Koepelnotitie

Communicatie bij digitale incidenten

Februari 2021

Inhoud

1. Inleiding

incidenten kunnen onze maatschappij in het hart raken en gedurende korte of langere tijd verlammen. Met enige regelmaat worden we opgeschrikt door incidenten die aantonen hoe groot de impact van een digitale storing of aanval kan zijn. De kwetsbaarheden in Citrix-producten, de onbereikbaarheid van 112 door een storing bij KPN en ransomware-aanvallen zoals op de Universiteit Maastricht zijn voorbeelden daarvan.

Natuurlijk biedt digitalisering ongekende kansen. Het zorgt ervoor dat bedrijven, onderwijsinstellingen en organisaties hun activiteiten tijdens de Covid-19 crisis grotendeels door kunnen laten gaan. De keerzijde is dat de digitale ruimte zwaarder dan ooit belast wordt en grootschalige digitale uitval of verstoring forse schade kan aanrichten.

Door de permanente digitale dreiging en potentieel maatschappij-ontwrichtende gevolgen moeten we blijvend aandacht hebben voor onze digitale weerbaarheid. Het Nationaal Crisisplan Digitaal biedt daar handvatten voor. Het helpt de vertaalslag te maken van de crisisaanpak op nationaal niveau naar operationeel uitgewerkte plannen en draaiboeken voor uw eigen organisatie.

Zoals in het NCP Digitaal staat: voor het bewaken van onze digitale veiligheid moeten we allemaal in beweging komen. Dat geldt ook voor communicatieprofessionals. Deze communicatienotitie is een verdere verdieping van het hoofdstuk Communicatie uit het NCP Digitaal. Het biedt handvatten om goed voorbereid te zijn voor het moment dat het nodig is. Want digitale crisis kennen eigen uitdagingen. Ze overschrijven razendsnel fysieke grenzen, zijn vaak minder goed te duiden voor een publiek en er is vaak meer tijd nodig voor een analyse van wat er nu eigenlijk aan de hand is. Dat laatste maakt snelle besluitvorming lastig en dat heeft weer direct gevolgen voor de communicatie.

Kortom, de uitdagingen voor communicatieprofessionals zijn groot als een digitaal incident zich voordoet. Een goede voorbereiding is dus noodzakelijk. Deze notitie helpt communicatieprofessionals die een rol hebben in de (crisis)communicatie bij digitale uitval, zowel op nationaal als op regionaal/lokaal niveau. Met dank aan de samenwerkingspartners met wie deze communicatienotitie tot stand is gekomen: de G4, NCTV, NCSC, BZK, EZK, IenW, Politie en vertegenwoordigers namens de Veiligheidsregio's en het OM.

Leeswijzer

De notitie start met uitgangspunten van crisiscommunicatie in het algemeen. Vervolgens zoomen we in op wat specifiek voor digitale incidenten van belang is als het gaat om crisiscommunicatie. Tot slot maken we expliciet wie waarvoor aan de lat staat op het moment dat het misgaat, en een digitaal incident leidt tot problemen in de fysieke wereld.

2. Crisiscommunicatie (algemeen)

Algemene uitgangspunten

In een tijd waarin door social media informatie (of die nu waar of niet waar is) binnen enkele minuten massaal gedeeld kan worden, zijn heldere uitgangspunten over communicatie 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.

- Communicatie is in eerste instantie gericht op schadebeperking, vervolgens op het beantwoorden van de maatschappelijke informatiebehoefte en betekenisgeving.
- Communicatie is omgevingsbewust, proactief, open, tijdig en consistent.
- Communiceer over het proces (wat is er al bekend en wat nog niet, stappen die de overheid zichtbaar maken) en communiceer wat de burger moet doen/laten of wil weten.
- We communiceren over zichtbare maatregelen en indien wenselijk/mogelijk ook over onzichtbare maatregelen (daarmee vertellen we wat we doen en bouwen we aan het vertrouwen in de overheid).
- Bevestig wat zichtbaar is, vertel wat je wel en wat je niet weet, ontkracht geruchten of laat weten dat je de geruchten kent en ze onderzoekt. Geef een handelingsperspectief mee: wat kunnen mensen doen?
- Communiceer zonder afstemming niet over SISOS: slachtoffers, identiteiten, scenario's, oorzaken en schade.

