Koepelnotitie

Crisiscommunicatie in het digitale domein

Januari 2023

Inhoud

1. Inleiding

Digitale incidenten kunnen onze maatschappij gedurende korte of langere tijd verlammen. En terwijl de dreiging van digitale incidenten toeneemt, blijft de weerbaarheid van Nederlandse bedrijven en overheden achter. Daarom moet digitale weerbaarheid topprioriteit zijn in alle geledingen van de samenleving. Niet alleen door een goed slot op de digitale deur te zetten, maar ook door voorbereidingen te treffen voor als het onverhoopt misgaat. Dat betekent oefenen, opleiden en trainen op alle niveaus - bínnen een organisatie én met partners.

In het Landelijk Crisisplan Digitaal (LCP Digitaal) staan de afspraken en sleutelbesluiten in geval van een grootschalig en maatschappij-ontwrichtend digitaal incident. Rijk, regio's en vitale partners zullen elkaar moeten vinden – ook als het gaat om het afstemmen van de (crisis)communicatie. Deze communicatienotitie is een verdieping van het hoofdstuk Communicatie uit het LCP Digitaal.

In deze herziene versie van de koepelnotitie helpen we communicatieprofessionals bij de voorbereiding op de crisiscommunicatie. Daarbij gaat het niet alleen om crisiscommunicatie bij crises met maatschappij-ontwrichtende effecten. Ervaring leert inmiddels dat communicatie en het afstemmen ervan ook in andere scenario's aan de orde is. Ook bij een digitale dreiging of een digitaal incident met beperkte (regionale) gevolgen wordt al actie van communicatieprofessionals verwacht. Daarom zijn in deze koepelnotitie deze drie scenario's verder uitgewerkt.

De praktische aanbevelingen van deze notitie zijn samen met onze partners tot stand gekomen: NCSC, BZK, DTC, EZK, IenW, Politie en vertegenwoordigers van de Veiligheidsregio's en het OM. We danken hen daar hartelijk voor.

2. Crisiscommunicatie bij digitale incidenten

Uitgangspunten

In een tijd waarin op social media binnen enkele minuten informatie massaal wordt gedeeld (of die informatie nu waar is of niet), zijn heldere uitgangspunten voor crisiscommunicatie van groot belang. Meer dan ooit is tijdens een crisis zichtbaarheid, eenduidigheid en tijdigheid in de communicatie doorslaggevend. Daarom stemmen alle relevante partijen hun timing en inhoud van communicatie zoveel mogelijk met elkaar af.

Doel

- Eenduidige en tijdige (publieks)communicatie.
- Gericht op schadebeperking (het geven van handelingsperspectief), informatievoorziening (voldoen aan de maatschappelijke informatiebehoefte) en betekenisgeving.

Wijze van communiceren

- Omgevingsbewust, proactief, open, tijdig en consistent.
- In afstemming met alle relevante partijen (timing en inhoud van communicatie).

Waarover

- Communiceer over het proces, ook als er nog weinig bekend is: vertel wat je weet en nog niet weet, welke stappen worden gezet - zorg dat de overheid zichtbaar is.
- Communiceer over zichtbare maatregelen en indien wenselijk/mogelijk ook over onzichtbare maatregelen.
- Geef indien mogelijk antwoord op de vraag: wat kunnen mensen doen? Hoe kan men zelf handelen en anderen helpen (bevorderen (zelf)redzaamheid).
- Bevestig wat waar is, ontkracht geruchten of laat weten dat je de geruchten kent en ze onderzoekt.

Waarover níet

Communiceer zonder afstemming niet over SISOS: slachtoffers, identiteiten, scenario's, oorzaken en schade.

In de voorbereiding

Pak positie in je organisatie

- Zorg voor aansluiting bij de operationele collega's die zich met digitale incidenten bezighouden.
- Maak duidelijke afspraken over (tijdige) opschaling en wijze van afstemming.
- Zorg voor communicatievertegenwoordiging in de crisisteams.
- Maak een plan B voor uitval van digitale communicatiemiddelen.
  - Hoe communiceer je dan met je collega's en partners? Maak een overzicht van (analoge) communicatiemiddelen die niet afhankelijk zijn van netstroom, denk aan persoonlijk contact, inzetten van intermediairs (zoals hulp- en zorgverleners), geluidswagens, media die via de ether uitzenden (ontvangst met autoradio, apparaten op batterij).

Organiseer de samenwerking

- Maak een overzicht van communicatiepartners, inclusief e-mailadres en (piket) nummer. Deze zijn vaak anders dan bij een fysieke crisis. Werk dit overzicht ieder half jaar bij.
- Maak een lijstje met (in-en externe) experts/deskundigen die technische informatie kunnen duiden tijdens een incident. Crisiscommunicatie bij incidenten met een digitale component vraagt veelal om vertaling van technische termen en uitleg van processen.
- Zoek uit aan welke specifieke expertise je behoefte hebt, welke kennis je nu mist, wat je nodig hebt om te kunnen communiceren.

Ken de materie

- Verkrijg inzicht in communicatieve vraagstukken, dilemma's en beslispunten.
- Bereid zoveel mogelijk kernboodschappen en beeld voor (visuals/ infographics etc.) die ingewikkelde materie begrijpelijk maken.

Opleiden, trainen en oefenen

- Beoefen en doorleef verschillende scenario's, bijvoorbeeld middels een tabletop.
- Zorg dat taken en rollen in de crisisorganisatie bekend én beoefend zijn.

Tijdens de uitvoering

Haal de buitenwereld binnen.

- Organiseer (communicatie) afstemming met betrokken externe partijen, binnen Rijk, regio en evt. private partners.
- Maak omgevingsanalyses en zorg dat je weet welke vragen er leven bij jouw doelgroepen en stakeholders.
- Richt webcare in om vragen te beantwoorden en geruchten waar nodig te ontkrachten.
- Wees alert op desinformatie (het doelbewust, veelal heimelijk, verspreiden van misleidende informatie, met het doel om het publieke debat, democratische processen, de open economie of nationale veiligheid te schaden of te verstoren).
- Overweeg onderzoek (o-meting/ flitspeiling) te doen onder je doelgroepen om vragen en sentiment te achterhalen.
- Moeten doelgroepen gedurende langere tijd iets doen of laten? Schakel gedragswetenschappers in om mee te denken over een langdurig effectieve aanpak van de crisiscommunicatie.
- Draag veel gestelde vragen en kernboodschappen op alle mogelijke manieren uit. Digitaal waar mogelijk, anders analoog.

