet verstaan en wat is het beoogde doel?
  - Waarvoor is opschaling nodig en wat wil je ermee bereiken? Is er bijvoorbeeld behoefte aan de inzet van (nood)bevoegdheden,[5] is een 'bestuurlijke heads-up' wenselijk (zodat burgemeesters en voorzitters veiligheidsregio alvast op de hoogte zijn van wat er speelt) en/of is er behoefte aan afstemming tussen burgemeesters?
- Hoe worden burgemeesters en voorzitters veiligheidsregio tijdens bovenregionale en landelijke (cyber)crises van informatie voorzien (door wie, hoe)?
- Hoe vindt bij bovenregionale crises bestuurlijke afstemming plaats: is dat via het Interregionaal Beleidsteam (IRBT) of anderszins?
- Is het nodig dat alle deelnemende veiligheidsregio's uniform opschalen, ook als sommige regio's daar niet meteen aanleiding toe voelen?

1.3 Werkwijzen

1.3.1 OL-call

Tijdens de oefening werden er door het LOCC twee zogeheten OL-calls georganiseerd: op dinsdagmiddag en woensdagochtend. OL-calls zijn een middel voor gemeenschappelijke beeld-, oordeels- en besluitvorming. De calls vormen een goed platform voor afstemming, dat door veiligheidsregio's al meerdere keren is ingezet, waaronder tijdens Covid en ISIDOOR-3. De calls, waaraan de operationeel leiders van de veiligheidsregio's, twee VR-ISAC-leden en op woensdag een directeur namens de veiligheidsregio's deelnamen, werden voorgezeten door het LOCC.

2 Onderdeel van de zogenaamde functionele keten binnen de cyberspecifieke crisisstructuur.
3 Onderdeel van de zogenaamde algemene keten binnen de cyberspecifieke crisisstructuur.
4 Het Veiligheidsberaad is een bestuurlijk overlegorgaan. Het VB heeft in die zin geen bevoegdheid als bevoegd gezag met doorzettingsmacht.
5 Voor het gebruik van (nood)bevoegdheden door een burgemeester of voorzitter van de veiligheidsregio is het in juridische zin niet noodzakelijk om conform GRIP op te schalen. Een burgemeester of voorzitter kan ook zonder opschaling gebruikmaken van zijn (nood)bevoegdheden.

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

In de aansturing en structuur van de twee calls was tijdens de oefening duidelijk verbetering zichtbaar. De tweede call sloot beter bij de behoeften van deelnemers aan dan de eerste op dinsdagmiddag: er was sprake van méér structuur, minder technische informatie en méér gezamenlijke afstemming. Volgens betrokkenen ontbrak het binnen het overleg wel aan kennis en senioriteit, aan iemand die leiderschap en regie uitoefent. Dat leiderschap werd tijdens de oefening informeel gepakt door een directeur van de veiligheidsregio.

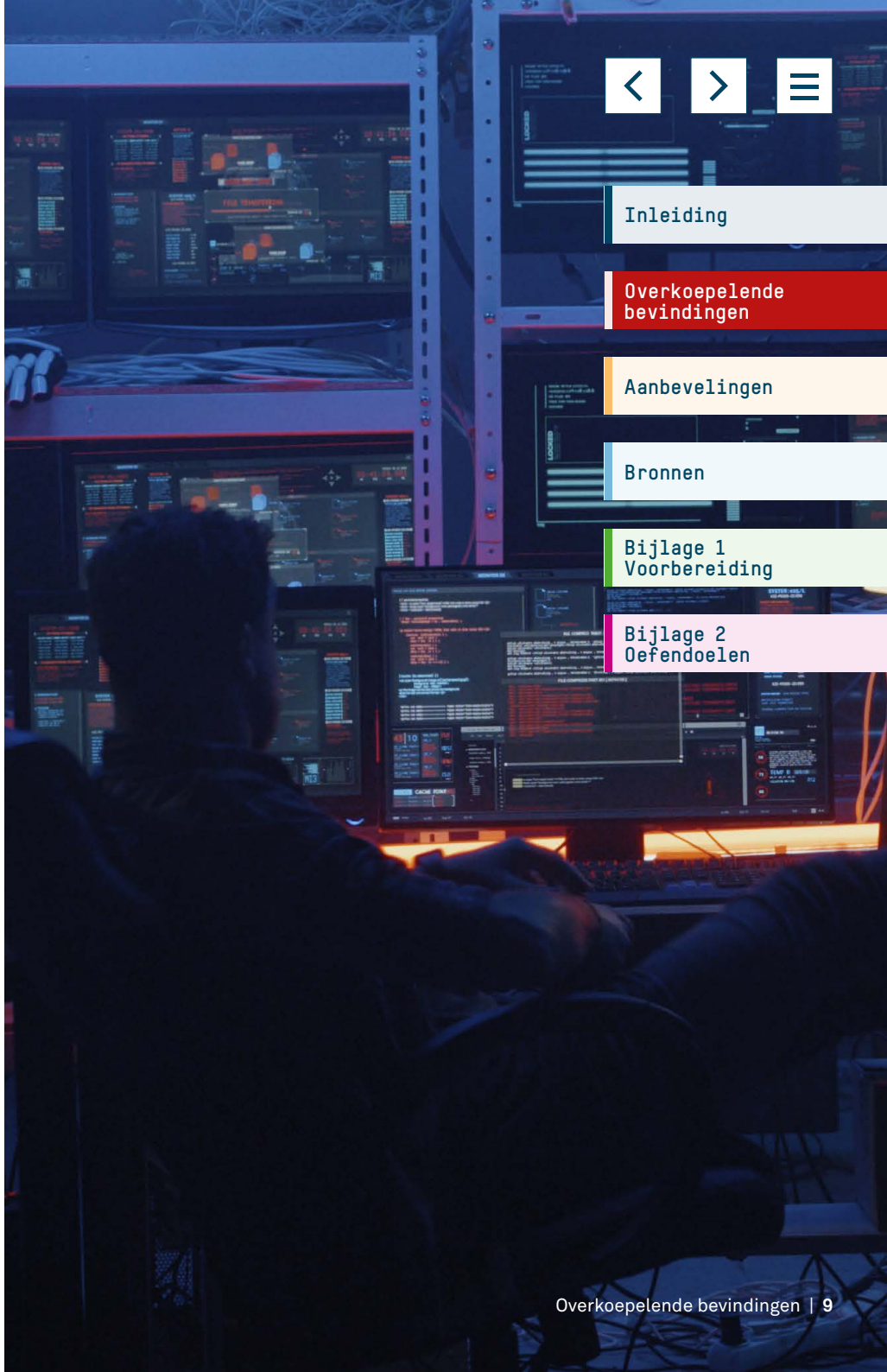
Lastig was bovendien dat in de eerste call zogenaamde 'incident handlers' vanuit het NCSC aansloten die de deelnemers voorzagen van technische cybersecurityinformatie (vakjargon). Die informatie bleek lastig te duiden voor de veiligheidsregio's. Normaliter zou dergelijke informatie van het NCSC bij het VR-ISAC terechtkomen.