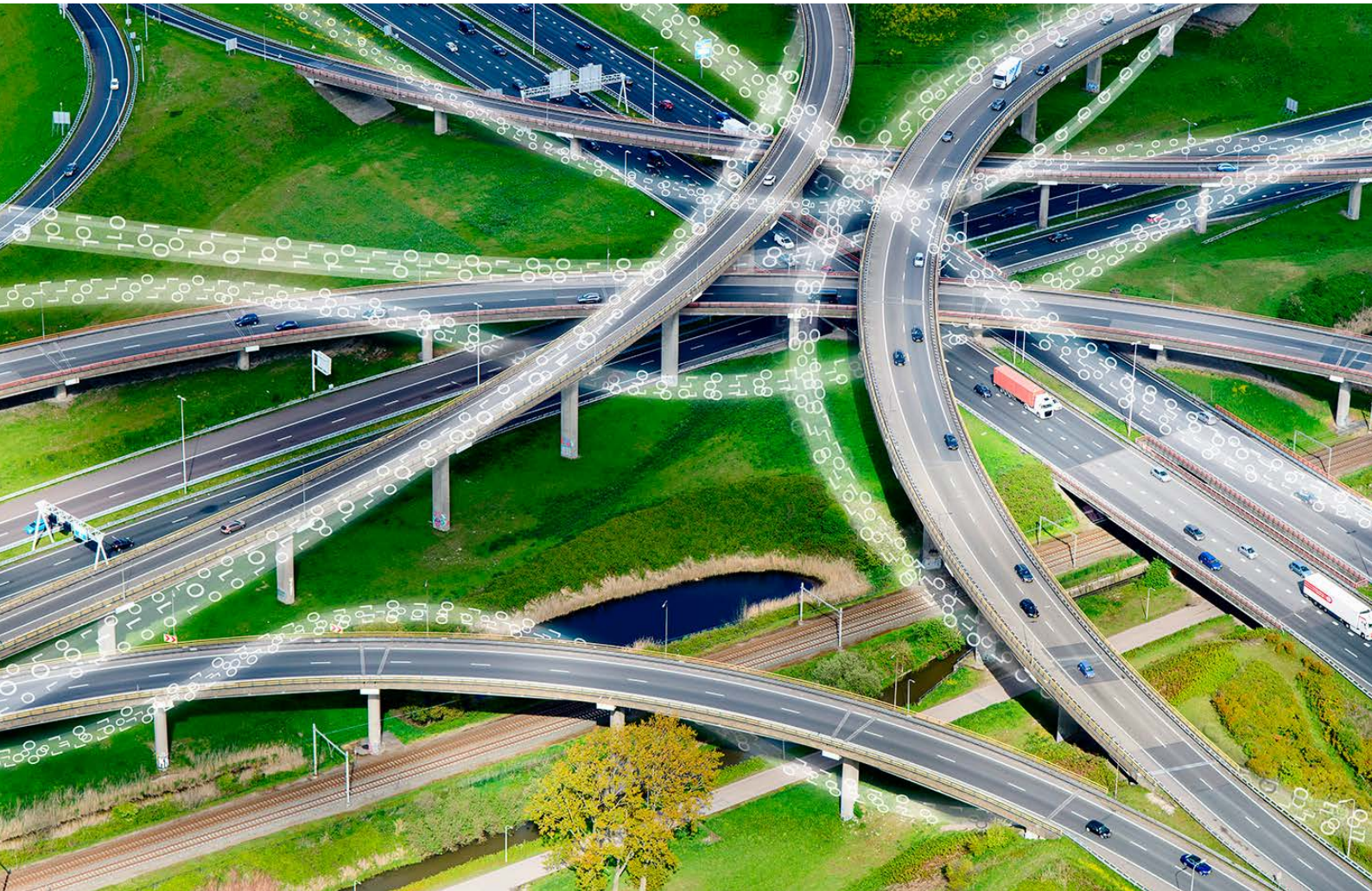
3. Crisiscommunicatie bij digitale incidenten

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. 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.