Pas je communicatie aan

- Denk na over de timing van je boodschap. Breng zoveel mogelijk zelf het nieuws naar buiten.
- Formuleer een kernboodschap.
  - Deel wat je al weet én wat je doet (procesinformatie): cyberanalyses kosten relatief meer tijd dan in fysieke wereld. Het duurt vrij lang om scenario's te kunnen wegstrepen.
  - Deel hierbij – indien nodig- ook de communicatiedilemma's.
  - Beschrijf wat er anders is bij een ICT-crisis:
    - Attributie (het is moeilijk te achterhalen wie of wat de crisis heeft veroorzaakt);
    - Analyse/ duiding;
    - Bestrijden verdere verspreiding (domino-effecten);
    - Digitaal versus fysieke effecten.

- Vertel zodra het kan wat mensen kunnen doen/ moeten laten.
- Communiceer (ook) in begrijpelijke, eenvoudige taal.
- Visualiseer ingewikkelde technische materie. Denk hierbij aan film, visuals en infographics, afgestemd per doelgroep.
- Zorg dat derden jouw informatie zo goed en consistent mogelijk kunnen delen.
- Beperk je niet tot digitale middelen; denk ook aan 'analoge kanalen' om doelgroepen te bereiken.
- Heb oog voor moeilijk bereikbare doelgroepen
  - mensen zonder toegang tot geijkte communicatiekanalen en –middelen;
  - mensen die de Nederlandse taal niet machtig zijn;
  - 'digibeten' of mensen voor wie ogenschijnlijk ingeburgerde (Engelse) cybertermen abracadabra zijn.
- Vergeet interne communicatie niet: ook medewerkers communiceren naar buiten of met partners.

Houd direct rekening met het ergste

- Werk *worst case* scenario's uit. Bij uitval van digitale middelen is de maatschappelijke impact al snel groot en wordt communiceren ernstig bemoeilijkt.
- Heb oog voor de mogelijke domino-effecten of cascade-effecten: digitaal, maar vooral ook fysiek. Deze kunnen al snel merkbaar zijn.
- Maatschappelijke onrust kan het vertrouwen in de overheid schaden. Houd via omgevingsanalyses vinger aan de pols en acteer waar nodig.

Nafase

- Heb bij de start van de digitale crisis, ook direct oog voor de nafase, de fase van herstel en nazorg. Laat de afschaling en overgang van de acute fase naar de na(zorg)fase geleidelijk verlopen en in samenspraak met de betrokken ministeries en andere betrokken partners.

3. Aan de slag met scenario's uit LCP Digitaal

Er zijn talloze scenario's denkbaar als het gaat om incidenten in het digitale domein, zeker in combinatie met een mogelijke doorwerking naar het fysieke domein. Daarom is in het Landelijk Crisisplan Digitaal gekozen voor een aanpak op basis van bouwstenen: oorzaak, bron, actor, geraakt domein, geraakt gebied en technische oplossingsperspectief. Door steeds een bouwsteen te wijzigen, ontstaan acht werkbare scenario's.

Elk scenario kent een eigen aard en verloop, met elk andere gevolgen/effecten. Die zijn weer mede bepalend voor de inrichting van de gewenste respons en benodigde maatregelen. Ook de communicatie kan per scenario verschillen in aanpak.
Om de crisiscommunicatie goed voor te bereiden is het raadzaam om per scenario enkele hoofdvragen te beantwoorden:

- Wat is er aan de hand, wat gaat er mis?
- Hoe erg is het, en voor wie?
- Wat zijn de belangrijkste mogelijke (in)directe gevolgen en effecten?
- Welke maatregelen zijn nodig om de gevolgen en effecten te voorkomen of te beheersen? Wat kunnen mensen zelf doen?
- Welke partijen zijn betrokken c.q. nodig voor een adequate aanpak?
- Wie communiceert (wie is afzender)?

Houd bij deze denkexercitie rekening met:

- Tijdige escalatie van de interne (crisis)organisatie;
- Mogelijke reputatieschade;
- De uitval van middelen en dienstverlening;
- Maatschappelijke onrust;
- Mogelijke cascade effecten die de eigen organisatie of anderen kunnen raken;
- De wijze van urgentie duidelijk maken als de gevolgen nog weinig zichtbaar zijn; - Oplostijden vaak onbekend (lange doorlooptijd mogelijk)
- Politieke druk om maatregelen te treffen;
- Grensoverschrijdende problematiek;
- Dilemma's die zich kunnen voordoen.

4. Drie crisiscommunicatie-scenario's

Wat maakt crisiscommunicatie bij digitale incidenten anders? Wat een digitaal incident in elk geval complex maakt, is de verwevenheid van het digitale met het fysieke domein. Ook zijn de gevolgen van een digitaal incident vaak langere tijd nog niet zichtbaar. Als er vervolgens effecten optreden, kan het ineens snel gaan: maatschappelijke ontwrichting als gevolg van incidenten in het digitale domein wordt vaak gekenmerkt door een razendsnelle verspreiding en meerdere cascade-effecten. De crisis ontstaat met weinig oog voor geografische grenzen, is mogelijk langdurig en er bestaat vaak lang onzekerheid over oorzaak, omvang en impact. Het kan daarmee zeer complex zijn om de gevolgen van digitale incidenten op korte en lange termijn te bepalen.

Crisiscommunicatie in het digitale domein wordt bepaald door de aard van de (dreigende) crisis. Bij een dreiging kan er technisch-operationeel nog niets aan de hand zijn, terwijl er op communicatiegebied al wordt opgeschaald: CERTs worden actief, de informatiebehoefte neemt toe terwijl de buitenwereld (nog) geen hinder ondervindt. Het incident blijft daarmee veelal technisch van aard en dus abstract voor veel mensen – dat vraagt vanzelfsprekend een andere aanpak dan wanneer de effecten de samenleving dreigen te ontwrichten.

