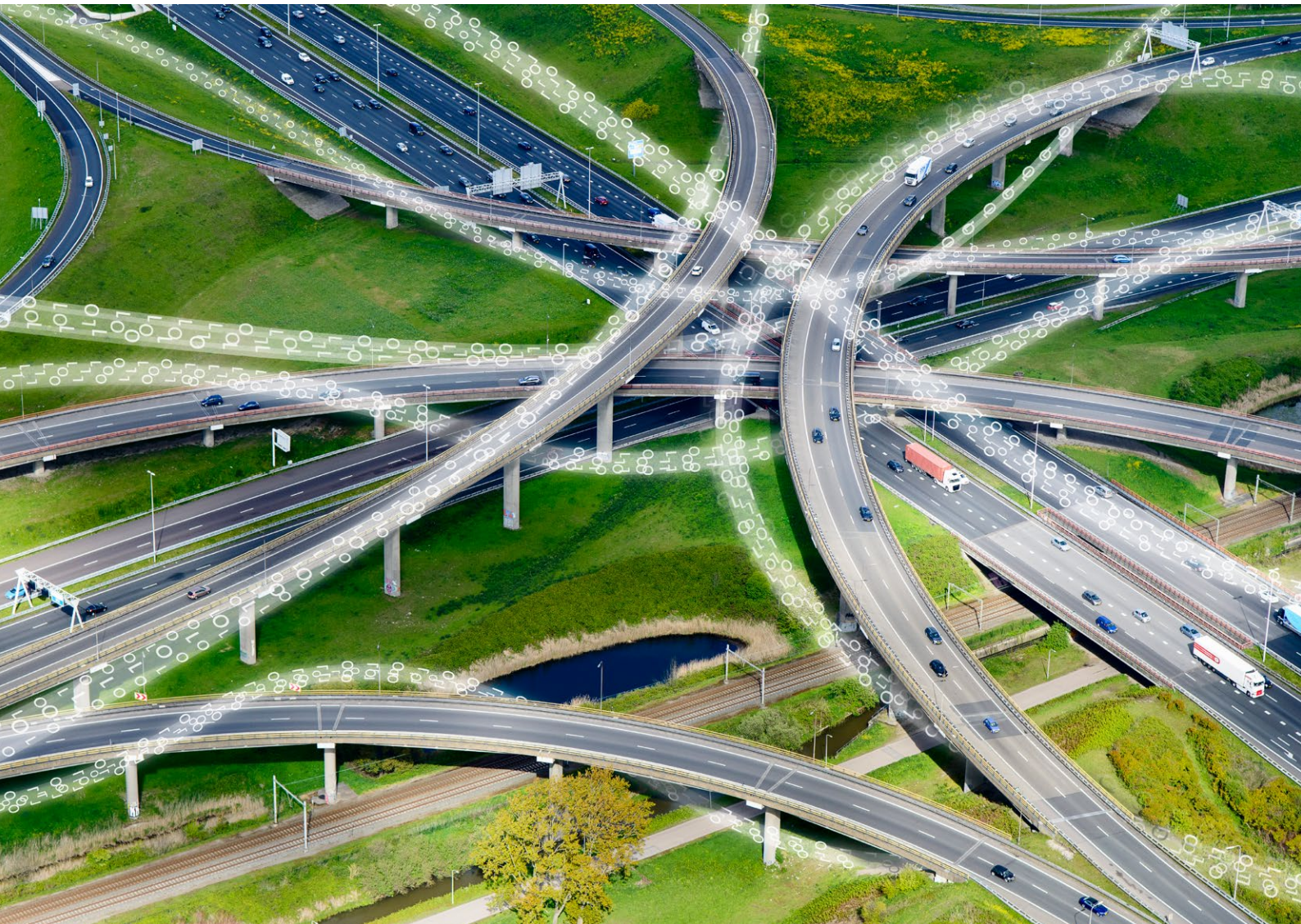
Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Nationaal Crisisplan Digitaal



Inhoudsopgave

Toegestane verspreiding TLP: WHITE
(Traffic Light Protocol)

Dit document heeft het label TLP: WHITE. Het NCTV gebruikt het Traffic Ligth Protocol (TLP) om eenduidig te definiëren wat er met informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard van First (www.first.org/tlp). Ontvangers mogen de informatie uit deze handreiking delen binnen en buiten hun organisatie, daarnaast mag informatie publiek gemaakt worden.