1.3.2 Reageren én anticiperen op de middellange termijn

Belangrijke bevinding uit de tweede leersessie was de observatie dat binnen de algemene crisiskolom sprake was van een vrij reactieve crisisrespons, dat wil zeggen: een aanpak gericht op het 'hier-en-nu' (korte termijn). Voor veiligheidsregio's die zelf te maken krijgen met een intern cyberincident is dat logisch. Hun eerste prioriteit ligt in die situatie bij acute incidentbestrijding. In de oefening waren er al concrete problemen die zich voordeden (email werkte niet; computersystemen functioneerden niet; medewerkers konden niet inloggen); dergelijke problemen vormen een concrete trigger voor optreden.

Ontbreken dergelijke triggers,[6] dan blijven de volgende vragen in de lucht hangen: is er al aanleiding bijeen te komen als (crisis)team? Kunnen en

6 Hierbij kan het zowel gaan om interne triggers (zoals verstoring van de bedrijfsvoering/vitale processen) als externe triggers (zoals het optreden van maatschappelijke onrust of problemen ten aanzien van de levering van maatschappelijke diensten zoals drinkwater, transport en vervoer, elektriciteit en energie).



Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

moeten we nu al iets doen? Het inschatten van de situatie is, juist in dat grijze gebied waar signalen ontbreken of diffuus zijn,[7] natuurlijk lastig en vergt een andere aanpak dan veiligheidsregio's van nature gewend zijn.

Regio's die zelf niet getroffen waren en waar zich nog geen concrete fysieke effecten op de openbare orde en veiligheid manifesteerden, zouden zich juist kunnen richten op de middellange termijn, bijvoorbeeld door middel van scenariodenken. Dat middellange termijn denken en -handelen kwam tijdens de oefening, zeker op bovenregionaal niveau, onvoldoende uit de verf.

Voor bovenregionaal scenariodenken zijn voor zover bekend geen afspraken of werkwijzen beschikbaar. Wel heeft op landelijk niveau een scenario-bijeenkomst plaatsgevonden en heeft scenariodenken plaatsgevonden in regionale crisisteams, zoals in Veiligheidsregio Utrecht en bij 'Voorwaarts Denken' in IJsselland. Hierbij horen activiteiten zoals we die kennen uit planningsstaven of pre-ROT's:

- Scenario's opstellen: maatregelen en sleutelbesluiten uitwerken.
- Omgevingsanalyse: wat speelt er?
- Netwerkanalyse en -relaties: wat speelt er bij (vitale) organisaties in het verzorgingsgebied en hoe staan we met hen in verbinding? Hebben we al contact met hen opgenomen, weten we wat er speelt?

Verder werd in de leersessie opgemerkt dat veiligheidsregio's niet hoeven afwachten tot er daadwerkelijk fysieke effecten optreden, maar juist ook al eerder actie kunnen ondernemen om 'aan de voorkant van een incident te komen'. Zo hadden zij zelf bij het LOCC kunnen aandringen op een OL-call voor eerste beeldvorming en consultatie met andere regio's, in plaats van afwachten tot het LOCC zo'n overleg zou organiseren.

7 Met 'grijze gebied' bedoelen we de situatie waarin er weliswaar signalen van een dreiging en/of crisis zijn ('weak signals'), maar de dreiging zich nog niet heeft vertaald in incidenten en zichtbare maatschappelijke effecten.

Hierbij past de kanttekening dat de OL-call vooraf reeds gepland stond als onderdeel van de oefening.