Vanwege de complexiteit van digitale incidenten maken we onderscheid in drie scenario's. Met daarbij direct de kanttekening dat de praktijk weerbarstiger zal zijn dan hier voorgesteld; de scenario's zijn bedoeld om inzicht te geven in communicerende partijen, lijnen en aandachtspunten.

A. Communicatie bij een digitale dreiging
B. Communicatie bij een digitaal incident met beperkte gevolgen
C. Communicatie bij een digitale crisis met maatschappelijke ontwrichting

A. Communicatie bij een digitale dreiging

Op 10 december 2021 is er een ernstige kwetsbaarheid gevonden in Apache Log4j. Dit is software die veel gebruikt wordt in webapplicaties en allerlei andere systemen. Het NCSC waarschuwt voor potentieel grote schade en adviseert organisaties daarom om zich voor te bereiden op een mogelijke aanval.

Kenmerken

- Potentiële maatschappelijke ontwrichting is groot, maar op dit moment zijn er (nog) geen fysieke effecten zichtbaar in de maatschappij.
- Geen opschaling nationale crisisstructuur, geen actief Nationaal Kernteam Crisiscommunicatie, vaak wel actieve lijnen om informatie uit te wisselen.
- Burgers ondervinden (nog) geen hinder, wel horen ze dat er íets aan de hand is.
- Het zijn vooral organisaties, vitale aanbieders en bedrijven die maatregelen moeten treffen.
- Ook veiligheidsregio's moeten maatregelen treffen: de VR's zijn daarmee vooral doelgroep, ze communiceren niet zelf naar hun inwoners.
- Er is bij samenwerkingspartners behoefte aan informatie over de ontwikkeling van de dreiging.

Doel

Als er sprake is van een digitale dreiging is het doel van crisiscommunicatie:

1. Schadebeperking
    a. Organisaties handelingsperspectief bieden: welke maatregelen (technisch/operationeel) moet men treffen.
    b. Indien van toepassing ook burgers handelingsperspectief bieden.
2. Informatievoorziening
    a. Beantwoorden aan de maatschappelijke informatiebehoefte
3. Betekenisgeving
    a. afhankelijk van de aard van de dreiging, kan de duiding plaatsvinden op lokaal, regionaal of nationaal niveau (vanuit oogpunt nationale veiligheid, bijvoorbeeld bij een statelijke dreiging).

Aandachtspunten

- Sta in verbinding met de crisisteam(s) binnen de eigen organisatie en denk aan interne communicatie.
- Communicerende partijen stemmen zelf af met meest betrokken partners over timing en boodschap.
- Het kan raadzaam zijn om informatie(beelden) over de ontwikkeling van de dreiging te delen met betrokken partners.

Communicatieverantwoordelijkheden

Wie	Richt zich op
NCSC	Schadebeperking: • handelingsperspectief (maatregelen technisch/ operationeel) voor NCSC-doelgroepen • indien van toepassing: handelingsperspectief voor burgers
	Informatiebehoefte: Feiten richting algemeen publiek • wat is er aan de hand? • wat doet de overheid? • wie is afzender van de communicatie?
	Betekenisgeving: Duiding digitale incidenten en dreigingen
DTC, CERTs en SOC-organisaties	Schadebeperking: handelingsperspectief (maatregelen technisch/ operationeel) voor de eigen doelgroepen
NCTV en/of MinJenV als coördinerend minister cybersecurity en verantwoordelijk voor nationale crisisstelsel	Betekenisgeving: Duiding dreiging vanuit oogpunt nationale veiligheid: wat kan dit betekenen?
AIVD	Betekenisgeving: Duiding activiteiten en dreigingen door statelijke actoren.

Naast bovenstaande overkoepelende communicatieverantwoordelijkheden communiceert elke organisatie zelf over eigen processen/verantwoordelijkheden.

B. Communicatie bij een digitaal incident met beperkte gevolgen

Een Amerikaanse softwareproducent meldt een kwetsbaarheid in enkele producten. De kans op misbruik wordt in eerste instantie als 'middelhoog' ingeschat. Een misvatting – zeker als blijkt dat de oplossing om het lek te dichten niet toereikend is en hackers vrij spel hebben. De kwetsbaarheid maakt het voor kwaadwillenden mogelijk om toegang te krijgen tot interne bedrijfsinformatie.

De betreffende applicaties worden wereldwijd in bedrijfsnetwerken gebruikt en zorgen o.a. dat medewerkers via internet op afstand toegang krijgen tot interne bedrijfsapplicaties. Om erger te voorkomen adviseert het NCSC organisaties om systemen waar dat kan uit te schakelen, waardoor weer andere problemen ontstaan. Medewerkers die normaal thuis zouden werken, moeten naar kantoor. Er ontstaan lange files in heel het land. In enkele gevallen komen primaire processen van organisaties tot stilstand; zo stoppen veel gemeenten noodgedwongen de dienstverlening aan inwoners.

Kenmerken

- Effect op bedrijfsvoering van organisaties kan ook (regionaal) zichtbare effecten veroorzaken; van grote maatschappelijke onrust is geen sprake, wel van ongemak.
- Nationaal Kernteam Crisiscommunicatie wordt geactiveerd om pers- en publiekscommunicatie te coördineren.
- Mogelijk opschaling (deel van de) nationale crisisstructuur.
- Het zijn vooral organisaties, vitale aanbieders en bedrijven die digitale maatregelen moeten treffen.
- Veiligheidsregio's moeten mogelijk digitale maatregelen treffen én hebben een rol in de communicatie over de fysieke, zichtbare gevolgen lokaal en/of regionaal.
- Er is bij samenwerkingspartners behoefte aan afstemming.

Doel

Als er sprake is van een digitaal incident met beperkte gevolgen, is het doel van crisiscommunicatie:

1. Schadebeperking
    a. Organisaties handelingsperspectief bieden: welke maatregelen (technisch/ operationeel) moet men treffen.
    b. Burgers ter plaatse handelingsperspectief bieden.
2. Informatievoorziening
    a. Beantwoorden aan de maatschappelijke informatiebehoefte.
3. Betekenisgeving
    a. afhankelijk van de aard van het incident en de gevolgen, kan de duiding plaatsvinden op lokaal, regionaal of nationaal niveau (vanuit oogpunt nationale veiligheid, bijvoorbeeld bij een statelijke dreiging).