Uw reacties zijn welkom op info@nctv.minjenv.nl.

Voorwoord

Ons land drijft op digitale systemen. Die technische vooruitgang is mooi, maar tegelijkertijd ook zorgelijk om te zien. Het maakt onze fysieke wereld kwetsbaar: een klein digitaal incident kan al grote gevolgen hebben voor ons maatschappelijke leven. Al is het maar een doorgebrande kabel of onbeveiligde server. Kortom, digitale veiligheid vereist aandacht, alertheid en aanpak. Een versterkte aanpak, die we blijven bijstellen om onze digitale en daarmee onze nationale veiligheid te beschermen, zoals we ook beschreven in de Nationale Veiligheid Strategie 2019.

Dagelijks heeft ons land te maken met digitale dreigingen. Het Cyber Security Beeld Nederland 2019 concludeert zelfs dat die dreiging voor de nationale veiligheid permanent is. En hoewel de NCTV samen met haar partners sterk inzet op het verhogen van onze digitale weerbaarheid om maatschappelijke ontwrichting te voorkomen, kan het onverhoopt toch misgaan. Sterker nog, digitale aanvallen en incidenten volgen elkaar steeds sneller op. Denk aan de KPN-storing met landelijke impact op 112, de ransomwareaanval op de Universiteit Maastricht of de Citrix-problematiek die onder andere het Medisch Centrum Leeuwarden digitaal hermetisch afsloot en ook de Rijksoverheid tot verregaande maatregelen dwong. Hiernaast zijn er nog tal van scenario's mogelijk met doorwerking in het fysieke domein die een adequate crisisaanpak vereisen. Allemaal met een gezamenlijk doel: schade beperken en snel herstel.

Dit 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. Dat gebeurt aan de hand van zes bouwstenen waarmee u een eigen specifiek crisisscenario kunt samenstellen. Vervolgens kunt u bekijken welke dynamiek dat met zich meebrengt voor uw organisatie en er consequenties aan koppelen.

Het plan leent zich daardoor ook goed voor oefeningen. Samen voorbereiden en oefenen is per slot van rekening noodzakelijk voor een effectieve crisisbeheersing. Mijn advies is dan ook om met de verschillende bouwstenen een scenario te creëren dat bij uw organisatie past en daar met elkaar mee aan de slag te gaan. Als Nationaal Coördinator Terrorismebestrijding en Veiligheid geef ik graag het goede voorbeeld: ook wij gebruiken dit plan als basis voor de aanpak van digitale incidenten en oefeningen op nationaal niveau.

Niet alleen vraag ik u om in beweging te komen, ook wij blijven meebewegen met de snelle digitale ontwikkelingen die gaande zijn. We beschouwen dit Nationaal Crisisplan Digitaal dan ook als een levend document, waarvan we jaarlijks bezien of actualisering nodig is.

Dit Nationaal Crisisplan Digitaal is gerealiseerd in nauwe samenwerking met publieke en private partners. Veel dank aan allemaal. We hebben met elkaar een helder document neergezet waar ik trots op ben. En een plan dat moet aanzetten tot actie. Want voor het bewaken van onze digitale veiligheid moeten we allemaal in beweging komen.

Pieter-Jaap Aalbersberg
Nationaal Coördinator Terrorismebestrijding en Veiligheid


ABN·AMRO

1. Inleiding

De huidige samenleving is grotendeels afhankelijk geworden van digitale middelen. Het Cyber Security Beeld Nederland 2019 concludeert dat de digitale dreiging voor de nationale veiligheid permanent is. Vrijwel alle vitale processen en diensten zijn deels of volledig afhankelijk van netwerk- en informatie-systemen.