1.3.3 Impact assessment: landelijk operationeel beeld

Goede beeld- en oordeelsvorming zijn bij een crisis belangrijk. Maar beeldvorming is ook altijd lastig, bijvoorbeeld door ontbrekende informatie of expertise om beschikbare informatie te duiden (NIPV, 2021). Tijdens de oefening speelden de volgende vraagstukken:

- Wie kan op bovenregionaal niveau de cyberspecifieke informatievoorziening vanuit het NCSC duiden?
- Wie heeft zicht op de vitale sectoren (aantal getroffen sectoren, ernst, duur en potentiële fysieke effecten)? Moeten veiligheids-regio's zelf de vitale partijen in hun verzorgingsgebied benaderen, of gebeurt dit landelijk?
- Wie brengt voor de veiligheidsregio's de impact op veiligheidsregio's én vitale sectoren in beeld?

In dit licht pleit een aantal deelnemers aan de oefening voor het nadenken over de vormgeving en opbouw van een integraal landelijk operationeel beeld. Tijdens de oefening heeft het VR-ISAC een rol gespeeld in het duiden en in beeld brengen van fysieke effecten. Hiervoor maakte het gebruik van de zogeheten 'Continuïteitsmonitor VR & Vitaal', een zelf opgestelde tool. Mogelijk kan deze tool behulp-zaam zijn bij de vorming van een operationeel beeld.

Een evaluator merkt op dat zowel het VR-ISAC als de crisisorgani-saties van de veiligheidsregio's vanuit de andere sectoren waarbij de continuïteit in het geding was, zoals de telecom-, energie- en watersector, weinig tot geen hulpvragen hebben gekregen De evaluator vindt dit opmerkelijk, mede gelet op de afspraken over melden en alarmeren uit het LCP-D (zie het kader op de volgende

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

pagina). Veiligheidsregio's werden, zoals ook al was geconstateerd in de evaluatie van ISIDOOR-3 (NIPV, 2021), niet actief benaderd door vitale partners. Hierdoor had men nauwelijks een beeld van potentiële maatschappelijke effecten op de regio's (en bleef het onduidelijk met welke scenario's zij rekening konden houden).[8]

Vitale partijen kunnen verschillende redenen hebben voor het niet informeren van veiligheidsregio's over cyberincidenten, bijvoorbeeld het uitblijven van fysieke gevolgen van interne incidenten. Of vitale partijen opereren vooral binnen hun eigen functionele keten. Een verkenning van achterliggende motivaties voor het al dan niet melden van incidenten zou op dit punt meer helderheid kunnen scheppen.

Melden van digitale incidenten met fysieke effecten

In het Landelijk Crisisplan-Digitaal (LCP-D) zijn de volgende richtlijnen opgenomen over het melden van digitale incidenten met (potentiële) impact voor de fysieke veiligheid en openbare orde:

- Vanwege de (potentiële) impact van een digitaal incident kan sprake zijn van gevolgen voor de fysieke veiligheid en openbare orde.
- Het NCC informeert bij grootschalige (dreigende) crises de betrokken veiligheidsregio('s) en/of het lokaal bevoegd gezag over het incident met mogelijke cascade- en gevolgeffecten, indien hier aanleiding toe is.
- Daarnaast kunnen incidenten met gevolgen voor de fysieke veiligheid en openbare orde direct gemeld worden bij de betrokken (hulp)diensten en/of regionale of lokale overheden, waaronder de veiligheidsregio.
- Informatie over een incident met (mogelijke) fysieke gevolgen binnen het regionaal of lokaal domein kan door de veiligheidsregio gecommuniceerd worden aan andere medeoverheden (gemeenten, provincies en waterschappen).
- Neem contact op met de meldkamer van de hulpdiensten. Indien uw organisatie behoort tot de overheid of vitale infrastructuur, contacteer direct de veiligheidsregio (NCTV, 2022: 30-31).

1.3.4 Inzet VR-ISAC

Het VR-ISAC is een netwerk waarin de Chief Information & Security Officers (CISO's) van de veiligheidsregio's zitting hebben. Binnen dit netwerk wordt informatie over dreigingen voor de interne bedrijfsvoering van veiligheidsregio's gedeeld en handelingsperspectief gegeven. Tijdens de oefening heeft VR-ISAC via Signal meerdere handelingsperspectieven en updates verstrekt aan zijn leden en telefonisch contact gehad met de directeuren in het IAO. Enkele bevindingen die tijdens de oefening naar voren kwamen zijn:

- De gehanteerde BOB-structuur functioneert naar behoren.
- Er zijn geen duidelijke regels over het informeren van het VR-ISAC: dit is een persoonlijke afweging van individuele leden.
- Er zijn geen afspraken over de wijze van alarmering van het VR-ISAC.
- Het ontbreken van formele toegang tot LCMS.
- Het invullen van de Scenariokaart Cybercrisis is een goede manier voor beeldvorming en het inschatten van impact en ernst van de situatie.

8 Waarschijnlijk hebben vitale sectoren vooral afstemming gezocht met organisaties binnen hun functionele kolom – organisaties die zij nodig hadden voor het oplossen van interne cybersecurity- en continuïteitsproblemen.

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

1.4 Mogelijkheden versterken landelijke aanpak cybercrises

In de leersessie is de deelnemers gevraagd welke mogelijkheden zij zien om de landelijke aanpak van cybercrises te versterken. Hieronder staat een overzicht van de reacties.

