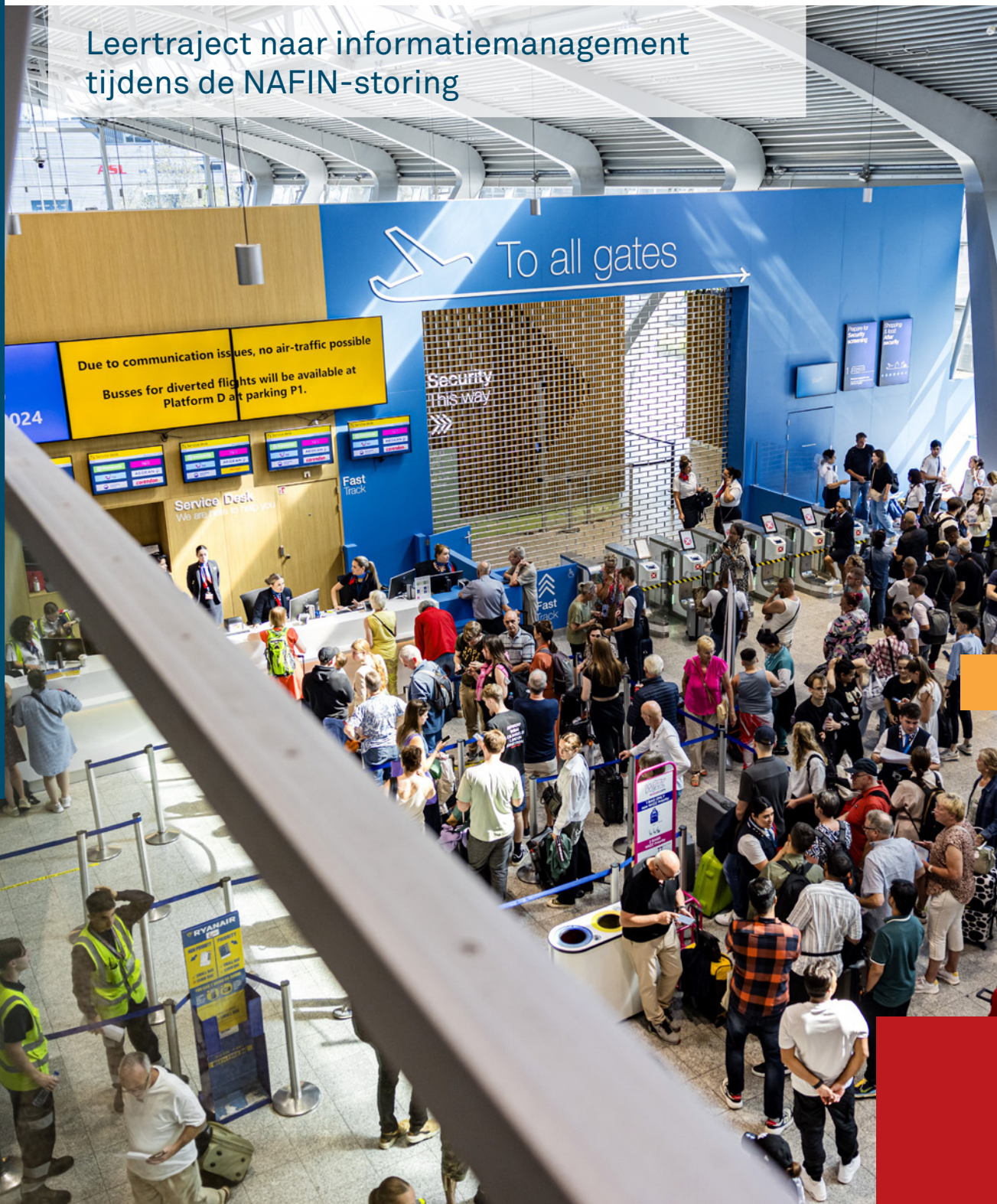


Leertraject NAFIN-storing

Leertraject naar informatiemanagement
tijdens de NAFIN-storing



Nederlandse Academie voor
Crisisbeheersing en Brandweezorg
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.nipv.nl
info@nipv.nl
026 355 24 00

Colofon

© Nederlands Instituut Publieke Veiligheid (NIPV), 2025

Auteurs	L. van der Varst, R. Terporten en T. Weimar
Contactpersoon	L. van der Varst
Opdrachtgever	Luc Dietz (LOCC/KCR2), Steven van de Looij (Coalitie Veiligheidsregio's) en Martijn Bekker (Coalitie Rijk)
Datum	4 april 2025
Foto cover	ANP

Wij hechten veel belang aan kennisdeling. Delen uit deze publicatie mogen dan ook worden overgenomen op voorwaarde van bronvermelding.

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

Inhoud

	Inleiding	4
1	Tijdslijn storing	7
1.1	Sleutelgebeurtenissen	7
1.2	Observaties van het verloop	8
2	Omgaan met dilemma's	11
2.1	Beschikbaarheid van informatie	11
2.2	Organiseren van de respons	13
2.3	Samenhang van de dilemma's	14
3	Bevindingen en aanbevelingen	15
3.1	Bevindingen	15
3.2	Aanbevelingen	16
3.3	Twee reflecties	18
	Bijlage 1: Leermethodiek	20
	Bijlage 2: Bronnen	22

Inleiding

Aanleiding

Op 27 augustus 2024 werd Nederland geraakt door een storing van het Netherlands Armed Forces Integrated Network (NAFIN). Dit glasvezelnetwerk van Defensie staat los van het internet en wordt onder meer gebruikt voor bedrijfsvoering van Defensie. De storing had impact op tal van plekken in Nederland:

- > Door de storing werden ook de P2000- en C2000-systemen geraakt, waardoor de communicatielijnen van kustwacht, marechaussee, meldkamers en politie werden beperkt. Meldkamers hadden problemen met het alarmeren, en communicatie tussen hulpdiensten op straat liep niet soepel.
- > Er waren meer dan negen uur lang geen inkomende of uitgaande vluchten meer mogelijk vanuit Vliegbasis Eindhoven.
- > Op meerdere plekken in het land konden overheidstaken niet meer worden uitgevoerd, zoals het verstrekken van passen of het gebruik van DigiD.

Uitval van een netwerk waarvan meerdere overheidsorganisaties gebruikmaken, hindert de overheid in haar functioneren. Hierdoor kan de nationale veiligheid in geding komen, zoals de Algemene Rekenkamer (2024) opmerkt.

Het is niet de eerste keer dat Nederland te maken had met een storing van een communicatienetwerk. Zo leidde in 2019 de landelijke KPN-storing tot uitval van noodnummer 112 en leidde in 2024 een software-update bij cybersecuritybedrijf CrowdStrike tot het vastlopen van IT-systemen. De NCTV waarschuwt in zijn *Cyber Security Beeld Nederland* al langer dat we rekening moeten houden met vaker voorkomende storingen. In de *Toekomstverkenning Crisisbeheersing* (Van der Varst et al., 2022) worden cyberstoringen als een prominent risicotype benoemd. Cyberstoringen zijn van grote invloed, omdat ze kunnen leiden tot maatschappelijke ontwrichting door kritische infrastructuren en/of communicatielijnen te verstoren (NCTV & NCSC, 2022). In het licht van hybride dreigingen en pleidooien voor meer weerbaarheid, is leren van dergelijke storingen zoals NAFIN van uitermate groot belang.

Wat is het NAFIN?