Door het bijna geheel verdwijnen van analoge alternatieven en de afwezigheid van terugvalopties is de afhankelijkheid van gedigitaliseerde processen en systemen zo groot geworden dat aantasting hiervan zal leiden tot maatschappij-ontwrichtende schade. Vitale processen zijn in hoge mate afhankelijk van elektriciteitsvoorziening en datacommunicatie. Uitval en verstoring hiervan, of van belangrijke processen in de samenwerkende keten(s), hebben zeer snel, binnen enkele uren, impact op een aantal vitale processen.[1]

Doel

Het Nationaal Crisisplan Digitaal (NCP-Digitaal) is een leidraad om op hoofdlijnen snel inzicht en overzicht te creëren in de bestaande afspraken op nationaal niveau over de beheersing van incidenten in de beveiliging van netwerk- en informatiesystemen met aanzienlijke maatschappelijke gevolgen. Het plan beschrijft op hoofdlijnen de crisisaanpak op rijksniveau en de samenwerking en aansluiting met betrokken publieke en private partners en netwerken op internationaal en regionaal niveau. Het plan is daarmee een uitwerking van de generieke aanpak van crises door het Rijk zoals beschreven in het Instellingsbesluit Ministeriële Commissie Crisisbeheersing en het Nationaal Handboek Crisisbesluitvorming.

Het NCP-Digitaal is een kaderstellend en overkoepelend plan voor de individuele, meer operationeel uitgewerkte plannen en draaiboeken van de betrokken actoren en organisaties. Het NCP-Digitaal vervangt de bestaande plannen van individuele organisaties of afspraken tussen organisaties niet. Deze plannen en draaiboeken moeten waar relevant wel in overeenstemming zijn met het NCP-Digitaal.

Het plan bevat een stappenplan om in een daadwerkelijke situatie, bij de voorbereiding daarop of tijdens een oefening de volgende drie hoofdvragen te beantwoorden:

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

Het voorliggende crisisplan is een herziening van het Nationaal Crisisplan ICT uit 2012, zoals aan de Tweede Kamer toegezegd in het kader van de Nederlandse Cyber Security Agenda 2018 en van de Agenda Risico- en Crisisbeheersing.[2]

Doelgroepen

Doelgroepen van dit plan zijn de actoren en organisaties binnen of direct verbonden aan de opgeschaalde nationale crisisstructuur die een rol hebben bij de beheersing van incidenten in de beveiliging van netwerk- en informatiesystemen met aanzienlijke maatschappelijke gevolgen. Dat betreft medewerkers, leidinggevenden en bestuurders van alle actoren en organisaties die binnen de opgeschaalde nationale crisisorganisatie[3] een rol kunnen hebben. Dit zijn onder andere de betrokken ministeries en specifieke organisaties in het digitale domein bij de Rijksoverheid zoals het Nationaal Cyber Security Centrum (NCSC). Daarnaast is het ook bedoeld voor andere organisaties om hun eigen voorbereiding en planvorming daarop af te stemmen en daarmee in overeenstemming te brengen, zoals veiligheidsregio's, politie, inlichtingen- en veiligheidsdiensten en private partners.

1 *Nationale Veiligheid Strategie 2019* (TK 2018-2019, 30 821, nr. 81).

2 *Nationale Cyber Security Agenda 2018* (TK 2017-2018, 26 643, nr. 536) en *Agenda risico- en crisisbeheersing* (TK 2018-2019, 30 821, nr. 50).

3 De nationale crisisorganisatie kan worden geactiveerd als de nationale veiligheid in het geding is of bij situaties met een grote maatschappelijke impact. Daarbij valt te denken aan een lokaal of regionaal incident of ongeval met veel slachtoffers, een incident of ongeval in het buitenland met een groot aantal Nederlandse slachtoffers of grote maatschappelijke impact in Nederland, of evenementen in Nederland met een (inter)nationale uitstraling.