Aandachtspunten

- Zorg voor goede samenwerking en afstemming met de eigen crisisorganisatie.
- Communicerende partijen stemmen in NKC-verband af over timing en boodschap om te zorgen dat de overheid met één mond spreekt.
- Informatie(beelden) over de ontwikkeling van het incident worden gedeeld via LCMS (Landelijk Crisis Management Systeem).

Communicatieverantwoordelijkheden

Wie	Richt zich op
Nationaal Kernteam Crisiscommunicatie	Coördineren van pers- en publiekscommunicatie over het digitaal incident en de zichtbare gevolgen
Hulpverleningsdiensten (politie, brandweer)	Schadebeperking: • handelingsperspectief voor burgers in fysieke ruimte
	Informatiebehoefte: • opsporingsonderzoek door politie (bij opzettelijk handelen)
Burgemeester, voorzitter veiligheidsregio	Handhaving en openbare orde Veiligheidsmaatregelen
	Betekenisgeving lokaal/regionaal
Publieke en private partijen	Informatiebehoefte en schadebeperking: • Gevolgen voor eigen organisatie en medewerkers, directe gevolgen voor klanten of leveranciers.
NCSC	Schadebeperking: • handelingsperspectief (maatregelen technisch/ operationeel) voor de eigen doelgroepen • indien van toepassing: handelingsperspectief voor burgers
	Informatiebehoefte: Over digitaal incident richting algemeen publiek • wat is er aan de hand? • wat doet de overheid?
	Betekenisgeving: Duiding digitale incidenten en dreigingen
DTC, CERTs en SOC-organisaties	Schadebeperking: handelingsperspectief (maatregelen technisch/ operationeel) voor de eigen doelgroepen
NCTV en/of MinJenV als coördinerend minister cybersecurity en verantwoordelijk voor nationale crisisstelsel	Betekenisgeving: Duiding dreiging vanuit oogpunt nationale veiligheid: wat kan dit betekenen?
Openbaar Ministerie, Landelijk Parket	Informatiebehoefte: Opsporingsonderzoek (zodra verdachte bekend is)
AIVD	Betekenisgeving: Duiding activiteiten en dreigingen door statelijke actoren.

C. Communicatie bij een digitale crisis met maatschappelijke ontwrichting

Het is begin juni 2021. Nederland wordt getroffen door meerdere cyberaanvallen. De gevolgen voor de samenleving zijn groot. Geen of vervuild water uit de kraan, de energievoorziening valt uit en digitaal betaalverkeer is niet meer mogelijk. De oorzaak: een complexe aanval door een (fictieve) statelijke actor. Het is het scenario van ISIDOOR 2021, de grootste nationale cyberoefening van een digitaal incident met fysieke gevolgen. De oefening begint technisch maar leidt al snel tot een nationale crisis.

Kenmerken

- De crisis is bovenregionaal, gaat waarschijnlijk zelfs over landsgrenzen heen en treft meerdere voorzieningen.
- Operationele, bestuurlijke en communicatieve afstemming is noodzakelijk om de crisis aan te gaan.
- De nationale crisisstructuur wordt geactiveerd, evenals het Nationaal Kernteam Crisiscommunicatie.
- Rijk en veiligheidsregio's werken samen volgens de afspraken in het Landelijk Crisisplan Digitaal.
- Zichtbare effecten veroorzaken maatschappelijke onrust. Er is veel behoefte aan informatie en handelingsperspectief op alle niveaus: organisaties, bedrijven, overheden en burgers.

Doel

1. Informatievoorziening
   a. Beantwoorden aan de maatschappelijke informatiebehoefte.
2. Schadebeperking
   a. Burgers handelingsperspectief bieden.
   b. Organisaties handelingsperspectief bieden: welke maatregelen (technisch/operationeel) moet men treffen.
3. Betekenisgeving
   a. duiding vindt sowieso plaats op nationaal niveau.
   b. ook op lokaal/regionaal niveau kunnen bestuurders aan betekenisgeving doen.

Aandachtspunten

- Zorg voor goede samenwerking en afstemming met de eigen crisisorganisatie.
- Partijen stemmen in NKC-verband af over timing en boodschap om te zorgen dat de overheid met één mond spreekt.
- Informatie(beelden) over de ontwikkeling van het incident worden gedeeld in LCMS.
- Zolang niet zeker is of een incident opzettelijk handelen is, vermijden we verwijzingen naar mogelijke oorzaken, duur en omvang.
- Wanneer vanuit veiligheidsoverwegingen communicatie over (technische en operationele) kwetsbaarheden en/of maatregelen niet mogelijk is, melden we dat (‘u ziet wat u ziet, wij doen uit veiligheidsoverwegingen geen nadere mededeling over de maatregelen’).
- Er is behoefte aan leiderschap en rust van bestuurders. Communicatie van bestuurders verbindt daarom de samenleving en doet een beroep op de veerkracht van individuele burgers en van de Nederlandse samenleving als geheel.

Verantwoordelijkheden

Iedere betrokken partij communiceert vanuit de eigen verantwoordelijkheid over eigen onderwerpen, maar stemt altijd af over timing en inhoud van de boodschap. Dit gebeurt in het Nationaal Kernteam Crisiscommunicatie.

Wie	Richt zich op
Nationaal Kernteam Crisiscommunicatie	Coördineren van pers- en publiekscommunicatie over het digitaal incident en de zichtbare gevolgen
Hulpverleningsdiensten (politie, brandweer)	Schadebeperking: • handelingsperspectief voor burgers in fysieke ruimte
	Informatiebehoefte: • opsporingsonderzoek door politie (bij opzettelijk handelen)
Burgemeester, voorzitter veiligheidsregio	Handhaving en openbare orde Veiligheidsmaatregelen
	Betekenisgeving lokaal/regionaal
Publieke en private partijen	Informatiebehoefte en schadebeperking: • Gevolgen voor eigen organisatie en medewerkers, directe gevolgen voor klanten of leveranciers.
NCSC	Schadebeperking: • handelingsperspectief (maatregelen technisch/ operationeel) voor de eigen doelgroepen • indien van toepassing: handelingsperspectief voor burgers
	Informatiebehoefte: Over digitaal incident richting algemeen publiek • wat is er aan de hand? • wat doet de overheid?
	Betekenisgeving: Duiding digitale incidenten en dreigingen
DTC, CERTs en SOC-organisaties	Schadebeperking: Handelingsperspectief (maatregelen technisch/ operationeel) voor de eigen doelgroepen

Wie	Richt zich op
NCTV en/of MinJenV als coördinerend minister cybersecurity en verantwoordelijk voor nationale crisisstelsel	Betekenisgeving: Duiding dreiging vanuit oogpunt nationale veiligheid: wat kan dit betekenen?
AIVD	Betekenisgeving: Duiding activiteiten en dreigingen door statelijke actoren.
Openbaar Ministerie, Landelijk Parket	Informatiebehoefte: Opsporingsonderzoek (zodra verdachte bekend is)
Betrokken vakminister	Informatiebehoefte en schadebeperking: Feiten en duiding handelingsperspectieven nationaal.