Het Netherlands Armed Forces Integrated Network (NAFIN) is een separaat glasvezelnetwerk dat door heel Nederland ligt. Hoewel het netwerk van origine uitsluitend voor militair gebruik bedoeld was, werd al vanaf de oprichting door de staatssecretaris van Defensie toegezegd dat mogelijkheden tot het aansluiten van andere gebruikers onderzocht werd (Algemene Rekenkamer, 2024). Inmiddels is een scala van partijen en systemen aangesloten op het netwerk, waaronder departementen, de Eerste en Tweede Kamer en de meldkamers. In een analyse naar de kracht en de kwetsbaarheid van het NAFIN-netwerk stelt de Algemene Rekenkamer dat het aantal aangesloten systemen groot is, en dat er géén duidelijk zicht is op welke gebruiker of dienst geraakt wordt bij uitval van (een gedeelte van) het netwerk (Algemene Rekenkamer, 2024).

De Rekenkamer merkt op dat hoewel NAFIN door Defensie niet formeel is aangewezen als vitaal netwerk, het functioneren van het netwerk wel randvoorwaardelijk is voor andere processen met het stempel 'vitaal', waaronder de inzet van Defensie en politie, het functioneren van de 112 meldkamers en de informatievoorziening vanuit de overheid. Een storing van NAFIN brengt de continuïteit van deze processen in gevaar.

Opdracht

In opdracht van de zogeheten 'Coalitie Rijk', Coalitie 'Veiligheidsregio's' en het Landelijk Operationeel Coördinatie Centrum (LOCC) / Knooppunt Coördinatie Regio's-Rijk (KCR2) heeft het lectoraat Crisisbeheersing (NIPV) een leertraject begeleid over de NAFIN-storing. Hierbij lag de focus op het informatiemanagement voor gemeenschappelijke beeldvorming van de storing in de eerste 24 uur. Doel van het leertraject was het:

Identificeren van goede praktijken en verbeterpunten ten aanzien van het informatiemanagement in de eerste 24 uur van de NAFIN-storing, teneinde de preparatie op vergelijkbare storingen te versterken.

Informatie is een belangrijk onderdeel van crisisbesluitvorming. Goede, gevalideerde informatie geeft crisisbeheersers zicht op de gevaarsetting, op de effecten en op de ontwikkeling van incidenten en crises. Vanuit dat beeld kunnen crisisteams een inschatting van de situatie maken, bepalen welke partijen bij de respons te betrekken en welke maatregelen nodig zijn (Bakker et al., 2021). Het *Handboek informatiemanagement* (Netwerk Netcentrisch Werken, 2022) noemt als kern van informatiemanagement het verzamelen, analyseren, filteren en doorgeleiden van de informatie die relevant is voor de operationele crisisbeheersing. Informatiemanagement ondersteunt crisisprocessen als alarmering, opschaling en leiding en coördinatie. Onder informatiemanagement verstaan we in dit onderzoek: het verzamelen, analyseren en beschikbaar stellen van informatie aan relevante actoren ten behoeve van onderlinge coördinatie en besluitvorming over responsmaatregelen.

Aanpak

Het leertraject is in vier stappen uitgevoerd.

Stap 1: Tijdlijn (Wat is er gebeurd?)

De gebeurtenissen tijdens de storing vanaf 27 augustus 0.00 u t/m 28 augustus 0.00 u zijn op een tijdlijn gezet. Informatie over de gebeurtenissen is gebaseerd op het Landelijk Crisis Management Systeem (LCMS) en later aangevuld met informatie uit interviews en leertafel.

Stap 2: Interviews (Wat zijn dilemma's, goede praktijken en verbeterpunten?)

Vervolgens zijn semigestructureerde interviews afgenomen met respondenten van betrokken partijen. Doel van de interviews was het identificeren van kerndilemma's, van goede praktijken en verbeterpunten. Deze dilemma's zijn vervolgens in de leertafel (zie onder) besproken. Een dilemma is een netelig of duivels probleem; een probleem waarop géén

eenvoudig of optimaal antwoord is; aan mogelijke antwoorden kleven onherroepelijk voor- én nadelen. Er zijn door twee onderzoekers in totaal zeven interviews afgenomen.¹

Stap 3: Leertafel (Wat zijn overkoepelende goede praktijken en quick actions?)

Op 10 december hebben we een leertafel georganiseerd met vertegenwoordigers van betrokken organisaties.² De leertafel had als doel om gezamenlijk met de betrokken partijen van het incident de belangrijkste lessen en goede praktijken te identificeren en concrete, snel omzetbare actielijnen – de quick actions – te bespreken. De leertafel werd gemodereerd door de onderzoekers van het NIPV en duurde in totaal 3 uur. In de leertafel stonden twee dilemma's centraal: beschikbaarheid van informatie en organiseren van de respons.

Stap 4: Rapportage

Op basis van de onderzoeksactiviteiten is een rapportage opgesteld. De rapportage is besproken met de opdrachtgever voor een controle op feitelijkheden en realiseerbaarheid van de aanbevelingen. De rapportage vormt de basis voor verdere kennisdeling.

Leeswijzer

In hoofdstuk 1 beschrijven we de tijdlijn met sleutelgebeurtenissen mét observaties en percepties van het incident. In hoofdstuk 2 staan de twee bovengenoemde onderwerpen centraal: beschikbaarheid van informatie en organiseren van de respons. We beschrijven beide thema's, inclusief oorzaken en anticiperende strategieën. We sluiten het hoofdstuk af met strategieën die door organisaties tijdens de NAFIN-storing werden toegepast. In hoofdstuk 3 presenteren we onze bevindingen en aanbevelingen. Bijlage 1 bevat de leermethodiek. Bijlage 2 bevat de geraadpleegde bronnen.

¹ Respondenten interviews: Defensie, LOCC/KCR2, Koninklijke Marechaussee, NCC, Veiligheidsregio Amsterdam-Amstelland, Veiligheidsregio Gelderland-Midden, Veiligheidsregio Zuid-Holland Zuid.

² Deelnemers leertafel: Defensie, LOCC/KCR2, Koninklijke Marechaussee, Kustwacht, NCC, LMS, Veiligheidsregio Amsterdam-Amstelland.

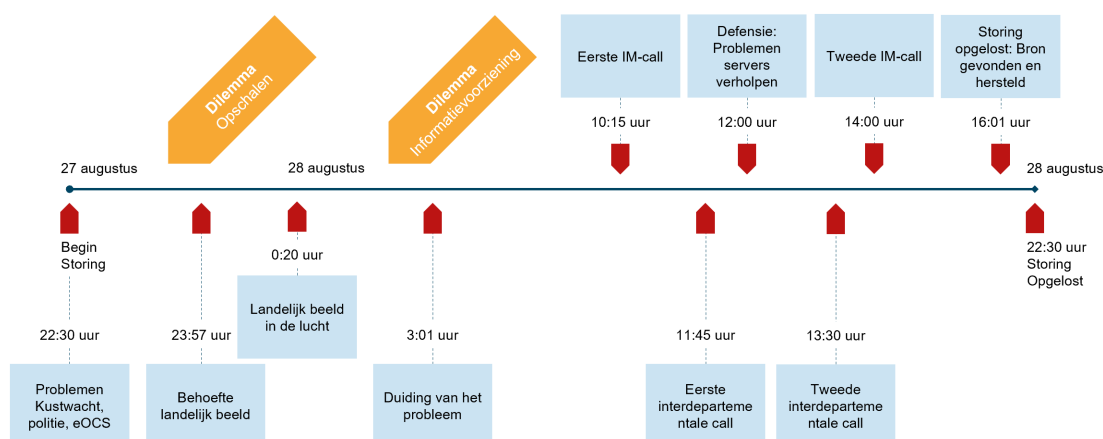
1 Tijdlijn storing

1.1 Sleutelgebeurtenissen

Om het verloop van het incident goed in kaart te brengen, is er een tijdlijn aangemaakt gebaseerd op de eerste 24 uur van het incident, beginnend op 27 augustus om 22.30 uur en lopend tot en met 28 augustus 22.30 uur. Gebaseerd op informatie uit de interviews, de leertafel en nieuwsmedia zoals NOS, hebben wij 58 tijdsmomenten opgenomen, waarvan we tien momenten identificeren als sleutelmomenten. Dit zijn gebeurtenissen in het verloop van het incident die door de deelnemers van de leertafel en door het onderzoeksteam beschouwd worden als van grote invloed op het verdere verloop van de storing (zie figuur 1.1). De NAFIN-storing ontplooidde zich als volgt:

1. **Begin storing:** Op 27 augustus om 22.30 uur worden problemen gemeld met het alarmerings- en communicatiesysteem van de hulpdiensten (P2000 en C2000); ook de kustwacht meldt problemen. Meldkamers hebben problemen met het alarmeren, en communicatie tussen hulpdiensten op straat loopt ook niet soepel.
2. **Behoeftelandelijk beeld:** Om 23.57 uur vraagt de dienstdoende informatiemanager ROT van Veiligheidsregio Amsterdam-Amstelland het LOCC om een landelijk beeld aan te maken.
3. **Landelijk beeld in de lucht:** Net na middernacht op 28 augustus om 0.20 uur is het eerste landelijk beeld in het LCMS aangemaakt om de situatie in kaart te brengen.
4. **Duiding van het probleem:** Om 3.01 uur is Defensie toegevoegd aan het landelijk beeld en wacht het MMC op vervolcontact met een medewerker van de Defensie Materieel Organisatie (DMO). Vanaf 7.00 uur vetrekken de eerste vluchten niet meer vanuit Eindhoven Airport.
5. **Eerste IM-call:** Om 10.15 uur vindt de eerste IM-call plaats met vertegenwoordigers van regionale en nationale crisisorganisaties om samen een beeld te vormen van de gevolgen van de storing.
6. **Eerste interdepartementale call:** Om 11.45 uur wordt een interdepartementale call georganiseerd door het Nationaal Crisiscentrum (NCC). Hoewel duidelijk is dat Defensie probleemeigenaar van de storing is en het niet gaat om een cyberaanval, dringt informatie over de specifieke oorzaak en de scope van de storing nog niet naar buiten.
7. **Oorzaak problemen verholpen:** Kort daarop, om 12.00 uur, geeft Defensie aan dat de problemen verholpen zijn en dat de servers weer in de lucht komen. Inderdaad zijn de problemen inmiddels ook op andere plekken weer verholpen, zoals bij DigiD, de Koninklijke Marechaussee (KMAR) en de politie.
8. **Tweede interdepartementale call:** Om 13.30 uur is een tweede interdepartementale call door het NCC georganiseerd.
9. **Tweede IM-call:** In een laatste IM-call om 14.00 uur wordt bevestigd dat het probleem opgelost is en dat de eerste veiligheidsregio's op de meldkamer weer terug kunnen naar de normale werkwijze.
10. **Storing opgelost:** Om 16.01 uur meldt Defensie officieel dat de bron van de storing is gevonden en inmiddels is hersteld. Ook de vluchten vanuit luchthaven Eindhoven zijn inmiddels weer hervat en de kustwacht is weer bereikbaar. Om 22.30 uur op 28

augustus zijn de meeste systemen weer in de lucht en lijkt de storing van het NAFIN-netwerk verholpen.



Figuur 1.1 Tijdlijn storing

1.2 Observaties van het verloop

We geven in deze paragraaf een duiding van de storing, gevolgd door enkele opmerkingen over het verloop van de storing en het informatiemanagement op basis van de interviews, leertafel en opgestelde tijdlijn.

Lastig, maar niet ontwrichtend. In eerste instantie werd de NAFIN-storing door de veiligheidsregio's ervaren als een 'normale' storing. De EOCS-server had, zo geven meerdere respondenten aan, wel vaker kortdurende problemen. Dit gepaard met het feit dat meldkamers terugvalopties hebben als er alarmeringsproblemen zijn, gaf het betrokkenen niet direct de impressie dat dit een storing met grote impact was. Het sentiment gedurende de nacht is dan ook dat het geen grote storing betrof. Zo zegt de piketfunctionaris van het LOCC: "Ons beeld was, het is lastig, maar niet maatschappij-ontwrichtend".

Ongrijpbaar incident; versnipperde informatie. Vrijwel alle respondenten geven aan dat een ICT-incident van nature wat ongrijpbaar en weinig tastbaar is voor een traditionele crisisorganisatie. Het is geen 'pats-boem-incident' met rook, zichtbare schade en slachtoffers. Eerder is sprake van een storing die op meerdere plekken (en verschillende tijdstippen) in het netwerk tot problemen leidt en waarvoor de oorzaak onduidelijk is. Veiligheidsregio's geven aan vooral een vinger aan de pols te hebben gehouden om de eigen processen te waarborgen, en op te kunnen treden bij verdere escalatie. Een operationeel leider van de VRAA omschrijft het zo: "Het was voor ons een feitelijk overzichtelijke casus, maar een casus die heel lang duurt en waarvan de informatievoorziening erg traag was". De lange duur en trage informatievoorziening droegen bij aan het feit dat men ook in de loop van de ochtend op 28 augustus nog steeds moeite had om de impact van het incident in te schatten. Het gevaar dat een aantal respondenten hier ziet is dat men te afwachtend wordt, waardoor kostbare tijd verloren gaat.

Een complicerende factor was het ontstaan van problemen laat op de avond en de verdere ontwikkelingen gedurende de nacht. Een organisatie zoals LOCC/KCR2 heeft weliswaar een nachtpiket (en is daardoor bereikbaar), maar draait niet 24/7 op volle bezetting. Ook

Defensie draait niet op volle kracht gedurende de nacht, waardoor het voor partijen lastig was Defensie te bereiken. Hierdoor was het moeilijk de impact van de storing in beeld te brengen, zo geven piketfunctionarissen van het LOCC en de informatiemanager van VRAA aan.

Observatie

We zien op 28 augustus een langere periode, tussen ongeveer 3.00 en 07.30 uur, waarin in LCMS weinig informatie wordt gedeeld en er vindt weinig formele coördinatie plaatsvindt.

Terwijl aan het begin van de storing de nodige acties zijn uitgevoerd, zoals te zien is in de tijdlijn, neemt het aantal 'geregistreerde acties' na 3.00 uur af: er wordt weinig informatie in LCMS gedeeld en er is weinig formele coördinatie. Het LOCC wordt gealarmeerd door meldkamer Amsterdam, die langer problemen ondervond dan andere meldkamers, omdat zij niet aangesloten is op de Landelijke Meldkamer Samenwerking (LMS). Hierom volgt aan het begin het telefonisch contact tussen de informatiemanager van Amsterdam-Amstelland met de piketmedewerkers van het LOCC; ook wordt een landelijk beeld in LCMS aangemaakt. Door partijen afzonderlijk worden acties ondernomen om geconstateerde problemen te verhelpen, onder meer door LMS en door het Joint Informatievoorziening Commando (JIVC) van Defensie. Maar die acties vinden vooral binnen de eigen organisatie plaats. Er is nog geen sprake van een gecoördineerde respons; het volle zicht op de effecten van de storing ontbreekt. Een mogelijke verklaring vormt het dilemma rond de beschikbaarheid van informatie (zie verder hoofdstuk 3). Hierdoor hebben partijen niet eenzelfde probleem- en urgentiebesef, wat een barrière vormt voor het organiseren van de respons (dilemma 2).