Afbakening

Het domein waarop dit crisisplan van toepassing is, wordt in de Nationale Veiligheid Strategie de digitale ruimte genoemd: "Het conglomeraat van ICT-middelen en -diensten dat alle entiteiten die digitaal verbonden kunnen zijn bevat permanente, tijdelijke en plaatselijke verbindingen en gegevens die zich in dit domein bevinden (o.a. data, programmacode, informatie), waarbij geen geografische beperkingen zijn gesteld".[4]

Conform de Wet beveiliging netwerken en informatiesystemen (Wbni) is een incident "elke gebeurtenis met een schadelijk effect op de beveiliging van netwerk- en informatiesystemen". Daarbij gaat het om beschikbaarheid, integriteit, vertrouwelijkheid en authenticiteit (biva) van netwerk- en informatiesystemen. Dit plan ziet op de beheersing van incidenten met aanzienlijke maatschappelijke gevolgen. Hieraan kunnen volgens het Cybersecuritybeeld Nederland (CSBN) de volgende typen incidenten/dreigingen ten grondslag liggen:[5]

- Verstoring/sabotage: het opzettelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of –diensten.
- Informatiemanipulatie: aantasting van de integriteit van informatie door het opzettelijk wijzigen van informatie.
- Informatiediefstal: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
- Spionage: aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
- Systeemmanipulatie: aantasting van informatiesystemen of –diensten; gericht op de vertrouwelijkheid of integriteit van informatiesystemen of –diensten. Deze worden daarna ingezet om andere aanvallen uit te voeren.
- Storing/uitval: aantasting van de integriteit of beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen.
- Lek: aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen.

Wanneer een of meer van voorgaande dreigingen/incidenten zich manifesteren, kan dit impact hebben op de nationale veiligheidsbelangen zoals door het kabinet gedefinieerd in de Nationale Veiligheid Strategie 2019 (NVS). Deze strategie identificeert cyberdreigingen als een van de dominante risico's met een grote impact en hoge waarschijnlijkheid die de nationale veiligheid in ernstige tot zeer ernstige mate kunnen aantasten. In dat geval is er sprake van maatschappelijke ontwrichting.

Kenmerken

Incidenten in de netwerk- en informatiesystemen verschillen in een aantal opzichten van andere incidenttypes:

- **De snelheid waarmee dergelijke incidenten zich manifesteren.** Een incident kan van het een op het andere moment ontstaan (aan/uit) of zich eerst als een veenbrand ontwikkelen met een reeks aan incidenten, die samen een crisis vormen of daartoe leiden. De hersteltijd na een verstoring kan zowel (extreem) kort als (extreem) lang zijn.
- **Door hyperconnectiviteit kan een incident gevolgen hebben voor álle vitale processen.** Dit kan leiden tot maatschappelijke ontwrichting als de verstoring meerdere dagen tot een week aanhoudt.
- **Door het spioneren/manipuleren van vitale en strategische informatie/data kunnen de vitale belangen van Nederland en zijn bondgenoten worden aangetast.**
- **Door complexe ketenafhankelijkheden kan de bron soms lastig te achterhalen zijn, waardoor respons wordt bemoeilijkt**. Organisaties werken samen in ketens waardoor problemen bij toeleveranciers kunnen leiden tot maatschappelijke ontwrichting.
- **De crisisorganisaties worden zelf mogelijk ook zwaar geraakt in hun functioneren**. Uitval of een beperkte beschikbaarheid van de eigen ICT-middelen hebben een direct effect op de responscapaciteit, zoals interne en externe communicatie (waaronder telefonie).
- **Bij de bronbestrijding is de overheid grotendeels afhankelijk van het handelen van private partijen**. Vrijwel alle ICT-infrastructuur en diensten zijn in handen van private partijen.
- **Bronbepaling en attributie zijn moeilijk**. Het is complex om te bepalen waar een incident vandaan komt, wie er achter een eventuele aanval zit en wat het eventuele doel van de aanval is. Vaak wordt er zeker door de betrokken diensten vanuit opsporingsperspectief vanuit gegaan dat er van opzet sprake is, totdat blijkt dat dat niet het geval is.
- **Een incident kan ontstaan doordat gebruik gemaakt wordt van een tot op dat moment onbekende kwetsbaarheid**. Dit betreft zogeheten *zero-day exploits*.
- **Een incident in de netwerk- en informatiesystemen treft zelden alleen het digitale domein.** Veelal zullen er ook ongewenste effecten optreden in het fysieke domein. Deze zullen niet altijd direct gekoppeld kunnen worden aan het incident in de netwerk- en informatiesystemen.
- **Netwerken en informatiesystemen houden zich niet aan landsgrenzen**. Het is aannemelijk dat het incident een internationaal karakter heeft, waarbij de oorzaak van de grootschalige verstoring in het buitenland kan liggen, in meerdere landen tegelijkertijd kan optreden, of waarbij de oorzaak mogelijk (mede) in Nederland ligt, maar het effect niet.