Bijlage 1: Organisatie van de (crisis)communicatie

Het Nationaal Kernteam Crisiscommunicatie (NKC)

Mocht zich een situatie voordoen dat de nationale crisisstructuur wordt geactiveerd dan vindt op nationaal niveau communicatieve afstemming plaats in het Nationaal Kernteam Crisiscommunicatie (NKC).

Het NKC coördineert de pers –en publieksvoorlichting van de Rijksoverheid bij een (dreigende) crisis met nationale impact. Het NKC is een vast onderdeel van de nationale crisisstructuur. In het NKC zijn de verschillende partners op nationaal niveau vertegenwoordigd. Bij een digitaal incident zijn dat in elk geval de ministeries van BZK en JenV, het departement dat verantwoordelijk is voor de getroffen sector, de NCTV, het NCSC en liaisons van OM, de politie en de AIVD. Als belangrijke (ketens aan) bedrijven of delen van de digitale infrastructuur zijn getroffen, neemt EZK deel. In een aantal scenario's zullen ook Buitenlandse Zaken, I&W, Defensie en SZW aansluiten.

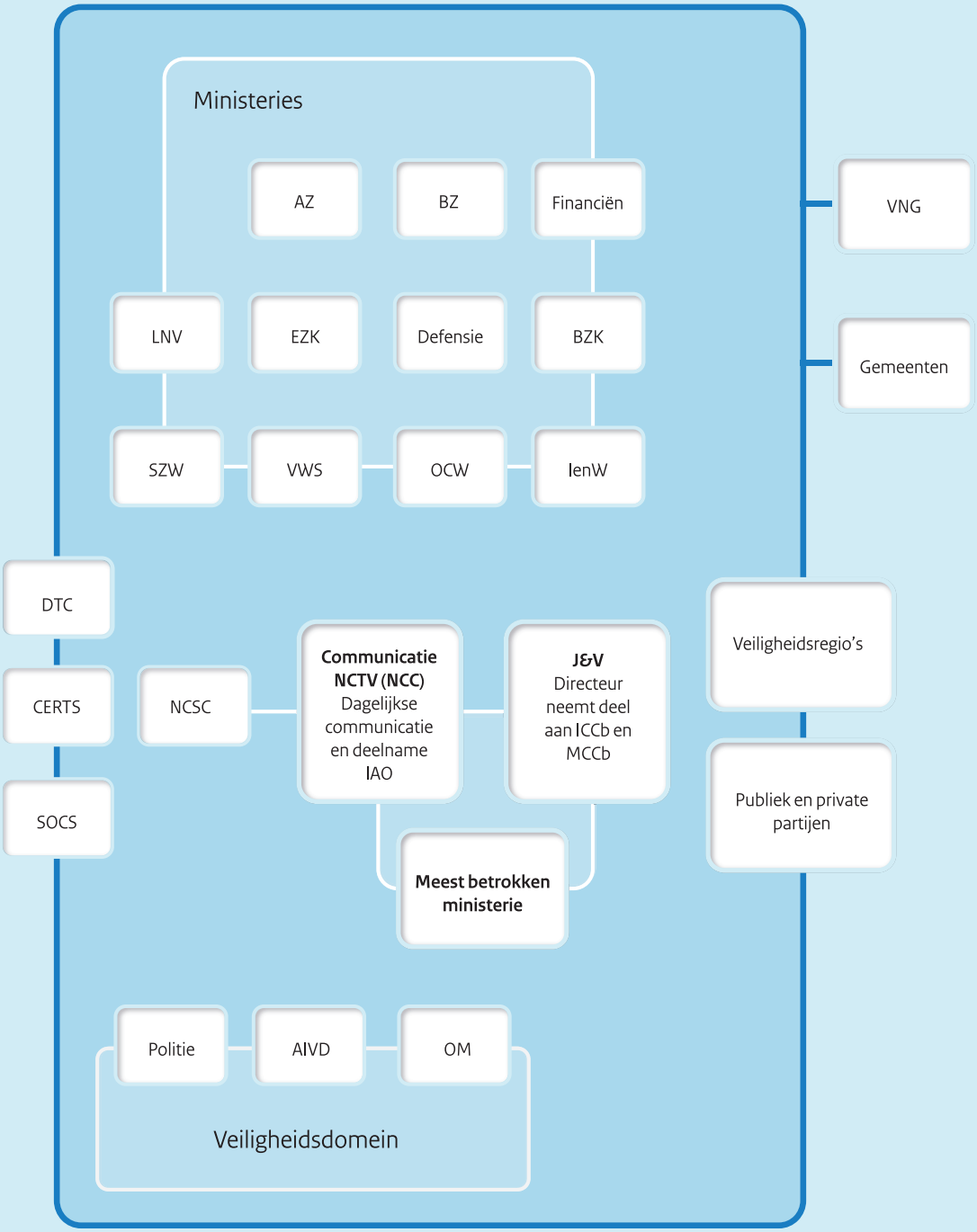
Wanneer het NKC aan de slag gaat, betekent dit niet een opschaling van de communicatie-verantwoordelijkheden naar nationaal niveau. Het betekent wel dat de communicatiestrategie, kernboodschappen en communicatiekaders wordt afgestemd voordat er gecommuniceerd wordt.