Hét uitgangspunt voor de organisatie van de crisiscommunicatie bij maatschappelijke ontwrichting als gevolg van digitale incidenten: we hebben oog voor het bijzondere dat een incident in het digitale domein met zich meebrengt maar houden wel vast aan bestaande structuren, rollen en werkwijzen.

Daarnaast houden we rekening met het volgende:

- Zolang niet zeker is of een incident opzettelijk handelen is, vermijden we verwijzingen naar mogelijke oorzaken, duur en omvang;
- Geef waar mogelijk procesinformatie. Het duurt soms lang voordat duidelijk is wat er precies aan de hand is;
- Wanneer vanuit veiligheidsoverwegingen communicatie over (technisch 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’);
- Communicatie van bestuurders verbindt de samenleving en doet een beroep op de veerkracht van individuele burgers en van de Nederlandse samenleving als geheel.



4. Aansluiten bij scenario's uit NCP 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 Nationaal Crisisplan Digitaal gekozen voor een aanpak op basis van enkele 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 drie hoofdvragen te beantwoorden:

1. Wat zijn de belangrijkste mogelijke (in)directe gevolgen en effecten?
2. Welke maatregelen (handelingsperspectief) zijn nodig om de gevolgen en effecten te voorkomen of te beheersen?
3. Welke partijen zijn betrokken c.q. nodig voor een adequate aanpak?

Houd bij deze denkexercitie rekening met:

- Tijdige escalatie
- Reputatieschade
- Uitval middelen
- Maatschappelijke onrust
- Uitval dienstverlening
- Door grote afhankelijkheid mogelijk cascade effecten
- Weinig zichtbare gevolgen, mogelijk impact groot, hoe urgentie laten zien?
- Oplostijden vaak onbekend
- Politieke druk
- Grensoverschrijdend
- Welke dilemma's kunnen er langs komen?

Tips voor de voorbereiding van de crisiscommunicatie

- Maak een overzicht van je communicatiepartners. Deze zijn vaak anders dan bij een fysieke crisis. Wellicht zijn het er meer, vanwege digitale en fysieke effecten.
- Zorg voor aansluiting bij de operationele collega's die zich met digitale incidenten bezig houden.
- Bereid een lijstje met (in-en externe) experts/deskundigen voor die technische informatie kunnen duiden tijdens een incident. Want crisiscommunicatie bij incidenten met een cyber component vraagt veelal om de vertaling van technische termen en uitleg van processen.
- Zorg dat je inzicht hebt (voor zover mogelijk) in de acht incidentscenario's uit het NCP Digitaal die jouw organisatie/domein zouden kunnen treffen.
- Zoek uit aan welke specifieke expertise je behoefte hebt, welke kennis je nu mist, wat je nodig hebt om te kunnen communiceren.
- Maak goede afspraken over (tijdige) opschaling en wijze van afstemming.
- Zorg voor communicatievertegenwoordiging in de crisisteams van de eigen organisatie.
- Verkrijg inzicht in communicatieve vraagstukken, dilemma's en beslispunten.
- Beoefen en doorleef de verschillende scenario's bijvoorbeeld door een tabletop.
- Maak een plan B uitval van digitale communicatiemiddelen.
- Denk na over hoe beeld (visuals, infographics etc.) kan bijdragen om duiding, en handelingsperspectief over vaak ingewikkelde technische materie, begrijpelijk te communiceren.

Tips voor uitvoering van de crisiscommunicatie

- Denk na over de timing van je boodschap. Breng zoveel mogelijk zelf het nieuws naar buiten
- Deel wat je al wél weet (procesinformatie)
  - Cyberanalyses kosten relatief meer tijd dan in fysieke wereld. Het duurt vrij lang om scenario's te kunnen wegstrepen.
- Beschrijf wat er anders is bij een ICT-crisis:
  - Attributie
  - Analyse/ duiding
  - Bestrijden verdere verspreiding (domino-effecten)
- Geef zodra het kan een handelingsperspectief
- Visualiseer ingewikkelde technische materie
- Formuleer een kernboodschap. Maak hierbij – indien nodig- je communicatiedilemma's bekend.
- Houd direct rekening met het ergste:
  - Bij uitval van digitale middelen is de maatschappelijke impact / ontwrichting al snel groot.
  - Heb oog voor de mogelijke domino-effecten / cascade effecten. Deze zijn al snel merkbaar.
- Gebruik beeld om je technische verhaal te ondersteunen. Denk hierbij aan film, visuals en infographics, afgestemd per doelgroep.
- Vergeet interne communicatie niet: ook medewerkers communiceren mogelijk naar buiten/partners.