4 *Nationale Veiligheid Strategie* 2019.

5 Conform dreigingsmatrix *Cyber Security Beeld Nederland* 2019 en eerdere edities.

- **Incidenten in het digitale domein houden zich eveneens niet aan geografische grenzen binnen eigen land**. In tegenstelling tot traditionele fysieke incidenten is bij dit type incidenten lastiger te achterhalen binnen welke veiligheidsregio('s) het incident zich afspeelt en wie aan zet is om het incident op te lossen.
- **Er bestaat mogelijk een tekort aan specifieke deskundigen**, met name binnen het digitale domein die aan bron- en effectbestrijding kunnen doen.
- **Het digitale domein kenmerkt zich door het overstijgen van jurisdicties**. Hierdoor zijn handhaving en opsporingsmogelijkheden op nationaal niveau beperkt en is in voorkomend geval internationale samenwerking vereist.
- **Een incident in het digitale domein kan onderdeel zijn van hybride conflictvoering**. Daarbij gaat het om een conflictvoering tussen staten, grotendeels onder het juridisch niveau van openlijk gewapend conflict, met geïntegreerd gebruik van middelen en actoren, met als doel bepaalde strategische doelstellingen te bereiken.

De gevolgen van een grote uitval of verstoring in het digitale domein kunnen doordringen in alle lagen van de samenleving. Dit plan richt zich dan ook op een *all-hazard* aanpak van de maatschappelijke gevolgen en effecten.

Leeswijzer

Hoofdstuk 2 bevat een aantal incidentscenario's in het digitale domein. Hoofdstuk 3 bevat per processtap in de crisisbeheersing een overzicht van de betrokken actoren. Hoofdstuk 4 gaat in op de crisiscommunicatie.

Bijlagen:

1. Overzicht vitale processen
2. Meest relevante wet- en regelgeving
3. Rolbeschrijvingen
4. Relevante bronnen en literatuur
5. Afkortingen

Crisisplan in relatie tot WRR-rapport

Bij deze herziening zijn voor zover nu mogelijk en wenselijk de bevindingen en aanbevelingen uit het WRR-rapport "Voorbereiden op digitale ontwrichting" meegenomen en verwerkt. Een kabinetsbrede reactie op dit rapport wordt gepubliceerd in het eerste kwartaal van 2020. Hierin staan mogelijk relevante passages die worden meegenomen bij de voorziene actualisatie van dit plan.

Algemene bepalingen

- Dit is de openbare versie van het NCP-Digitaal. Enkele bijlagen zijn niet openbaar in verband met de nationale veiligheid.
- Het Directeurenoverleg Crisisbeheersing (DOCB) is ambtelijk opdrachtgever van het NCP-Digitaal.
- Het NCP-Digitaal is opgesteld door een projectgroep met vertegenwoordigers van de ministeries van BZ, BZK, DEF, EZK, FIN, IenW en JenV, politie, veiligheidsregio's, AIVD en OM en ter advisering voorgelegd aan de Commissie Vitale Infrastructuur en het Publiek-Privaat Directeurenoverleg Cyber Security.
- Het NCP-Digitaal is vastgesteld door het Directeurenoverleg Crisisbeheersing (DOCB), het Directeurenoverleg Cybersecurity en daaraanvolgend in de Ministeriële Commissie Economie en Veiligheid van 11 februari 2020 en de ministerraad van 14 februari 2020.
- Het NCP-Digitaal wordt gebruikt als basis voor cybercrisisoefeningen op nationaal niveau, zoals ISIDOOR.