- vergroten van de landelijke bekendheid van het stelsel
- vroegtijdig contact tussen Operationeel Leiders
- betere verbinding tussen de crisisteams van het Rijk en van de veiligheidsregio's
- vaker landelijke crises beoefenen; dit geldt voor alle thema's
- afspraken uit LCP-D concreet maken en scenario uitwerken
- integrale beeldvorming regionaal, bovenregionaal en landelijk
- duiding van maatschappelijke effecten
- scenariodenken op alle niveaus
- elkaars expertise via een gesprek (tabletop) beter leren kennen en begrijpen
- niet alleen technisch duiden door cyberexperts, maar ook de mogelijke gevolgen
- informatie van alle DCC's over de situatie betreffende de vitale infra in een landelijk beeld
- oefen de schakels tussen Rijk en regio
- VR-ISAC laten aansluiten bij CERT's van andere sectoren (banken, waterschappen et cetera).
- snelle duiding van de situatie: gaat het om een cyberincident of cyberaanval?
- blijf in gesprek en heb begrip
- landelijk handelingsperspectief formuleren
- landelijke doelen delen
- IAO, ICCB en MCCB tijdens de oefening voor veiligheidsregio's mee laten doen.

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

Inleiding

Overkoepelende bevindingen

Aanbevelingen

Bronnen

Bijlage 1 Voorbereiding

Bijlage 2 Oefendoelen

2. Aanbevelingen

We komen op grond van deze evaluatie tot enkele aanbevelingen. De aanbevelingen richten zich op de landelijke aanpak van cybercrises.

2.1 OL-call: leiderschap en regie

Een OL-call is een nuttig instrument voor gemeenschappelijke afstemming tussen veiligheidsregio's en voor beeld- en oordeelsvorming. Om in de toekomst effectief te kunnen zijn, moet zo'n gemeenschappelijk overleg strakker worden ingericht. Daarvoor zijn wat ons betreft nodig:

- senior voorzitterschap
- strategisch leiderschap: voor duiding, sensemaking en besluitvorming
- herkenbare vergaderregels, waaronder een duidelijke (BOB-)structuur en overlegagenda én een duidelijke 'wie-is-wie'.

Deze randvoorwaarden zijn echt essentieel, zeker bij bovenregionale crises waarbij meerdere veiligheidsregio's betrokken zijn.

Daarnaast kan dit overleg volgens ons worden gebruikt om deelnemers meer uitleg te geven over de werking van de landelijke crisisstructuur: wat speelt er op landelijk niveau, welke teams zijn er actief, welke sleutelbesluiten zijn genomen, wanneer kunnen bepaalde producten (zoals een landelijk operationeel beeld, een duiding van de situatie, scenario's) worden verwacht? Zo'n uitleg draagt in onze optiek bij aan meer gemeenschappelijke beeld- en begripsvorming, wat nodig is tijdens zo'n veelomvattende, hybride crisis.

2.2 Opbouw landelijk operationeel beeld

Verken hoe bij bovenregionale cybercrises een landelijk operationeel beeld kan worden opgebouwd, welke informatie daarbij behulpzaam is, wie die informatie kan aanleveren en van betekenis kan voorzien. Voer als LOCC zo'n verkenning uit samen met veiligheidsregio's, het VR-ISAC en NCTV/NCSC. Neem daarin de vraag mee hoe de impact van verstoringen binnen de vitale sectoren op de openbare orde en veiligheid in beeld wordt gebracht. Qua relevante data kan gedacht worden aan:

- impact van cyberdreigingen en verstoringen op de bedrijfsvoering van veiligheidsregio's
- maatschappelijke impact: effecten van cyberdreigingen en verstoringen op de openbare orde en veiligheid
- informatie over vitale sectoren: getroffen sectoren, ernst, duur en potentiële fysieke effecten van verstoringen.

De 'Continuïteitsmonitor VR & Vitaal' van het VR-ISAC kan daarbij als inspiratie dienen.

2.3 Planvorming voor landelijke (cyber) crises

In paragraaf 2.2.1 is opgemerkt dat specifieke afspraken en procedures in bestaande planvorming onvoldoende helder zijn. Daarbij gaat het onder meer over de deelname van de veiligheidsregio's aan het IAO en ICCB, de wijze van terugkoppeling uit het IAO naar veiligheidsregio's én de bestuurlijke informatievoorziening en afstemming. Ook zouden in het LCP-D de taken, rollen en informatielijnen van een VR-ISAC, SOC en CERT als onderdeel van de zogenaamde functionele keten binnen de cyberspecifieke crisisstructuur opgenomen kunnen worden, zo werd geopperd. Voer met betrokken partijen een verkenning uit naar deze lacunes in planvorming (idealiter ook in relatie tot andere crisistypen) en bekijk vervolgens of concrete afspraken nodig zijn voor invulling van die lacunes.

2.4 Opleiding: wegwijs in de landelijke structuur

Bezie waar bestaande opleidingen voor sleutelfiguren in crisisbeheersing, zoals informatiemanagers, operationeel leiders en communicatieadviseurs, aangevuld kunnen worden met kennis over de werking van de landelijke crisisstructuur (taken en rollen, procedures en processen). Op deze manier maak je sleutelfiguren wegwijs in de werking van de landelijke structuur. Neem daarin ook scenariodenken mee, als belangrijke vaardigheid van crisisleiders om te anticiperen op de middellange termijn.