Bredere impact; uitdaging organiseren respons. Pas bij het opstarten van de dag op 28 augustus wordt duidelijk dat de problemen breder spelen. In de ochtend blijken niet alleen de meldkamers, Defensie en de Kustwacht getroffen, maar ook de Haagse ring en Vliegbasis Eindhoven. Ministeries kunnen geen e-mails versturen, de 088-lijnen zijn niet beschikbaar, en in de loop van de ochtend ontstaan problemen bij gemeenten en de Douane. Meerdere respondenten vroegen zich af of er vanuit de beheerder van het NAFIN-netwerk (lees: JIVC van Defensie) wel genoeg zicht was op waar de technische problemen op doorwerkten en welke effecten optraden. Een operationeel leider van VGGM vat zijn ervaring samen door te stellen: "Rond 11:00 uur [...] dacht ik, dit gaat helemaal niet lekker. Er zijn allemaal effecten die ik vanuit mijn positie niet kan verklaren".

Observatie

We constateren a) dat organisaties gedurende de eerste 12 uur een ander informatiebeeld van de storing hebben en b) dat het volle zicht op de effecten van de storing ontbreekt.

Betrokken partijen hebben elk een ander beeld van de storing. Dat beeld wordt in belangrijke mate ingegeven door problemen waarmee de desbetreffende partijen te kampen hebben. Zo geeft de Kustwacht aan vanaf het begin van de storing "blind, doof en stom" te zijn geweest; met andere woorden: verstoken te zijn van alle communicatiemiddelen. Veiligheidsregio Amsterdam-Amstelland heeft op de avond van de 27e al een beeld van wat er aan de hand is, waarna ze opschaalt naar GRIP-1. De Koninklijke Marechaussee meldt om 5.36 uur officieel een storing, terwijl Veiligheids- en Gezondheidsregio Gelderland-Midden pas de volgende ochtend op de hoogte raakt van de situatie. Een beter geïntegreerd beeld van de

storing komt die eerste uren niet tot stand. Een mogelijke verklaring is het dilemma van beschikbaarheid van informatie (zie verder hoofdstuk 3). Zoals eerder opgemerkt, ontbreekt bij partijen het volle zicht op de effecten van de storing. De verschillen in impact zorgen ervoor dat niet meteen een gezamenlijk probleem- en urgentiebesef bestaat – een situatie die de vorming van een geïntegreerde respons belemmert.

Observatie

We zien op 28 augustus vanaf 8.30 uur meer formele coördinatie en gezamenlijke beeldvorming ontstaan.

Zoals hierboven beschreven, is het voor betrokken partijen vanaf de eerste melding van problemen tot het ontstaan van meer formele coördinatie in de eerste IM-call 'ieder voor zich'.³ Partijen zijn vooral binnen hun eigen organisatie bezig met het oplossen van geconstateerde problemen, ieder vanuit haar eigen situatiebeeld. Dat hindert het organiseren van de respons (dilemma 2, zie hoofdstuk 3). Een extra complicatie was daarbij de verstoring van standaard communicatielijnen, waardoor het moeilijk was om sleutelpersonen te bereiken. Het piket van het LOCC heeft in de nacht geprobeerd contact te krijgen met LMS en NCC over deze storing, maar er kwam geen duidelijke reactie. Doordat de storing in de nacht plaatsvond, was er weinig personele capaciteit voor consultatie, afstemming en inwinnen van inlichtingen. Dit verandert pas in de ochtend. Dan nemen partijen zoals het LOCC en NCC initiatief tot coördinatie middels calls. Die wijze van coördineren wordt breed gezien als een goede praktijk, hoewel sommige betrokkenen opmerken dat de coördinatie laat tot stand komt. Uit de interviews met het NCC blijkt een afwachtende houding. Er wordt ook aangegeven dat het achteraf gezien professioneel zou zijn geweest om kernpartijen eerder bij elkaar te roepen, alleen was het op het moment zelf onvoldoende duidelijk wat er aan de hand was. Pas in de ochtend ontstaat, onder meer door de informatie van partijen te bundelen in de calls en in LCMS, beter zicht op de effecten van de storing.

Observatie

We constateren dat de informatie die door Defensie wordt verstrekt in de departementale calls van 11.45 uur en 13.30 uur de onzekerheid over de storing vermindert.

Voor crisismanagement is een goede informatiepositie cruciaal. Op basis van informatie worden maatregelen getroffen, wordt bepaald welke partijen bij crisisoverleg te betrekken en kan geanticipeerd worden op middellange termijn gevolgen. Daarbij helpt het als een expert of gezaghebbend instituut de ontstane situatie van duiding kan voorzien: wat speelt er, waarmee hebben we te maken?

Tijdens de NAFIN-storing is langere tijd onduidelijk waar de oorzaak van de storing ligt, of het probleem kan worden verholpen, wanneer en door wie. Indien dergelijke informatie ontbreekt, is het voor betrokken partijen navigeren in de mist. Dat het hoofd Nationale Operaties van Defensie aansluit in de interdepartementale calls en meer informatie verstrekt over de storing is cruciaal. De vragen van partijen in het informatiemanagement over de storing kunnen op dat moment worden beantwoord. Dat geeft rust en vermindert de onzekerheid over het verdere verloop van het incident.

³ In de periode 27 augustus om 22.30 uur tot 28 augustus om 10.15 uur.

2 Omgaan met dilemma's

In het leertraject stonden twee dilemma's centraal: beschikbaarheid van informatie en organiseren van de respons. In elke crisis doen zich dilemma's voor. Zoals eerder opgemerkt beschouwen we een dilemma als een netelig probleem; een probleem waarop géén eenvoudig of optimaal antwoord is; aan mogelijke antwoorden kleven onherroepelijk voor- én nadelen.

Leren omgaan met dilemma's is een cruciale vaardigheid voor crisismanagers. We beschrijven hieronder beide dilemma's, inclusief mogelijke oorzaken en anticiperende strategieën om ermee om te gaan. We sluiten elke paragraaf af met een korte duiding van de strategieën die door de organisaties tijdens de NAFIN-storing zijn toegepast.

2.1 Beschikbaarheid van informatie

2.1.1 Oorzaken en anticiperende strategieën

"Making sense in (and of) crises is a daunting task (...) The high degree of uncertainty that characterises such situations creates a typical dilemma: act on the basis of imperfect, incomplete, inconclusive and partially digested information or risk missing fleeting windows of opportunity to affect a fast-moving course of events" (Boin et al., 2016; Dearstyne, 2007; OECD, 2015).

Een terugkerend dilemma in crisismanagement gaat over de beschikbaarheid van informatie. Die informatie (over oorzaken, omvang, duur, ernst en impact) is van belang om de crisisrespons te coördineren en te organiseren, maar is schaars, zeker in de eerste uren van een incident.⁴ De beperkte beschikbaarheid van informatie kan **verschillende oorzaken** hebben:

- > Er is simpelweg (nog) geen informatie.
- > Er is informatie, maar deze informatie is niet beschikbaar, doordat de betreffende partner geen onderdeel uitmaakt van het responsnetwerk.
- > Er wordt nog geen aanleiding gezien om informatie breder te delen, bijvoorbeeld vanwege het label dat aan de storing wordt toegekend (een incident komt niet over een bepaalde drempelwaarde) of doordat de aandacht zich concentreert op het oplossen van het probleem.
- > Er is informatie, maar organisaties zijn om verschillende redenen niet bereid of in staat om informatie te delen. Bijvoorbeeld vanuit concurrentieoverwegingen, vanwege wettelijke verplichtingen of interne validatieprocedures.
- > Er is geen gevalideerde informatie, waardoor onduidelijk is hoe betrouwbaar de beschikbare informatie is.
- > De probleemeigenaar die beschikt over gevalideerde informatie en de situatie gezaghebbend kan duiden zit niet aan tafel.

⁴ Naarmate een crisis vordert, kan juist ook sprake zijn van een overschot aan informatie.

- > De complexiteit van het probleem, waardoor vele verschillende partijen over informatiebrokken beschikken.