Beheercyclus

- De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is eigenaar van en verantwoordelijk voor beheer en actualisatie van het NCP-Digitaal. De NCTV beziet jaarlijks in overleg met de betrokken actoren en organisaties of actualisering van het NCP-Digitaal nodig is.

Bouwsteen		Bouwsteenwaarde
Oorzaak		**Niet-opzettelijk handelen**: Het incident (storing, uitval, lek) wordt veroorzaakt door een technische of menselijke fout, waarbij geen opzet in het spel is.
		**Opzettelijk handelen**: Het incident wordt door opzettelijk handelen veroorzaakt.
Bron		**Binnen Nederland**: De oorzaak van het incident ligt in Nederland.
		**Buiten Nederland**: De oorzaak van het incident ligt (ook) in het buitenland. De bron kan in één land liggen, maar ook in meerdere landen waaronder Nederland.
Actor		**Niet-statelijke actor**: Er is sprake van een incident veroorzaakt door een niet-statelijke actor.
		**Statelijke actor**: Het incident is met opzet veroorzaakt door een statelijke actor of een partij die nauwe banden heeft met een staat.
Geraakt domein		**Alleen in digitale domein**: De effecten van het incident zijn alleen te merken in het digitale domein; er is geen sprake van effecten in de fysieke buitenwereld.
		**Maatschappelijk belangrijke voorzieningen (niet-vitaal)**: De vitale processen zoals gedefinieerd door de rijksoverheid worden niet geraakt. De effecten zijn wel te merken in bijvoorbeeld openbaar vervoer (incl. verkeerssignalering), zorg, tankstations, supermarkten, scholen, bedrijven. Burgers, bedrijven en/of overheden buiten de getroffen organisatie ondervinden significante hinder van het incident.
		**Vitale processen**: De effecten van het incident zijn (ook) te merken bij de aanbieders van vitale processen. Een of meer vitale processen zoals gedefinieerd in de vitaliteitsbeoordeling van de rijksoverheid ondervinden (ernstige) hinder. Een van de vitale processen die geraakt kunnen worden zijn de ICT-kritische onderdelen van de responscapaciteit van de betrokken actoren en organisaties in de nationale en regionale crisisorganisaties. Burgers, bedrijven en/of overheden ondervinden hier significante hinder van.
Geraakt gebied		**Eén (veiligheids)regio**: Het incident leidt tot effecten in één (veiligheids)regio in Nederland.
		**Meerdere (veiligheids)regio's**: De verstoring heeft effecten in meerdere (veiligheids)regio's. Deze regio's kunnen naast elkaar liggen maar ook verspreid zijn door Nederland.
		**Meerdere landen**: Het incident heeft (ook) effecten in het buitenland. Dit kan gaan om een of meerdere landen, maar ook om een combinatie van effecten in Nederland en andere landen.
Oplossings-perspectief (technisch)		**Technisch oplossingsperspectief aanwezig**: Het is (of wordt snel) duidelijk hoe het incident opgelost kan worden. De benodigde maatregelen hiervoor kunnen genomen worden.
		**Technisch oplossingsperspectief langdurig onbekend**: Het is onduidelijk hoe het incident opgelost kan worden, waardoor er geen maatregelen met betrekking tot het incident zelf in gang gezet kunnen worden (alleen effect mitigerende maatregelen).

2. Incidentscenario's

Optimale flexibiliteit is het uitgangspunt bij de organisatie, inrichting en werkwijze van de nationale crisisstructuur. Voor alle onderdelen en overleggen binnen die structuur geldt dat deze naar behoefte worden ingezet en flexibel ingericht en samengesteld. Er is sprake van maatwerk per situatie en zo nodig per bijeenkomst.[6]

Omdat er talloze scenario's denkbaar zijn als het gaat om incidenten in het digitale domein, zeker in combinatie met een mogelijke doorwerking naar het fysieke domein, is in dit crisisplan gekozen voor een aanpak gebaseerd op bouwstenen. Bij de definiëring van de bouwstenen is geredeneerd vanuit voor de crisisrespons betekenisvolle verschillen. Het gaat om de volgende bouwstenen: oorzaak, bron, actor, geraakt domein, geraakt gebied en technisch oplossingsperspectief. Door de waarde van telkens één bouwsteen te wijzigen ontstaan acht fictieve scenario's naast een zogeheten nul-scenario. Het gaat om de volgende acht scenario's: opzettelijk handelen, technisch falen buiten Nederland, statelijke actor, maatschappelijk belangrijke voorzieningen (niet-vitaal), vitale processen, regio-overschrijdende effecten, effecten in het buitenland en technologisch oplossingsperspectief onbekend.