5. Verantwoordelijkheden

Crisiscommunicatie bij incidenten in het digitale domein volgt de reguliere bevoegdheden en verantwoordelijkheden. Iedere betrokken partij communiceert dus vanuit de eigen verantwoordelijkheid over eigen onderwerpen, maar stemt (indien ingezet in het NKC) af over timing en inhoud van de boodschap.

In de tabel hieronder staan de reguliere communicatieverantwoordelijkheden zoals die altijd gelden. Ze beschrijven op hoofdlijnen wie waarover communiceert. Deze rolverdeling blijft gelden bij de opschaling van de nationale crisisstructuur. De afspraak om timing en inhoud van boodschappen af te stemmen geldt in alle gevallen.

Communicatie over	Verantwoordelijk
Feiten lokaal	Hulpverleningsdiensten
Duiding en handelingsperspectief lokaal	Burgemeester binnen driehoek/ Voorzitter veiligheidsregio (bij opzettelijk handelen scenario)
Handhaving openbare orde en veiligheid	Burgemeester / Voorzitter Veiligheidsregio
Veiligheidsmaatregelen lokaal	Burgemeester / Voorzitter Veiligheidsregio (maatregelen openbare orde) en OM (maatregelen in het kader van opsporing)
Duiding Nationale Veiligheid en veiligheidsmaatregelen algemeen	NCTV (en/of MinJenV zelf als coördinerend minister op cybersecurity en verantwoordelijk voor nationale crisisstelsel)
Duiding maatregelen technisch operationeel en handelingsperspectief voor de eigen doelgroep/ organisatie	NCSC, CERT- en SOC-organisaties
Duiding activiteiten en dreigingen door statelijke actoren. Handelingsperspectief waar ICT-beveiliging voor nationale veiligheid van belang is (via NBV).	AIVD
Opsporingsonderzoek	Openbaar Ministerie
Feiten en duiding; handelingsperspectieven nationaal/ sectoraal	Betrokken vakminister
Gevolgen voor eigen organisatie en medewerkers, directe gevolgen voor klanten of leveranciers.	Publieke en private partijen

6. 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. In een aantal scenario's zullen ook Buitenlandse Zaken, I&W, EZK, Defensie en SZW aansluiten.

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, 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.

Ook betekent het dat het NKC het aanspreekpunt voor communicatie op rijksniveau is. Het NKC coördineert en verzorgt actief de afstemming met veiligheidsregio's, gemeenten en andere betrokken partijen, zoals NCSC, IBD. Communicatiedilemma's op rijksniveau worden beslecht in het NKC en indien nodig in de ICCb of MCCb.

Aansluiting communicatie op sturingslijnen en informatielijnen

Het NKC is onderdeel van de nationale crisisstructuur via een vertegenwoordiger in de ICCb en de MCCb. 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 in contact met het NKC.

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 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 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 we wie contactpersoon is vanuit de getroffen departement/regio/gemeente/organisatie; bereikbaar voor een contactpersoon vanuit het Rijk;
- bespreken we of er liaisons uitgewisseld worden.

Rol aangewezen CERTs, OKTTs en het NCSC

Is er sprake van een dreiging of een incident in netwerk- en informatiesystemen van vitale aanbieders, onderdelen van het Rijk, of de tijdelijk in de Wet beveiliging netwerk- en informatiesystemen (Wbni) genoemde organisaties, dan verleent het NCSC bijstand (informeren, adviseren, etc.) aan deze organisaties. Daarbij kan het NCSC voor zover mogelijk schakelen met de SOCs/CERTs van deze doelgroeporganisaties.

Het NCSC kan met inachtneming van de toepasselijke wettelijke kaders (Avg, Wbni), vervolgens ook 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. Bij dreigingen of incidenten betreffende netwerk- en informatiesystemen van enkele categorieën digitale dienstverleners (online marktplaatsen, etc.) verleent het CSIRT voor digitale diensten (EZK) bijstand.