2.5 Scenariodenken: anticiperen op de middellange termijn

Onderzoek de mogelijkheden om als veiligheidsregio's beter in te spelen op de middellange termijn: situaties waarin duidelijke triggers voor opschaling ontbreken, maar waarin je wel al preventief kunt nadenken over scenario's en mogelijke responsmaatregelen. Leer daarbij van elkaar, bijvoorbeeld ten aanzien van de inzet van planningsstaven of pre-ROT's. Qua activiteiten kan gedacht worden aan het opstellen van scenario's met sleutelbesluiten, omgevings- en netwerkanalyses. Bespreek met de NCTV hoe veiligheids-regio's kunnen bijdragen aan het landelijke scenarioteam (en hoe de daar opgestelde scenario's op regionaal niveau benut kunnen worden).

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

Bronnen

Bakker, M., Berger, E., Van der Varst, L., & Karacan, O. (2021). *Informatiemanagement in veiligheidsregio's. een onderzoek naar de ervaringen van informatiemanagers en operationeel leidinggevenden.* NIPV.

Draaiboek ISIDOOR IV (2023). Veiligheidsregio's, LOCC, VR-ISAC.

Domrose, J. & Van der Varst, L. (2021). *Evaluatie veiligheidsregio's ISIDOOR 2021.* NIPV.

Evaluatieformulieren veiligheidsregio's, LOCC en VR-ISAC.

NCTV (2022), Landelijk Crisisplan Digitaal.

NIPV- 26- landelijk beeld ISIDOOR IV (2023).

VR-ISAC, evaluatie ISIDOOR IV (TLP Amber), 30-11.2023.

Inleiding

Overkoepelende bevindingen

Aanbevelingen

Bronnen

Bijlage 1 Voorbereiding

Bijlage 2 Oefendoelen

Bijlage 1

Voorbereiding

Hieronder geven we een beeld van de wijze waarop de deelnemers zich hebben voorbereid op cybergevolgbestrijding, c.q. ISIDOOR-4.

Aanpak intern cyberincident

Veiligheidsregio's IJsselland, Rotterdam-Rijnmond en Haaglanden hebbenmet een intern cyberincident geoefend. In IJsselland richt een intern cybercrisisteam zich op de aanpak van de verstoring in de bedrijfsvoeringsprocessen, in Rotterdam-Rijnmond is dat het ICT-incidenten ResponseTeam (IRT) en in Haaglanden het kernteam crisisrespons. In dat kernteam hebben zitting: de directeur Bedrijfsvoering, het Hoofd I&A en Hoofd communicatie, de Functionaris Gegevensbescherming (FG), Coördinator Functioneel beheer, Contractmanager ICT en een ondersteuner.

Vanuit het VR-ISAC namen drie vertegenwoordigers deel aan de oefening. Zij vormden het kernteam, bestaande uit een voorzitter, vicevoorzitter en secretaris. De focus van het VR-ISAC lag op de interne continuïteit binnen de sector.

Crisisgevolgbestrijding

In de veiligheidsregio's IJsselland en Rotterdam-Rijnmond oefent naast het intern responsteam het vrijwel complete Regionaal Operationeel Team (ROT) mee. De ervaring van de ROT's verschilt, zowel binnen als tussen de regio's. Zo heeft het ROT in IJsselland al meerdere cyberoefeningen gedraaid, maar zijn niet alle potentiële ROT-deelnemers geoefend op cyber. In Rotterdam-Rijnmond is cyber beperkt geoefend, maar is juist veel ervaring opgedaan met de gevolgen van een uitval van meldkamersystemen, transportketens, zorginstellingen en telefonie.

In Noord-West 4 is geoefend met het interregionaal operationeel team NW4 (iROT). Veiligheidsregio Utrecht oefent met het operationeel kernteam (OKT), bestaande uit twee regionaal operationeel leiders, een coördinerend informatiemanager, communicatieadviseur en de CISO. Het operationeel kernteam is nog nieuw en er zijn nog geen cyber-incidenten geweest in de crisisorganisatie. Op de meldkamer oefenen twee Calamiteitencoördinatoren (CaCo's) mee.

Vanuit het LOCC oefende het Piketteam mee, bestaande uit drie piketfunctionarissen: Front Office (FO), Back Office (BO) en een lid van het Management Team (MT). De ervaring van het team met cybergevolgbestrijding is beperkt vanwege de afwezigheid van grootschalige cyber-incidenten waarbij er een rol voor het LOCC is.

Voorbereiding

Deelnemers hebben zich op verschillende manieren voorbereid op de oefening, waaronder kennisnemen van plannen en deelnemen aan Webinars die werden georganiseerd door het NCSC/NCTV. Vanuit het LOCC is deelgenomen aan trainingen van de Nationale Academie voor Crisisbeheersing (NAC), waaronder scenariodenken en IAO. Het VR-ISAC heeft met zijn leden in juni een crisisoefening georganiseerd en werksessies met de deelnemers belegd, waarin voorbereide plannen zijn doorgenomen.