Uiteraard geldt in crisismanagement het 'adagium van Rutte': 100 % besluiten nemen op basis van 50 % informatie. Met andere woorden: je zult keuzes moeten maken ook als je niet over alle informatie beschikt. Niettemin is het raadzaam te zoeken naar meer informatie ter onderbouwing van besluiten. We onderscheiden in tabel 2.1 strategieën om te anticiperen op het dilemma. Aan elke strategie kleven voor- en nadelen. Zo kan 'afwachten' verspilling van tijd en middelen voorkomen, maar ook leiden tot tijdverlies en achter de feiten aanlopen.

Tabel 2.1 Anticiperende strategieën

Strategie	Beschrijving
1. Afwachten	Wachten tot meer informatie beschikbaar komt.
2. Informeel afstemmen binnen eigen team / organisatie	Raadplegen van directe collega's voor hulp en consultatie.
3. Omgeving scannen	Scannen van gebeurtenissen in de omgeving, bijvoorbeeld door sociale-media-analyses en raadplegen van online bronnen.
4. Actief zoeken buiten eigen organisatie	Zelf op zoek gaan naar informatie en (andersoortige) bronnen raadplegen; rondbellen; beroep doen op informele netwerken; experts raadplegen.
5. Escaleren	Bij een hoger (hiërarchisch) echelon aan de bel trekken met het verzoek om meer informatie en duiding. Verzameling (proces)informatie: <ul style="list-style-type: none"> > Bekendheid probleem en primaire en/ of secundaire betrokkenheid netwerk en partijen > Duiding probleemeigenaar > Identificatie onzekerheden en processtappen > Verkenning informatiebehoefte op verschillende niveaus.

2.1.2 Wijze van optreden in deze casus

Wat we zagen tijdens de NAFIN-storing is een combinatie van factoren die het beschikbaar komen van informatie bemoeilijken: zo is er eerste uren van de storing weinig informatie, kan Defensie beschikbare informatie nog niet delen en er is informatie bij de LMS, maar deze maakt geen onderdeel uit van het informatiemanagement responsnetwerk.

We zien in deze casus dat partijen meerdere strategieën toepassen: terughoudendheid betrachten (bij het LOCC), informeel afstemmen binnen de eigen organisatie (onder andere het LOCC), een beroep doen op informele netwerken (Marechaussee, LOCC) en actief zoeken naar informatie buiten de eigen organisatie (Veiligheidsregio Amsterdam-Amstelland). We zien ook dat strategieën zoals escaleren eigenlijk niet worden toegepast. Dat zou in toekomstige situaties het bestaande actierepertoire kunnen uitbreiden.

2.2 Organiseren van de respons

2.2.1 Oorzaken en anticiperende strategieën

"[...] organising the cooperative effort is almost as difficult as the problems they are created to address" (Kapucu et al., 2010).

Een tweede terugkerend dilemma in crisismanagement gaat over het organiseren van de respons (Treurniet, 2022). Gebrekkige organisatie draagt ertoe bij dat de crisisrespons minder efficiënt en effectief verloopt, waardoor meer schade en hogere kosten ontstaan, en maatschappelijke onrust kan toenemen. Het dilemma van 'het organiseren van de respons' kan verschillende oorzaken hebben:

- > Tijd: er is simpelweg te weinig tijd om de respons adequaat te organiseren (met name bij kortdurende crises of flitsincidenten).
- > De aard van het scenario: organisaties zijn niet of onvoldoende voorbereid op nieuwe en uitzonderlijke crises. Procedures, planvorming en training ontbreken. Taken, rollen en verantwoordelijkheden zijn niet helder.
- > Omvang en complexiteit van het scenario: bijvoorbeeld een grootschalige natuurramp of pandemie, waardoor taken en verantwoordelijkheden van betrokken partijen diffuus zijn en onduidelijk is wie de regie neemt.

Geen crisis laat zich vooraf beschrijven. Crisismanagement blijft het vinden van een balans tussen structuur en improvisatie. Niettemin is het raadzaam te zoeken naar mogelijkheden om de crisisrespons tijdig, efficiënt en doeltreffend te organiseren. We noemen in tabel 2.2 strategieën om te anticiperen op het dilemma.

Tabel 2.2 Anticiperende strategieën in de acute respons

Strategie	Beschrijving
1. Terugvallen op routines (acute fase)	Volgen van bestaande procedures, zoals beschreven in handboeken en plannen (voor andersoortige incidenten).
2. Focus op bronbestrijding	Aandacht en inspanningen richten op het technisch oplossen van het probleem, of bronbestrijding; weinig oog voor de effecten van de verstoring.
3. Focus op impact / scenario's	In plaats van bronbestrijding de aandacht richten op de maatschappelijke gevolgen van een storing en/of het uitwerken van scenario's.
4. Improviseren / regie nemen (acute fase)	Initiatief nemen om zelf de crisisrespons te organiseren; improvisatie centraal stellen: doen wat gezien de situatie nodig en wenselijk lijkt.
5. Preparatief professioneel organiseren (acute fase)	Geen formele opschaling, maar wel als crisisteam en crisisorganisaties bij elkaar komen voor uitwisseling van informatie, inschatting van de situatie en vereiste acties (denk aan: planningsstaf) voor juiste focus op organiseren en/of coördineren.

2.2.2 Wijze van optreden in deze casus

Wat we in de NAFIN-storing constateren is (wederom) een combinatie van factoren die de respons bemoeilijken. Het kost tijd om de respons adequaat te organiseren, mede door het plaatsvinden van de storing buiten reguliere kantoor tijden en door de aard van het scenario, waarop minder planvorming en preparatie heeft plaatsgevonden

We zien in deze casus dat betrokken partijen meerdere strategieën toepassen. Zo neemt Amsterdam-Amstelland het initiatief om het LOCC te benaderen voor een landelijk beeld (strategie 2), richt Defensie zich op bronbestrijding (strategie 2) en vallen organisaties als LOCC, Defensie en veiligheidsregio's in hoofdzaak terug op bestaande routines (strategie 1). We zien ook dat sommige strategieën niet of weinig worden toegepast, met name de focus op impactmanagement en het uitwerken van scenario's. Dat vormt een aanknopingspunt voor verbetering van de respons. Tevens is strategie 5 lastig, zodra er een 'nationale dimensie' gaat spelen; laagdrempelige afstemming is lastiger met zwaardere departementale betrokkenheid.

2.3 Samenhang van de dilemma's

De impact van de dilemma's rondom informatievoorziening en respons is nauw verweven. Door gebrekkige of juist ontbrekende informatievoorziening kan een adequate respons worden belemmerd. Immers, als het voor crisisprofessionals van begin af aan duidelijk was wat de oorzaak, impact en duur van de storing waren, dan was men waarschijnlijk veel sneller overgeschakeld naar het organiseren van een call met alle betrokken partijen aan boord. Tegelijkertijd heeft de manier waarop wordt omgegaan met het organiseren van een respons invloed op het verschaffen van cruciale informatie. Alleen door het organiseren en samenwerken van de betrokken partijen kan een transparante uitwisseling van informatie plaatsvinden. Door aan een goede preparatie en kennisopbouw te werken, raken betrokken partijen beter ingespeeld op dit soort storingen. Een aangepaste attitude en professionaliteit, net zoals procesverbeteringen zouden tijdens de acute fase van een storing kunnen helpen.

3 Bevindingen en aanbevelingen

Op 27 augustus 2024 wordt Nederland geraakt door een storing van het NAFIN-netwerk. De storing heeft onder andere impact op communicatiesystemen van Kustwacht, marechaussee, meldkamers en politie. Het duurt bijna 24 uur voordat de storing is opgelost. In dit leertraject hebben we het informatiemanagement vanuit KCR2 tijdens deze storing bestudeerd. In dit hoofdstuk presenteren we onze bevindingen en aanbevelingen.