Aard en verloop van het incident zijn mede bepalend voor de inrichting van de gewenste respons. Per bouwsteen is op hoofdlijnen geïnventariseerd hoe gevolgen/effecten en de benodigde maatregelen kunnen doorwerken op de inrichting en werkwijze van de crisisrespons. Het gaat om een denkexercitie aan de hand van drie hoofdvragen.

De beschrijvingen van de afwijkende bouwsteenelementen gaan er steeds vanuit dat alleen het betreffende element afwijkt van het nul-scenario. In de praktijk zal veelal een combinatie van verschillende elementen aan de orde zijn. Het is vooral bedoeld als hulpmiddel waarmee de doelgroepen van dit kaderstellende crisisplan bij hun eigen voorbereiding en in een daadwerkelijke situatie zelf als volgt aan de slag kunnen.

Stappenplan

Stap 1: Bepaal of en in welke mate een bouwsteen geraakt is. *(Er zijn (naar verwachting) altijd meerdere bouwstenen geraakt en daarmee meerdere scenario's van belang.)*

Stap 2: Beantwoord per scenario de volgende drie vragen:

- ***Wat zijn de belangrijkste mogelijke (in)directe gevolgen en effecten van het incident?***
- ***Welke mitigerende maatregelen zijn nodig om de gevolgen en effecten (slachtoffers, schade) te voorkomen of te beheersen?***
- ***Welke partijen zijn betrokken c.q. nodig voor een adequate aanpak?***

Stap 3: Voeg de antwoorden op de drie hoofdvragen voor de van belang zijnde scenario's samen.

Stap 4: Nadere informatie is opgenomen in hoofdstuk 3 en 4 en in de bijlagen.

Situational awareness, monitoring en informatievoorziening zijn op 24/7-basis reguliere taken van het NCSC en de NCTV (NCC). Daarnaast is de NCTV stelselverantwoordelijk voor de nationale crisisbeheersing. Beide organisaties zijn derhalve bij alle scenario's betrokken.

Politie, inlichtingen- en veiligheidsdiensten en het Openbaar Ministerie zijn vanaf het begin betrokken omdat lang onduidelijk kan zijn of de scenario's "opzettelijk handelen" en "statelijke actor" van toepassing zijn. Het ministerie van Buitenlandse Zaken is vanaf het begin betrokken zolang onduidelijk is of het scenario "statelijke actor" van toepassing is.

6 Nationaal Handboek Crisisbesluitvorming.

Bouwsteen	Bouwsteenwaarde		
Oorzaak	**Niet-opzettelijk handelen**	Opzettelijk handelen	
Bron	**Binnen Nederland**	Buiten Nederland	
Actor	**Niet-statelijk**	Statelijk	
Geraakt domein	**Alleen in ICT-domein**	Maatschappelijk belangrijke voorzieningen (niet-vitaal)	Vitale processen
Geraakt gebied	**Eén veiligheidsregio**	Meerdere veiligheidsregio's	Meerdere landen
Oplossingperspectief	**Technisch oplossings-perspectief aanwezig**	Technisch oplossings-perspectief onbekend	

Nul-scenario

Op basis van de gedefinieerde bouwstenen en bouwsteenwaarden kan een nul-scenario worden geschetst. In dit nul-scenario blijven de gevolgen en te treffen maatregelen beperkt tot het digitale domein en is alleen incident-bestrijding nodig door de direct getroffen partijen. Het nul-scenario leidt niet tot opschaling van de nationale crisisorganisatie.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Blijven beperkt tot het digitale domein, i.c. verstoring bedrijfsprocessen getroffen partijen
Maatregelen	BCM-maatregelen getroffen partijen
	Reguliere taak situational awareness, monitoring en informatiedeling NCSC/NCC/EZK
Betrokken partijen	Digitale dienstverleners getroffen partijen
	Eventueel derde (commerciële) partijen voor ondersteuning, expertise of kennis
	Getroffen partijen
	NCSC en NCTV