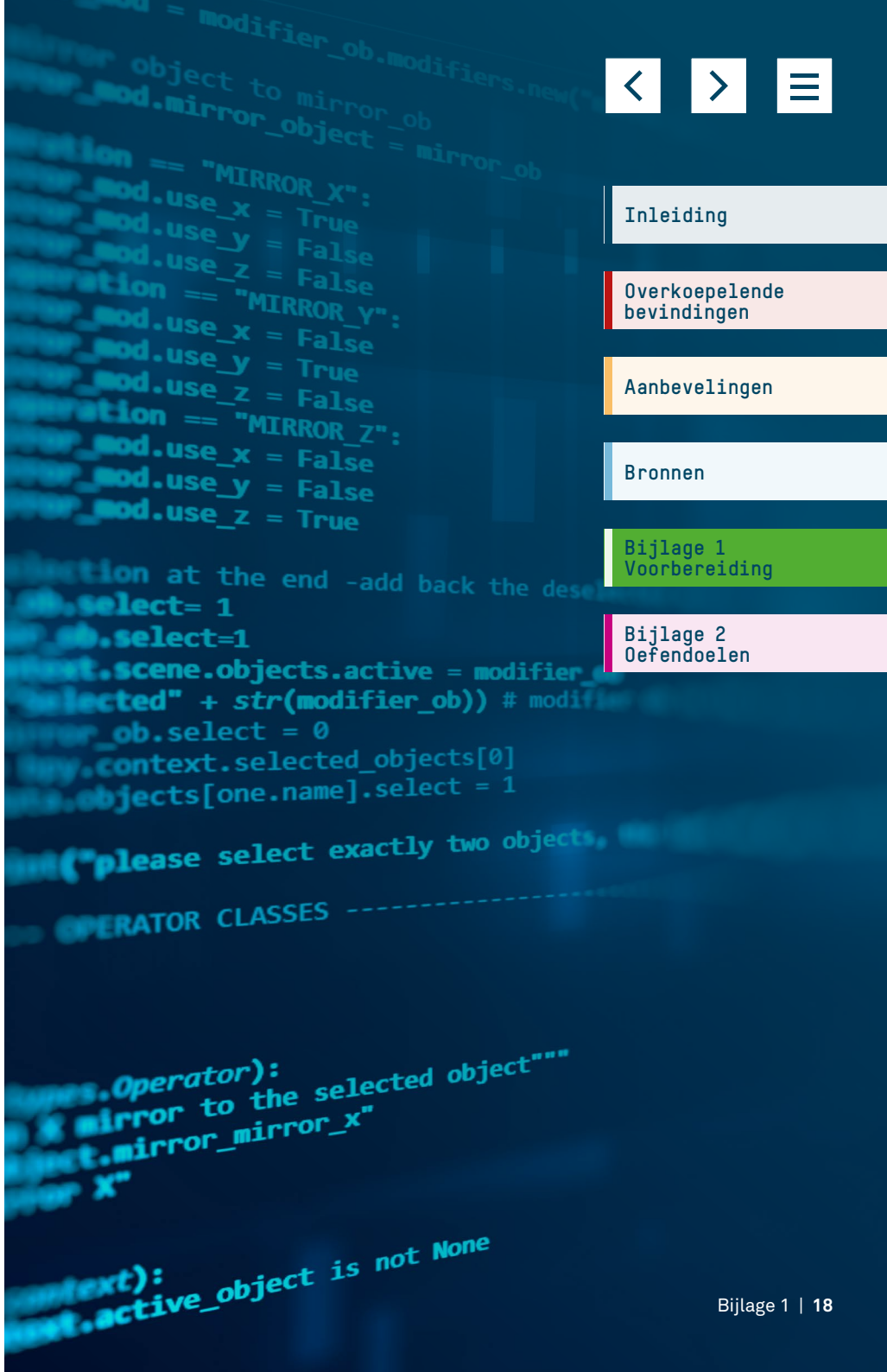
Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

Planvorming

Alle deelnemende organisaties beschikken over planvorming.

Naast het LCP-D gaat het onder meer om:

- Handboek cyberincidentrespons
- Multidisciplinaire scenariokaart cyber(gevolgbestrijding)
- Bestuurlijke Netwerkkaarten Crisisbeheersing, Netwerkkaart 21b: Cybersecurity
- Aandachtskaart Cybergevolgbestrijding & Netwerkanalyse Cybergevolgbestrijding
- Handleiding duiding van digitale verstoringen voor ROL
- Toolkit cyber.



Bijlage 2

Oefendoelen

Dit hoofdstuk bevat een beschrijving van de oefendoelen en de mate waarin deze doelen volgens de deelnemers zijn behaald.

Sectorale oefendoelen

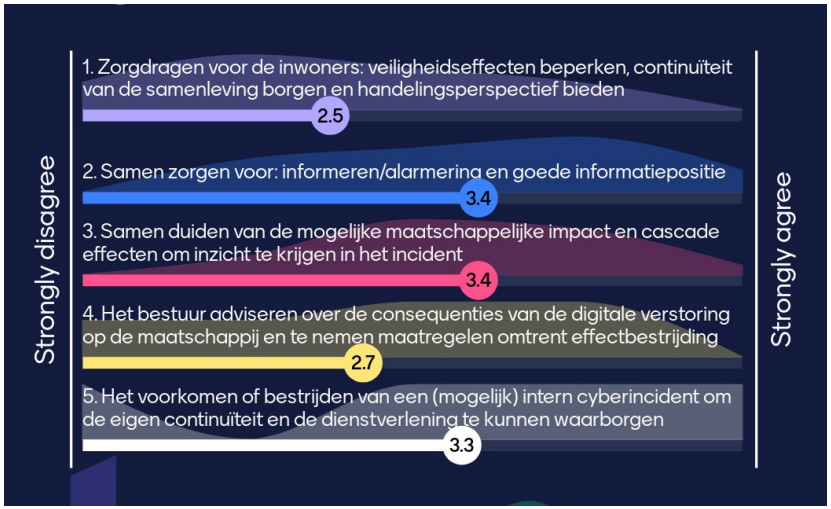
In het draaiboek ISIDOOR zijn vijf oefendoelen opgenomen.[9]