3.1 Bevindingen

1. **De NAFIN-storing was een storing die niet beperkt bleef tot één sector, maar effecten had op tal van plekken.** De partijen in het informatiemanagement waren verrast over de 'versnipperde gevolgen' over het hele land heen. Dit vereiste inzicht in afhankelijkheden tussen organisaties en communicatiestructuren. Bovendien ontbrak het aan het volle zicht op de effecten van de storing.
2. **We zien dat informatiemanagement in zo'n storing netwerksamenwerking vereist, waarin partijen elkaar proactief opzoeken en laagdrempelig informatie met elkaar delen.** De aanpak van zo'n complexe storing vereist een proactieve attitude van informatiemanagers van betrokken actoren en omgevingsbewustzijn. Ook vereist zo'n storing een open organisatie- en netwerkcultuur, waarin informatie makkelijk wordt gedeeld. Ook de scope en de rollen van de betrokkene partijen moeten duidelijk zijn in het proces van informatiemanagement. Dat moet verbeteren.
3. **We zien dat diverse werkwijzen (interdepartementale calls, calls voor informatiemanagers, gebruik van LCMS) behulpzaam zijn in het informatiemanagement.** Ook de aanwezigheid van het Hoofd Nationale Operaties van Defensie in de call hielp. Deze werkwijzen kunnen, met enkele verbeteringen, zonder meer voortgezet worden. Zij helpen betrokken partijen bij collectieve beeld- oordeels- en besluitvorming.
4. **We zien in deze casus dat de beschikbaarheid van informatie en het organiseren van de respons een dilemma vormen.** De achterliggende oorzaken en responsstrategieën bij deze dilemma's bieden aanknopingspunten voor het versterken van het informatiemanagement. Bovendien zien we in deze casus dat de vorming van een landelijk informatiebeeld, onderlinge coördinatie en informatiedeling in de nacht kwetsbaar zijn én dat de snelheid waarmee informatie-calls tot stand komen beter kan.
5. **We constateren dat de preparatie op dit soort high impact storingen beter moet, evenals het opvolgen van lessen uit oefeningen als ISIDOOR.** Dit is van belang in het licht van hybride dreigingen, kans op nieuwe storingen en onze afhankelijkheid van ICT.
6. **We zien bij betrokken partijen ambitie om het informatiemanagement (inclusief de onderlinge coördinatie) tijdens storingen te versterken,** onder meer op het vlak van vroegtijdiger schakelen, 'connecting the dots' en preparatie op systeemstoringen als NAFIN, KPN en CrowdStrike.

3.2 Aanbevelingen

Omdat de dilemma's (beschikbaarheid van informatie en het organiseren van de respons) zo nauw samenhangen en elkaar kunnen versterken, is het van groot belang om niet alleen te focussen op de aanbevelingen met betrekking tot één dilemma. Aanbevelingen worden daarom zo geformuleerd, dat ze ingaan op de impact van beide dilemma's. Gebaseerd op de lessen en observaties van de leertafel worden aanbevelingen geformuleerd die ingaan op de preparatie en op de acute fase van een storing. Ze zijn geclusterd rond vier onderwerpen: preparatie, kennisopbouw, attitude en professie en procesverbeteringen.

Preparatie

Organisaties worden, zoals duidelijk werd tijdens de NAFIN-storing, verrast door onderlinge verwevenheid van netwerken en ICT-voorzieningen. Deze casus liet zien dat er géén overzicht was van wat allemaal op het NAFIN-netwerk aangesloten is. Om de preparatie op dit soort storingen te versterken adviseren we:

- > *Wijze van optreden.* Werk drie of vier maatgevende 'systeemstoringsscenario's' uit. In die scenario's zou de gewenste wijze van optreden van betrokken actoren centraal moeten staan, waaronder de wijze van alarmering en opschalen, informatiedeling en onderlinge leiding en coördinatie. De eerder opgestelde 'Cyberscenario's voor veiligheidsregio's' (Daan et al., 2021) zouden daarbij als inspiratie kunnen dienen.
- > *Afhankelijkheden in beeld.* Breng de mate waarin cruciale informatie-, hulpverlenings- en crisismanagementsystemen afhankelijk zijn van bepaalde aanbieders zoals Defensie, KPN en ODIDO beter in kaart.
- > *Inrichten 'single point of contacts'.* Organiseer verbindingsofficieren bij vitale (telecom)aanbieders zoals Defensie, KPN en ODIDO. Dit advies kan door de NCTV in samenwerking met LOCC/KCR2 worden doorgevoerd in de doorontwikkeling van landelijke planvorming.
- > *Redundantie.* Daarop voortbouwend: welke alternatieven zijn er beschikbaar als fall-back optie. Dergelijke fall-back-opties kunnen een plek krijgen in business continuïteitsplannen.

Kennisopbouw

Geconfronteerd met nieuwe risico's is het opbouwen van kennis en ervaring met planvorming en procedures wenselijk. Daarvoor geven we de volgende adviezen.

- > *Meer toegespitst oefenen.* Organiseer, in aanvulling op ISIDOOR, verdiepende oefeningen om planvorming en operationele processen, zoals informatiemanagement en procedures zoals calls concreter te testen en te doorleven, bijvoorbeeld in de vorm van kleinschalige table tops.
- > *Evaluatie en leercyclus.* Richt als KCR2 een evaluatie- en leercyclus in, waarin inzetten standaard worden geëvalueerd en lessen geïmplementeerd.
- > *Kennisopbouw door casusonderzoek.* Laat onderzoek uitvoeren naar eerdere (en toekomstige) systeemstoringen zoals KPN en CrowdStrike, gericht op terugkerende dilemma's, patronen en responsstrategieën. Benut daarbij als beoordelingskader voor de respons hoofdstuk 3.

Attitude en professie.

Nieuwe risico's vereisen een doorontwikkeling van de crisisprofessie. Een storing kent een ander verloop en verschijningsvorm dan een klassieke flitscrisis.

- > *Laagdrempelig informatiedelen.* Informele netwerken bleken tijdens de storing heel geschikt om, ongeacht de beperkte communicatielijnen, toch informatie te verzamelen. Een manier om deze informele kanalen te benutten voor informatieverzameling en -deling is het aanmaken van een Signal-groep. Dat is laagdrempeliger dan het bewandelen van formele informatielijnen (zie verder: paragraaf 3.3.2, reflectie 2).
- > *Proactieve attitude.* Tijdens de leertafel werd geopperd om functionarissen zoals informatiemanagers en operationeel leiders bij de veiligheidsregio's en andere partijen aan te moedigen om proactief het LOCC te benaderen voor een IM/OL-call of het organiseren van een landelijk beeld. Een dergelijke proactieve houding, gebaseerd op een behoefte van een of meerdere stakeholders, helpt het LOCC om 'aan te gaan'. Bovendien zorgt zo'n geïnternaliseerde werkhouding ervoor dat de partijen binnen het netwerk in staat zijn tot snellere informatiedeling en eerste duiding van de situatie, als oplossing voor het geconstateerde dilemma. In de ISIDOOR-evaluatie adviseerden we over een onderwijsmodule 'Wegwijs in de landelijke crisisstructuur'. Hierin zouden de relatie, de proactieve attitude en samenwerking met het LOCC tijdens bovenregionale crises voor informatie- en crisismanagers een plek kunnen krijgen.
- > *Contextuele bril ontwikkelen.* Tijdens de leertafel pleitten deelnemers voor het stimuleren van 'crisisdenken' onder crisisprofessionals zoals informatiemanagers (zie verder: paragraaf 3.3.1, reflectie 1). Wat crisisdenken precies inhoudt, is niet helder, hoewel gedacht wordt aan zaken als:
 - denken in mogelijke scenario's en cascade-effecten; out-of-the-box denken
 - situationeel en omgevingsbewustzijn
 - bijeenleggen van 'weak signals'
 - raadplegen van andere partners voor informatie
 - het brede plaatje leren zien door over de grenzen van de eigen organisatie, sector of regio heen te kijken.