Het NKC communiceert via de (crisis)kanalen van de Rijksoverheid over zichtbare maatregelen en geeft procesinformatie over wat de overheid doet en waarom. Elke uitvoeringsorganisatie/gemeente/veiligheidsregio /vitale aanbieder blijft verantwoordelijk voor de communicatie over datgene dat binnen zijn bevoegdheden ligt. Belangrijk is om hierbij in gezamenlijkheid aandacht te hebben voor moeilijk bereikbare doelgroepen/

Het NKC is het aanspreekpunt voor communicatie op rijksniveau. Het NKC coördineert, deelt informatie (zoals omgevingsanalyses) en verzorgt actief de afstemming (inhoud en timing) van boodschappen met veiligheidsregio's, gemeenten en andere betrokken partijen, zoals het NCSC en de Informatie Beveiligingsdienst voor gemeenten (IBD). Communicatiedilemma's op rijksniveau worden beslecht in het NKC en indien nodig in de ICCb of MCCb.

Bij een langdurige opschaling kan specialistische kennis aan het NKC worden toegevoegd. Denk hierbij aan campagneontwikkelaars, gedragswetenschappers en onderzoeksbureaus.

Het Nationaal Kernteam Crisiscommunicatie (NKC)



Aansluiting communicatie op sturingslijnen en informatielijnen

Het NKC is onderdeel van de nationale crisisstructuur via een vertegenwoordiger in de ICCb (hoog-ambtelijk niveau) en de MCCb (ministerieel niveau). De informatiemanager van het NKC is aangesloten op de informatielijn en heeft toegang tot LCMS en andere informatiesystemen. Bij de politie neemt communicatie deel aan het NSGBO. Bij de KMar neemt communicatie deel aan het LSGBO. Bij het OM neemt een woordvoerder deel aan het crisiscentrum van het Parket Generaal. Zij staan ieder in contact met het NKC via de afgevaardigde van politie/OM/KMAR).

Op regionaal niveau is communicatie vertegenwoordigd bij de verschillend bestuurlijke overleggen, bijvoorbeeld die van de voorzitters Veiligheidsregio's met de burgemeesters van de desbetreffende regio. Op lokaal niveau is communicatie vertegenwoordigd in het GBT/RBT, het ROT en CoPI. Daarnaast nemen (in de meeste gevallen) ook persvoorlichting OM en de woordvoerder van de burgemeester/ voorzitter van de veiligheidsregio deel aan de overleggen van de lokale driehoek/ vierhoek.

Om afstemming van de communicatie te vergemakkelijken, kan een liaison van het NKC (op verzoek) aanschuiven in het crisiscommunicatieteam van de getroffen gemeente/regio en vice versa. Wanneer het NKC aan het werk gaat, betekent dit niet een opschaling van de communicatie-verantwoordelijkheden naar nationaal niveau. Het betekent wel dat de communicatiestrategie wordt afgestemd voordat er gecommuniceerd wordt.

Afstemming

Conform de uitgangspunten, stemmen de betrokken partijen hun kernboodschappen en de timing daarvan met elkaar af. Tijdens iedere eerste afstemming (vaak via een conference call/Webex) gebeurt het volgende:

- delen we de omgevings- en media-analyses;
- delen we timing en inhoud van de eerste statements;
- maken we afspraken voor de komende uren: wie gaat er wanneer naar buiten,
- wie zijn de 'talking heads';
- bevestiging rolverdeling en bevoegdheden;
- wanneer spreken we elkaar weer;
- bevestigen wie contactpersoon is vanuit het getroffen departement/regio/gemeente/organisatie, bereikbaar voor 1 contactpersoon vanuit het rijk;
- bespreken we of er liaisons uitgewisseld worden.

Er vindt daarnaast veelvuldig afstemming plaats met afgevaardigden vanuit Rijk-Regio via appgroepen als WhatsApp, Signal en Threema.

Rol aangewezen CERTs, OKTTs en het NCSC

NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC is het nationale CERT, dat in het bijzonder bijstand verleent aan de Rijksoverheid en vitale aanbieders bij digitale dreigingen en incidenten. Daarbij kan het NCSC waar nodig schakelen met SOCs en de CERTs van o.a. doelgroeporganisaties en partijen binnen het landelijk dekkend stelsel.
Het NCSC kan met inachtneming van de toepasselijke wettelijke kaders (Avg, Wbni), vervolgens ook informatie verstrekken aan:

- bij ministeriële regeling aangewezen computercrisisteams;
- organisaties die kenbaar tot taak hebben om andere organisaties of het publiek te informeren (OKTTs);
- CSIRTs (CSIRT voor digitale diensten, CSIRTs van EU-lidstaten);
- Aanbieders van internettoegang- en internetcommunicatiediensten.

Deze organisaties zetten na ontvangst deze informatie, voor zover relevant, door naar hun doelgroeporganisaties die buiten de doelgroep van het NCSC vallen, of verrijkt deze informatie met relevante informatie voor hun specifieke doelgroep. Bij dreigingen of incidenten betreffende netwerk- en informatiesystemen van enkele categorieën digitale dienstverleners (online marktplaatsen, etc.) verleent het CSIRT-DSP (EZK) bijstand.

Internationaal

Het NKC stemt tijdens een incident dat de landsgrenzen overschrijdt, de crisiscommunicatie af met andere Europese lidstaten via het Crisis Communications Network, met vertegenwoordigers van alle EU-lidstaten en EU-organen, en het Benelux Crisis Centre Communication.

Contactgegevens

Het Nationaal Crisiscentrum (NCC), en daarmee de nationale crisiscommunicatiecollega's, zijn 24 uur per dag bereikbaar via ***070 - 751 51 51***.

Bijlage 2: Communicatiepartners bij digitale incidenten

We houden vast aan bestaande structuren, rollen en werkwijzen, met oog voor het bijzondere dat een cybercomponent met zich meebrengt.

- Iedere betrokken partij communiceert vanuit eigen verantwoordelijkheid over eigen onderwerpen, maar stemt centraal af over timing en inhoud van de boodschap.
- Iedere betrokken partij communiceert over de eventuele gevolgen voor de eigen dienstverlening.
- Berichtgeving van een partner wordt zoveel mogelijk ondersteund door de andere partijen door elkaar bijvoorbeeld te quoten en berichtgeving door te sturen (denk aan retweeten).