1. Handelingsperspectief: Zorgdragen voor de inwoners: veiligheids-effecten beperken, continuïteit van de samenleving borgen en handelingsperspectief bieden.
2. Informatie: Samen zorgen voor: informeren, alarmering en een goede informatiepositie.
3. Duiden impact: Samen duiden van de mogelijke maatschappelijke impact en cascade-effecten om inzicht te krijgen in het incident.
4. Bestuurlijk adviseren: Het bestuur adviseren over de consequenties van de digitale verstoring op de maatschappij en te nemen maatregelen omtrent effectbestrijding.
5. Bestrijden intern cyberincident: Het voorkomen of bestrijden van een (mogelijk) intern cyberincident om de eigen continuïteit en de dienstverlening te kunnen waarborgen.

Behalen oefendoelen

In de leersessie op 22 november 2023 is de deelnemers gevraagd te reflecteren op de sectorale oefendoelen en aan te geven in hoeverre de gestelde oefendoelen zijn behaald (op een range van 0-5). In het onderstaande overzicht staan de resultaten van die peiling.

Figuur B2.1 Peiling sectorale oefendoelen



Wat opvalt is dat oefendoel 2, 3 en 5 het hoogst scoren. Oefendoel 1 en 4 scoren in vergelijking relatief laag. Hiervoor zijn meerdere verklaringen, maar de belangrijkste om mee te geven is het feit dat de opzet van de oefening in mindere mate het oefenen van die oefendoelen (1 en 4) stimuleerde. Tijdens de eerste leersessie werden als grootste uitdaging van de oefening gezien: het verwerken van een adequate informatiepositie, het duiden en bieden van handelingsperspectief.

9 Draaiboek ISIDOOR IV 2023. Veiligheidsregio's, LOCC, VR-ISAC.

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen

In onderstaande tabel is voor alle oefendoelen uitgewerkt welke leerpunten naar voren zijn gekomen in de evaluatiesessie met de deelnemers.