Procesverbeteringen

Naast een verandering in houding, zijn ontwikkelmogelijkheden geïdentificeerd in werkprocessen van het LOCC/KCR2, in het bijzonder de werkwijze rond de zogeheten calls. (Zie ook: Broeders & van der Varst, 2024). Daartoe worden de volgende adviezen gegeven.

- > *Informatiesheet call.* Maak een factsheet over het verloop van IM/OL-call, wat informatiemanagers en operationeel leiders van die calls kunnen (en mogen) verwachten, welke bijdrage zij zelf kunnen leveren (proactief aanvragen call, actief informatie delen, vertellen welke acties en maatregelen door de eigen organisatie worden genomen), welke partijen aansluiten, wat mogelijke doelstellingen van calls zijn.
- > *Professionaliseer de calls.* Voor een soepel en doeltreffend verloop van calls wordt geadviseerd de werkwijze van calls verder te versterken. Deze acties dragen bij aan beide dilemma's. Hierbij kan gedacht worden aan:
 - *Vergaderregels.* Herkenbare vergaderregels, waaronder een duidelijke (BOB-) structuur, overlegagenda en duidelijk wie-is-wie.
 - *Standaard checks.* Bijvoorbeeld: ontbreken er partijen aan tafel die informatie hebben en 'informatie dots' zoals LMS Caco Call, VR ISAC en het Interdepartementale Infoteam?
 - *Landelijk beeld koppelen aan call.* Tevens kan overwogen worden standaard een call bij het opstarten van een landelijk beeld te organiseren. Op deze manier kan het landelijk beeld direct worden besproken en voorzien worden van eerste duiding en mogelijke vervolgacties. Bijvoorbeeld ook: welke afspraken maken de

informatiemanagers over het proactief informeren van hun regionaal operationeel leider bij sluimerende incidenten.

3.3 Twee reflecties

We sluiten dit hoofdstuk af met twee reflecties.

3.3.1 Reflectie 1: breder kijken

Tijdens de leertafel werd duidelijk dat het van groot belang is om een incident te benaderen door een contextuele bril op te zetten, dat wil zeggen: naar het brede plaatje leren zien door over de grenzen van de eigen organisatie heen te kijken, en ervan uitgaan dat andere organisaties met dezelfde storing te maken hebben, omdat de eigen organisatie deel uitmaakt van een breder netwerk.

Maar hoe deze benadering geconcretiseerd kan worden, blijft onduidelijk. Waar liggen de grenzen van de eigen organisatie en hoe ver zou men over deze grenzen heen moeten kijken? Dit vereist vaardigheden die aangeleerd moeten worden. Wij adviseren vier mogelijke invalshoeken die helpen breder te kijken en zo een contextuele bril te ontwikkelen.

1. *Deelname aan regionale risicoanalyses.* Veiligheidsregio's werken met risicoprofielen op verschillende niveaus, van operationeel naar strategisch niveau. Door een inventarisatie en analyse van risico's kunnen de waarschijnlijkheid en impact van die risico's geschat worden. De deelname van bijvoorbeeld piketmedewerkers zou kunnen helpen om inzicht te krijgen in welke organisaties en structuren op het spel staan op het moment dat risico's zich manifesteren.
2. *Ontwikkelen van scenariodenken.* Het ontwikkelen van scenario's kan volgens Luesink et al. (2024) op verschillende manieren. Het is vooral van belang om toekomstgericht te kijken naar de mogelijke manifestatie en ontwikkeling van risico's. Scenariodenken gaat ook in op de mogelijke betrokkenheid van organisaties en partijen. Door middel van workshops of cursussen kunnen crisisprofessionals zich de methodiek van scenariodenken zelf aanleren.
3. *Deelname aan een cursus systemische risicoanalyse.* Systemische risicoanalyse betekent kijken naar de samenhang en interacties van risicofactoren. Sommige risico's kunnen elkaar versterken en vormen zo een drijvende kracht voor een crisis. Door naar de interactie en cascade-effecten van risico's te kijken, kan de betrokkenheid van andere partijen of organisaties belicht worden. Dit helpt om over de grenzen van de eigen organisatie heen te kijken.
4. *Roulatie met crisisorganisaties.* Door in de schoenen van iemand anders te staan, wordt het makkelijker om de impact van storingen of incidenten op andere organisaties te begrijpen. Roulatie of meeloopdagen met andere organisaties zijn daarom geschikt om de perspectieven van andere organisaties te leren kennen.

3.3.2 Reflectie 2: laagdrempelig organiseren van de respons

Tijdens de leertafel werd gesuggereerd dat professioneel organiseren ofwel alarmeren vooral laagdrempeliger moet gebeuren. Daarom werd onder andere voorgesteld om een Signal-groep te organiseren waar iedereen snel en informeel met zijn vragen, opmerkingen of bijzonderheden terecht kan, zonder meteen over te gaan op professioneel organiseren op een grotere en formele schaal. Tijdens de leertafel werd het advies genoemd om iedereen

op een heel laagdrempelige manier deze Signal-groep te laten gebruiken, met als 'quick action' dat aan iedereen gevraagd moet worden hierin snel en tijdig berichten te plaatsen.

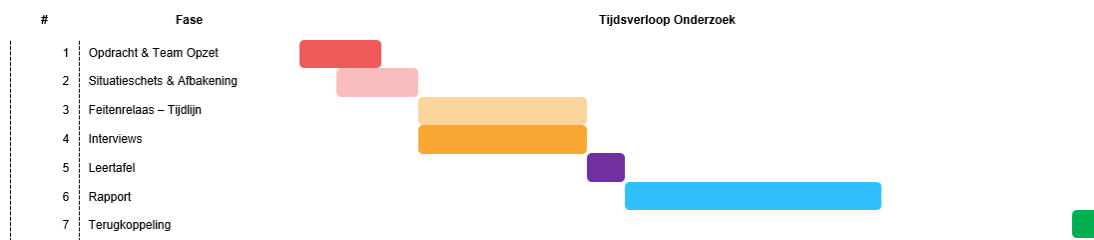
Maar laagdrempeligheid kun je niet zomaar eisen; laagdrempeligheid moet door iedereen worden beleefd. Puur het bestaan van een Signal-groep gaat laagdrempeligheid niet faciliteren, vooral als in de groep spelers van verschillende organisaties zitten, met wie mensen nog geen goede band hebben. Laagdrempeligheid ontstaat door goede, informele netwerken waarvan men deel uitmaakt. Deze netwerken zijn niet per se gekoppeld aan de hiërarchieën en processen van een organisatie, maar ontstaan door informele gesprekken op de werkvloer, tijdens vergaderingen of andere buitenprofessionele activiteiten. Het waren deze informele lijntjes die ook tijdens de NAFIN-storing faciliterend waren voor het oplossen van het incident.

Daarom is het van belang om informele netwerken te versterken door:

1. Al bestaande informele netwerken te identificeren (door bijvoorbeeld aan iedere medewerker te vragen: bij wie kun je bij onzekerheden het makkelijkst je vragen en twijfels kwijt?).
2. Sociale vergaderingen met andere organisaties te bevorderen.
3. Een werk- of rolswitch van medewerkers uit de eigen organisatie met medewerkers met een soortgelijke positie van een andere organisatie.
4. Deelname aan (cyber)oefeningen met een diversiteit aan medewerkers uit andere organisaties met een gezamenlijk doel.