Nationaal Cyber Security Centrum (NCSC)	Het NCSC informeert, geeft duiding en adviseert over bij digitale dreigingen en incidenten aan organisaties binnen de rijksoverheid en vitale aanbieders als belangrijkste groep; andere partijen informeert het NCSC via het Landelijk Dekkend Stelsel. Het NCSC heeft een nationale, coördinerende rol op het gebied van digitale veiligheid en werkt bij een nationale cybercrisis nauw samen met NCC.
NCTV/ Nationaal Crisis Centrum (NCC)	Bij een nationale cybercrisis is het NCC (onderdeel van de NCTV) informatieknooppunt en 24/7 beschikbaar voor hulp, vragen en afstemming. Er is sprake van een nationale crisis wanneer een digitaal incident een ontwrichtend effect heeft op de samenleving of als één of meer van de vitale belangen wordt aangetast. Het NCC kan zelfstandig of op verzoek van de betrokken regio's, ministeries of vitale partners een coördinerende rol oppakken richting betrokken veiligheidsregio's en landelijke partners.
Nationaal Kernteam Crisiscommunicatie (NKC)	Nationaal Kernteam Crisiscommunicatie is actief bij incidenten met effect op nationale veiligheid of met grote maatschappelijke impact. In het NKC vindt afstemming plaats met regionaal, lokaal via liaisons over de timing en inhoud van communicatieboodschap.
Veiligheidsregio	Afhankelijk van de (verwachte) ernst van de situatie, opschalen van (onderdelen van) de crisisorganisatie en de crisiscommunicatie-organisatie. Zijn er meerdere betrokken veiligheidsregio's en er is geen duidelijke aanwijsbare incidentregio, dan is het verstandig om (in overleg) een coördinerende veiligheidsregio aan te wijzen, waarbij de communicatieadviseurs van betrokken partners kunnen aansluiten. De Veiligheidsregio verzorgt de pers –en publiekscommunicatie voor de eigen regio.

Digital Trust Centre (DTC)	Het DTC informeert het niet-vitale bedrijfsleven over de crisis. Indien nodig 'vertaalt' zij de boodschap voor vitaal naar niet-vitaal en verspreidt een zo concreet mogelijk begrijpelijk handelingsperspectief via haar eigen online kanalen en samenwerkingsverbanden.
Gemeente / Burgemeester	De burgemeester of voorzitter Veiligheidsregio is verantwoordelijk voor aanpak van de effecten van de verstoring op de openbare orde en veiligheid.
Algemene Inlichtingen- en Veiligheidsdienst (AIVD)	Activiteiten en dreigingen door statelijke actoren worden geduid door de AIVD. Daarnaast biedt het Nationaal Bureau voor Verbindingsbeveiliging (NBV) als onderdeel van de AIVD handelingsperspectief waar ICT-beveiliging voor nationale veiligheid van van belang is in relatie tot statelijke actoren. Ook houdt het NBV binnen Nederland toezicht op de bescherming van gerubriceerde NAVO- en EU-informatie.
De Informatie Beveiligingsdienst (IBD)	De Informatie Beveiligingsdienst (onderdeel van de VNG) is de sectorale CERT/CSIRT voor alle Nederlandse. De IBD ondersteunt gemeenten bij (dreigende) incidenten en crisissituaties op het vlak van informatiebeveiliging. Ook is de IBD voor gemeenten het schakelpunt met het NCSC.
Politie	De politie is samen met het Openbaar Ministerie verantwoordelijk voor communicatie over het opsporingsonderzoek (wanneer er sprake is van (verdenking) van moedwillig veroorzaken van een digitaal incident). De politie communiceert tevens over incidenten met een openbare orde- of opsporingscomponent die ten gevolge van het digitale incident zijn ontstaan.
Openbaar Ministerie	Vanaf het moment dat een verdachte wordt voorgeleid aan de rechtercommissaris neemt het OM de woordvoering voor zijn rekening. Het OM stemt hierover af met de Politie en bespreekt dit eventueel in de driehoek en/of op landelijk niveau.
Vitale aanbieders	Als zodanig aangewezen aanbieders van diensten in de vitale processen zoals energie, drinkwater, keren en beheren, ICT/telecom, financiën, chemie, nucleair en vervoer, zijn verplicht om ernstige ICT-incidenten in hun vitale processen te melden aan het NCSC. Aanbieders van vitale processen communiceren via de eigen communicatiemiddelen over de storing, de verwachte duur daarvan, herstelwerkzaamheden en handelingsperspectieven.
Autoriteit Persoonsgegevens	Als een datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen, zijn organisaties verplicht om een datalek te melden bij de AP.

Bijlage 3: Crisiscommunicatie checklist bij digitale incidenten

Afspraken & contacten

- Bekend met eigen taak en rol.
- Afspraken over (tijdige) opschaling en wijze van afstemming bekend.
- Overzicht (in –en externe) communicatiepartners, inclusief e-mailadres en (piket) nummer.
- Piketnummer NCTV crisiscommunicatie opgeslagen: 070 - 751 51 51.
- Lijstje met (in-en externe) experts/deskundigen voor duiding technische informatie.
- Communicatievertegenwoordiging in crisisteam geregeld.
- Inzicht in (crisis)communicatiestructuren.
- Aansluiting operationele collega's.
- Maak gebruik van technische communities.

Inhoud boodschap

- Handelingsperspectieven voorbereid.
- Procesinformatie voorbereid.
- Weet wat te doen bij desinformatie, *fake news*.
- Gedragsadviezen voorbereid.
- Basis kernboodschap(pen) paraat.

Communicatiemiddelen

- Beelden (visuals/ infographics etc.) op de plank die ingewikkelde materie begrijpelijk maken.
- Plan B voor bij uitval van digitale communicatiemiddelen paraat.
- Webcare ingericht.

Onderzoek

- Omgevingsanalyses uitgevraagd.
- Onderzoek (0-meting/ flitspeiling) of vragenlijst voorbereid.

Intern

- Interne communicatie in het vizier.
- Inzicht in communicatieve vraagstukken, dilemma's en beslispunten.
- Zowel communicatieve als bestuurlijke dilemma's.
- Check timing van je boodschap.

Doelgroepen

- Moeilijk bereikbare doelgroepen inzichtelijk.
- Rekening gehouden met begrijpelijke, eenvoudige taal.
- Overweeg vertalingen in meerdere talen.