Rol 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 belang is. Ook houdt het NBV binnen Nederland toezicht op de bescherming van gerubriceerde NAVO- en EU-informatie.

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 1: Communicatiepartners bij cyberincidenten

Uitgangspunt is en blijft dat we vasthouden 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.
- 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)	• Bijstand (informeren, adviseren, etc.) bij digitale dreigingen en incidenten betreffende systemen van rijksoverheid en vitale aanbieders; informeren van andere partijen (bv. AIVD) over die dreigingen en incidenten. • Verdere versterking van de digitale weerbaarheid van Nederland, door bv. algemene advisering en doorverstrekking van informatie aan schakelorganisaties. • Coördinerende rol (op cybersecurity) bij een nationale cybercrisis in samenwerking met NCC. 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. • Delen van informatie om digitale weerbaarheid van Nederland te versterken. • Database met hulpmiddelen: advisory's, factsheets, checklists, handreikingen etc.
NCTV/ Nationaal Crisis Centrum (NCC)	• Het NCC is informatieknooppunt en 24/7 beschikbaar voor hulp, vragen en afstemming. • 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 is actief bij incidenten met effect op nationale veiligheid of met grote maatschappelijke impact. Afstemming met regionaal, lokaal via liaisons over de timing en inhoud van communicatieboodschap.
Veiligheidsregio	• afhankelijk van de (verwachte) ernst van de situatie, synchroon of Asynchroon opschalen van (onderdelen van) de crisisorganisatie en de crisiscommunicatieorganisatie. • Indien er sprake is van meerdere betrokken veiligheidsregio's en er is geen duidelijke aanwijsbare incidentregio, wijs (in overleg) een coördinerende veiligheidsregio aan, waarbij de communicatieadviseurs van betrokken partners kunnen aansluiten.
Gemeente / Burgemeester	• De burgemeester of voorzitter Veiligheidsregio is verantwoordelijk voor aanpak van de effecten van de verstoring op de openbare orde en veiligheid. • Informatiebeveiligingsdienst voor gemeenten.
De Informatie Beveiligingsdienst (IBD)	• De Informatie Beveiligingsdienst is de sectorale CERT/CSIRT voor alle Nederlandse gemeenten en onderdeel van de VNG. De IBD ondersteunt gemeenten op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het NCSC. • Het Computer Emergency Response Team (CERT) van de Informatiebeveiligingsdienst voor gemeenten (IBD) kan de gemeente ondersteuning leveren in geval van (dreigende) incidenten en crisissituaties op het vlak van informatiebeveiliging.

Politie	• De politie is verantwoordelijk voor communicatie over het opsporingsonderzoek (wanneer er sprake is van (verdenking) van moedwillig veroorzaken van een digitaal incident). • De politie communiceert over incidenten met een openbare orde- of opsporingscomponent die door 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 Openbaar Ministerie 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 eigencommunicatiemiddelen 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

Bijlage 2: 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
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
LDS	Landelijk Dekkend Stelsel
LOCC	Landelijk Operationeel Coördinatiecentrum
LSGBO	Landelijke Staf Grootschalig en Bijzonder Optreden
MCCb	Ministeriële Commissie Crisisbeheersing
NCC	Nationaal Crisiscentrum
NCSA	Nederlandse Cybersecurity Agenda
NCSC	Nationaal Cyber Security Centrum
NCSS	Nationale Cyber Security Strategie
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NKC	Nationaal Kernteam Communicatie
NRN	Nationaal Respons Netwerk
NSGBO	Nationale Staven Grootschalig en Bijzonder Optreden
NVS	Nationale Veiligheid Strategie
OKTT	Organisatie die objectief kenbaar tot taak heeft andere organisaties of het publiek te informeren.
OM	Openbaar Ministerie
SOP	Standard Operating Procedure
SSO	Shared Service Organisatie
VNG	Vereniging Nederlandse Gemeenten
VR	Veiligheidsregio

Eenheid Communicatie NCTV
communicatie@nctv.minjenv.nl

Februari 2021 | Publicatie-nr. 21400527