Informele lijntjes komen dus tot stand door het bevorderen van bijeenkomsten waar mensen op een informele manier kennis met elkaar kunnen maken. Hierdoor worden informele netwerken vergroot, welke wederom op een organische manier heel laagdrempelig kunnen worden gebruikt. Ook kunnen door informele netwerken alternatieve communicatielijnen ontstaan die gebruikt kunnen worden als de standaardlijnen uitvallen.

Bijlage 1: Leermethodiek



#	Fase	Uitvoering
1	Opdracht & Team Opzet Duur: ~1-2 weken	Doel: Aanvraag opdracht en bestemming van het onderzoeksteam en aanspreekpartners van de opdrachtgevers. Proces: Na de initiële aanvraag van de opdracht bespreken de opdrachtgevers en het onderzoeksteam gezamenlijk de aanleiding van de opdracht en de teamopzet voor de uitvoering van het onderzoek. Hierbij spreekt iedereen af te focussen op waarderend en toekomstgericht onderzoek, door kort-cyclisch te leren om tot snelle en concrete actielijnen te komen.
2	Situatieschets & Afbakening Opdracht Duur: ~1-2 weken	Doel: Uitwerking doelstelling, omvang, duur en planvorming van het onderzoek. Proces: Tijdens een oriëntatiefase stellen de opdrachtgevers en het onderzoeksteam gezamenlijk de scope van het onderzoek vast. Vragen over een eerste indruk van de impact van het incident en welke organisaties geraakt werden, zijn van belang. Het team definieert het doel van de opdracht en zorgt voor een goede afbakening van het onderzoek door de doelgroep, duur en resulterende producten vast te leggen. Ook spreekt het team de planvorming af: wanneer moeten welke stappen van het onderzoek af zijn? Kort-cyclisch onderzoek vraagt om een snelle uitvoering, maar diepgaande inzichten eisen ook tijd. De taak van het team is om hierin een goede balans te vinden.
3	Feitenrelaas – Tijdlijn Duur: ~2-4 weken	Doel: In kaart brengen van de context van het incident op een tijdlijn. Proces: Het onderzoeksteam verzamelt informatie en tijdstippen van de gebeurtenissen rondom het incident door te focussen op drie factoren: het tijdstip van een gebeurtenis, de omschrijving en de sleutelmomenten. De verdeling van de tijdstippen geeft inzicht in de spreiding van gebeurtenissen over de duur van het incident. De omschrijving geeft niet alleen inzicht in wat er gebeurde, maar ook in de betrokkenheid van partijen. Het onderzoeksteam definieert sleutelmomenten die een significante invloed hebben gehad op het verdere verloop van het incident. Het team scherpt de sleutelmomenten aan met de inzichten uit de interviews en de leertafel. Het onderzoeksteam koppelt de inzichten uit de tijdlijn terug aan de opdrachtgevers.
4	Interviews Duur: ~2-4 weken	Doel: Subjectieve, eerste verzameling van inzichten over het incident; ook ter voorbereiding van de leertafel. Proces: Het onderzoeksteam selecteert een aantal respondenten voor de interviews die een goede doorsnede en diversiteit van betrokken partijen

tijdens het incident weergeven. De onderzoekers letten bij de interviews op inzichten in de betrokkenheid van de respondent tijdens het incident, identificeren dilemma's en uitdagingen, bespreken goede lessen en praktijken en verzamelen verwachtingen over de leertafel. Vervolgens werken de onderzoekers de inzichten van alle respondenten uit en vatten dilemma's, uitdagingen, goede lessen en praktijken samen. Het resultaat bespreken de onderzoekers vervolgens met de opdrachtgevers.

- 5 Leertafel** **Doel:** Actieve uitwisseling van ervaringen, dilemma's, goede lessen en praktijken die opgedaan of uitgevoerd zijn door alle betrokkene partijen tijdens het incident om gezamenlijk tot concrete actielijnen te komen.
- Duur: ~3-5 uur
- Proces:** Tijdens de leertafel modereren de onderzoekers de voortgang van de discussie. Hierbij focust het team vooral op de goede praktijken en hoe deze vertaald kunnen worden naar concrete, snelle actielijnen. De onderzoekers presenteren aan het begin van de leertafel de inzichten uit de tijdlijn en de interviews en stellen vervolgens de belangrijkste dilemma's voor. Daarna is het vooral aan de deelnemers om de open discussie te verrijken.
- 6 Rapport** **Doel:** Aan de ene kant verzameling van inzichten uit de tijdlijn, interviews en leertafel, maar aan de andere kant ook kritische reflectie en adviezen.
- Duur: ~3-6 weken
- Proces:** Het onderzoeksteam verzamelt alle inzichten uit de afspraken met de opdrachtgevers, tijdlijn, interviews en leertafel in een beknopt rapport. Bovendien zorgen de onderzoekers voor een onafhankelijke, kritische reflectie op de door de leertafel uitgewerkte actielijnen. In het rapport wordt ook de potentie voor vervolgonderzoek aangegeven.
- 7 Terugkoppeling** **Doel:** Verkenning van de toepasbaarheid van adviezen en in hoeverre deze omgezet zijn in de praktijk.
- Duur: ~1 uur
- Proces:** De onderzoekers nemen een half jaar na afloop van het onderzoek contact op met de opdrachtgevers voor een terugkoppeling over alle opgezette actielijnen. De inzichten uit de terugkoppeling zijn informatief voor het onderzoeksteam voor mogelijke, toekomstige kort-cyclische opdrachten.

Bijlage 2: Bronnen

- Algemene Rekenkamer. (2024). *De kracht en kwetsbaarheid van het digitale krijgsmachtnetwerk NAFIN*. Algemene Rekenkamer.
- Bakker, M., Berger, E., Varst, L. van der, & Karacan, O. (2021). *Informatiemanagement in veiligheidsregio's. Een onderzoek naar de ervaringen van informatiemanagers en operationeel leidinggevendenden*. NIPV, 55.
- Boin, A., Stern, E., & Sundelius, B. (2016). *The politics of crisis management: Public leadership under pressure*. Journal of Contingencies and Crisis Management.
- Broeders, S., & van der Varts, L. (2024). *Sectorale evaluatie ISIDOOR-4*. NIPV.
- Daan, H., van der Varst, L., & Groenendaal, J. (2021). *Cyberscenario's voor veiligheidsregio's*. NIPV, 21.
- Dearstyne, B. (2007). *The FDNY on 9/11: Information and Decision Making in Crisis*. Government Information Quarterly, 24(1), 24–46.
- Kapucu, N., Arslan, T., & Demiroz, F. (2010). *Collaborative emergency management and national emergency management network*. Disaster Prevention and Management, 19(4), 452–468.
- NCTV, & NCSC. (2022). *Cybersecuritybeeld Nederland 2022*. CsbN, 1–76.
https://www.thehaguesecuritydelta.com/media/com_hsd/report/237/document/CSBN2019-online-tcm31-392768.pdf
- Netwerk Netcentrisch Werken. (2022). *Handboek Informatiemanagement Crisisbeheersing*. NIPV, 52.
- OECD. (2015). *The Changing Face of Strategic Crisis Management*. OECD Reviews of Risk Management Policies, OECD Publishing.
- Treurniet, W. (2022). *Between chaos and continuity: A common operational picture in support of emergency response networks*. PhD-Thesis - Research and Graduation Internal, Vrije Universiteit Amsterdam.
- Van der Varst, L., Domrose, J., Berger, E., Luesink, M., Van der Spek, S., & Van Duin, M. (2022). *Toekomstverkenning Crisisbeheersing. Wendbare crisisbeheersing. Wen er maar aan*. NIPV.
- Wolbers, J., Luesink, M., van Duin, M., & Kuipers, S. (2024). *Scenario planning to enable foresight in crisis management Menno van Duin*. ISCRAM Proceedings, 21.