Bijlage 4: Bouwblokken kernboodschappen

De exacte elementen, opbouw en toonzetting van een kernboodschap zijn sterk afhankelijk van de aard, omstandigheden, verwacht verloop en omvang van een (dreigende) crisis. Belangrijk in elke kernboodschap is: probeer zo concreet mogelijk te zijn en vertaal lastige (technische) informatie naar duidelijke taal. Als handvat voor kernboodschappen is onderstaand model te gebruiken, met dank aan de collega's van Rijkswaterstaat.

- **We know:**
  Dit is wat we weten/kunnen zeggen
- **We do:**
  Dit is wat we doen én dit is wat u moet/kunt doen; handelingsperspectief.
  Let op: geef geen inzicht in technische maatregelen (dat maakt opnieuw kwetsbaar). Benoem hier alleen de maatregelen die merkbaar/zichtbaar zijn.
- **We care:**
  Dit voelen we erbij (zeker als er sprake is van slachtoffers / grote overlast)
- **We will get back:**
  We komen op moment x bij u terug

Bij een digitale dreiging

We know:
[organisatie] heeft bekendgemaakt dat er in [software/systeem] een serieuze kwetsbaarheid zit. De software [uitleg wat het doet]. Ook [organisatie] maakt gebruik van deze software.

Door deze kwetsbaarheid kunnen kwaadwillenden [impact]

We do:
[technici/specialisten van ....] onderzoeken hoe groot het risico is. Op advies van [organisatie] hebben we [maatregelen genomen]. We adviseren medewerkers/ klanten/burgers [handelingsperspectief digitaal].

We care:
We realiseren ons dat deze kwetsbaarheid ook onzekerheid met zich meebrengt. We doen er alles aan om daar zo snel mogelijk duidelijkheid over te verkrijgen.

We will get back:
We werken nauw samen met [organisaties] aan de oplossing van dit probleem. Zodra er een update beschikbaar is, zullen we die zo snel mogelijk delen. De volgende update verwachten we daarom om [tijd] uur. Deze update delen we via [kanalen].

Digitaal incident met beperkte gevolgen

We know:
[organisatie] is slachtoffer geworden van [aard van het probleem]. In [software/ systeem] is er sprake van [aard van het probleem} Hierdoor [impact beschrijven die waarneembaar is].

We do:
Op dit moment werken onze technici samen met [betrokken organisaties] aan een oplossing van de problemen. [evt verwachting wanneer is opgelost]. We hebben daartoe de volgende maatregelen [zichtbaar en evt onzichtbaar] getroffen. We adviseren medewerkers/klanten/burgers [handelingsperspectief digitaal en/of fysiek].

We care:
We realiseren ons dat mensen veel [overlast/onzekerheid] ondervinden. We doen er alles aan om de problemen zo snel mogelijk te verhelpen.

We will get back:
We werken nauw samen met [organisaties] aan de oplossing van dit probleem. Zodra er nieuwe informatie beschikbaar is, zullen we die zo snel mogelijk delen via [kanalen].

Digitale crisis met maatschappelijke ontwrichting

We know:
Ook [organisatie] is slachtoffer geworden van [aard van het probleem]. In [software/ systeem] is er sprake van [aard van het probleem} Hierdoor [impact beschrijven die waarneembaar is].

We do:
Op dit moment werken onze technici samen met [betrokken organisaties] aan een oplossing van de problemen. [evt verwachting wanneer is opgelost]. Om deze situatie zo snel mogelijk op te lossen en verdere impact te beperken, is binnen [organisatie] de crisisorganisatie geactiveerd. [Eventueel iets opnemen over (Rijks) brede crisisstructuur].

We hebben inmiddels de volgende maatregelen [zichtbaar en evt onzichtbaar] getroffen. We adviseren medewerkers/klanten/burgers [handelingsperspectief digitaal en/of fysiek]. [oproep tot solidariteit en omkijken naar mensen die minder zelfredzaam zijn]

We care:
We realiseren ons dat de problemen grote gevolgen hebben voor alle getroffenen. We richten onze hulp nu eerst op [primair getroffenen] omdat [reden van prioritering]. We doen er alles aan om de problemen voor iedereen zo snel mogelijk te verhelpen.

We will get back:
We werken nauw samen met [organisaties] aan de oplossing van dit probleem. Ga voor de meest recente informatie en hulp naar [organisatie] . Zodra er nieuwe informatie beschikbaar is, zullen we die zo snel mogelijk delen via [kanalen]. Houd u ondertussen de berichtgeving van [(nieuws)organisatie] in de gaten.

Bijlage 5: Afkortingenlijst

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CERT	Computer Emergency Response Team
CIO-BERAAD	Overleg departementale Chief Information Officers
CSIRT	Cyber Security and Incident Response Team
DCC	Defensie Cyber Commando / Departementaal Coördinatiecentrum
DTC	Digital Trust Centre
EGC	European Government CERTs group
EZK	Ministerie van Economische Zaken en Klimaat
ENISA	European Network & Information Security Agency
FIRST	Forum of Incident Response and Security Teams
ICCb	Interdepartementale Commissie Crisisbeheersing
ICT	Informatie- en communicatietechnologie
IAO	Interdepartementaal Afstemmingsoverleg
IRB	ICT Response Board
ISAC	Information Sharing & Analysis Center
IWWN	International Watch and Warning Network
JenV	Ministerie van Justitie en Veiligheid
LCMS	Landelijk Crisis Management Systeem
LDS	Landelijk Dekkend Stelsel
LOCC	Landelijk Operationeel Coördinatiecentrum

MCCb	Ministeriële Commissie Crisisbeheersing
NCC	Nationaal Crisiscentrum
NCSA	Nederlandse Cybersecurity Agenda
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NKC	Nationaal Kernteam Communicatie
NLCS	Nederlandse Cybersecurity Strategie
NRN	Nationaal Respons Netwerk
NVB	Nationaal Bureau voor Verbindingsbeveiliging van de AIVD
NVS	Nationale Veiligheid Strategie
NSGBO	Nationale Staf Grootschalig en Bijzonder optreden
OKTT	Organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren.
OM	Openbaar Ministerie
SOC	Security Operations Centre
SOP	Standard Operating Procedure
SSO	Shared Service Organisatie
VNG	Vereniging Nederlandse Gemeenten
VR	Veiligheidsregio