Tabel B2.1 Leerpunten

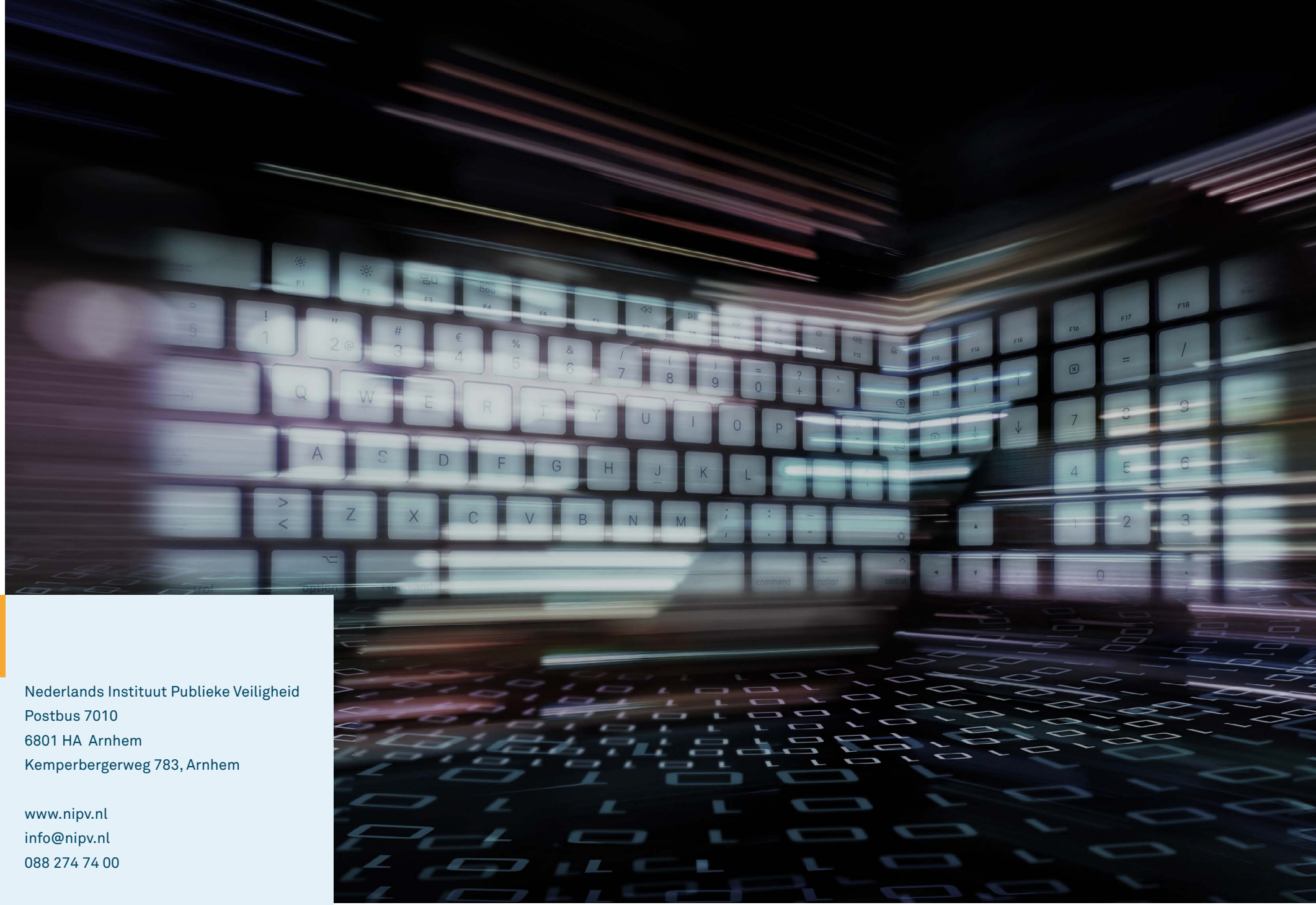
Oefendoelen	Belangrijkste leerpunten
Algemeen	› Kennismaking dynamiek landelijke crisis. Context en karakteristieken van cyberscenario. Er lopen veel lijnen naar redelijk onbekende gremia waar we niet dagelijks mee te maken hebben. › Rijk-Regio: knelpunten tussen het landelijke stelsel en de reguliere crisisorganisatie. De landelijke structuur is log en niet helpend geweest. › Verbinding tussen de functionele en de algemene kolom. › Collega's in het veld beter leren kennen; de rol van de veiligheidsregio's / het VR-ISAC was niet duidelijk voor verschillende partijen. › De oefening sloot op sommige punten niet voldoende aan op de regionale crisisstructuur, zodat enkele processen niet goed konden worden geoefend. › Een IROT is een onnodige tussenlaag tussen de veiligheidsregio en andere organisaties.
1. Zorgdragen voor de inwoners	› In een enkele regio kon dit oefendoel niet worden uitgevoerd, doordat er geen uitgevallen infrastructuur was. › Andere regio's worstelden met de vraag wie de communicatie moest doen, regionaal óf landelijk. Er werd getwijfeld over de vraag bij wie de verantwoordelijkheid ligt voor het delen van handelingsperspectieven in dit cyberscenario.
2. Informeren en alarmeren	› De landelijke beeldvorming duurde te lang. Er was lange tijd geen goed beeld van de vitale infrastructuur. › Informatiebehoeften waren niet altijd duidelijk. › Balans vinden tussen informatie gestuurd werken en vroegtijdig landelijk in verbinding komen. › De eerste OL-call verliep chaotisch en was onduidelijk en ongestructureerd. Ook werd teveel technische informatie gegeven, die niet aansluit bij de doelgroep: de operationeel leiders.
3. Duiden maatschappelijke impact	› Benutten van de nieuwe continuïteitsmonitor van het VR-ISAC. › Wie heeft die verantwoordelijkheid: regio of Rijk? › Wie brengt de impact op vitale sectoren in beeld?
4. Bestuurlijke advisering	› In de oefening was weinig sprake van bestuurlijke advisering. › De deelnemers misten in de OL-call de terugkoppeling van wat in het IAO besproken is.
5. Voorkomen of bestrijden intern incident	› Continuïteitsmanagement intern is noodzakelijk om extern de crisis te kunnen beheersen.

Mogelijkheden versterken regionale aanpak cybercrises

In de leersessie is de deelnemers gevraagd welke mogelijkheden zij zien om de regionale aanpak van cybercrises te versterken. Hieronder staat een (woordelijk) overzicht van de reacties.

- Gesprekken in tabletop vorm … elkaar begrijpen.
- Breng VR-ISAC beter in positie.
- Betere lijn naar VR-ISAC.
- Sterkere verbinding tussen intern team voor continuïteit en extern gericht ROT.
- Voor landelijke problemen die zich landelijk voordoen, landelijke handelingsperspectieven.
- Is voor bedrijven/organisaties helder dat bij Cyber een veiligheidsregio een belangrijke rol heeft?
- Scenariodenken.
- Basiskennis cyber en/of grenswerker tussen cyber en fysieke domein.
- Scenariodenken direct starten.
- Organiseer kleine oefeningen op de knelpunten uit de evaluatie. Pas eventueel LCP-D daarna aan.
- ICT aan tafel.
- Zorg dat theorie en praktijk overeen komen.
- OBV geleerde lessen het LCP-D en nationaal handboek crisisbesluitvorming opnieuw beoordelen.
- Aandacht voor forensische processen.
- Voor de crisis komen: bij reële dreiging al een landelijke OL-call met bijvoorbeeld NCC en scenario ontwikkelen of delen.
- Laat cybercrisis (nog meer) aansluiten bij de reguliere crisisorganisaties.
- Eerder beginnen met scenario's. Misschien standaard worst case scenario ontwikkelen.
- VR-ISAC aansluiten bij andere ISAC's (banken, waterschappen etc.).
- Het netwerk beter in beeld krijgen. Hoe lopen de lijnen in deze crisis.
- Meer oefenen.
- Vooraf in hoofdlijnen vaststellen 'commanders intent'.
- Duiding verbeteren en meerwaarde bieden op informatiegebied. Realisatie dat de wereld naast sectoren ook uit de regio bestaat.

Inleiding
Overkoepelende bevindingen
Aanbevelingen
Bronnen
Bijlage 1 Voorbereiding
Bijlage 2 Oefendoelen



Nederlands Instituut Publieke Veiligheid
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem

www.nipv.nl
info@nipv.nl
088 274 74 00