Scenarioschets

Als gevolg van een technisch probleem, fysieke oorzaak (bijv. brand of een overstroming) en/of een menselijke fout gaat er iets mis in de ICT-voorziening(en) van een (of meer) organisatie(s) - niet zijnde aanbieders van vitale processen - waardoor de beschikbaarheid, integriteit en/of exclusiviteit van deze voorziening(en) in het geding komt. De betreffende organisatie(s) kan/kunnen hier intern last van hebben (in hun bedrijfsprocessen) maar de fout/het probleem zorgt niet of beperkt voor effecten in de (fysieke) buitenwereld. Wel kan informatiedeling van belang zijn om herhaling bij andere organisaties te voorkomen. Als het incident in de buitenwereld bekend wordt, kan het wel voor media-aandacht zorgen, bijvoorbeeld als een publieke organisatie is getroffen. In dat geval kan het incident ook politiek-bestuurlijke vraagstukken opleveren. Het probleem kent echter een oplossing en is van dien aard dat men binnen afzienbare tijd weer terug kan gaan naar de oorspronkelijke situatie.

Bouwsteen	Bouwsteenwaarde		
Oorzaak	Niet-opzettelijk handelen	**Opzettelijk handelen**	
Bron	**Binnen Nederland**	Buiten Nederland	
Actor	**Niet-statelijk**	Statelijk	
Geraakt domein	**Alleen in ICT-domein**	Maatschappelijk belangrijke voorzieningen (niet-vitaal)	Vitale processen
Geraakt gebied	**Eén veiligheidsregio**	Meerdere veiligheidsregio's	Meerdere landen
Oplossingperspectief	**Technisch oplossings-perspectief aanwezig**	Technisch oplossings-perspectief onbekend	

Oorzaak

Opzettelijk handelen

Er is sprake van een incident door opzettelijk handelen vanuit Nederland, waarbij de effecten ook beperkt blijven tot Nederland.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Mensen en instanties worden gedupeerd (bijvoorbeeld financieel, chantage, laster, imagoschade)
	Afname vertrouwen aangeboden digitale diensten
	Integriteit informatievoorziening aangetast
	Maatschappelijke onrust, verstoring openbare orde
	Gevolgen, effecten eventueel groter door mogelijkheid nieuw incident, herhaling of onbekendheid aantal betrokkenen
Maatregelen	Opsporing
	Analyses om wel/niet opzet vast te stellen, rekening houden met '*copycats*'
	Desnoods (on)gevraagd veiligstellen van data
Betrokken partijen	Digitale dienstverleners getroffen partijen
	Aanbieders getroffen vitale processen
	Politie
	Openbaar Ministerie
	KMar
	Forensische/onderzoekende en commerciële partijen
	Ministeries, verantwoordelijk voor getroffen domeinen of partijen
	NCSC en NCTV

In het geval van opzettelijk handelen leidt het Openbaar Ministerie het onderzoek en geeft de politie daar uitvoering aan.

Het zal doorgaans niet direct duidelijk zijn dat een ICT-incident met opzet is veroorzaakt. Vanuit opsporingsperspectief wordt altijd rekening gehouden met het feit dat er sprake kan zijn van opzettelijk handelen, tot het moment dat dit expliciet wordt uitgesloten.

In de incidentrespons moeten bewuste keuzes gemaakt worden tussen het belang van opsporing enerzijds, en het belang van herstel en het beperken van (maatschappelijke) impact anderzijds. Als het ICT-incident evident niet-opzettelijk is, kan er toch sprake zijn van strafbare feiten, waardoor opsporingsbevoegdheden misschien mogelijk blijven.

Bouwsteen	Bouwsteenwaarde		
Oorzaak	**Niet-opzettelijk handelen**	Opzettelijk handelen	
Bron	Binnen Nederland	**Buiten Nederland**	
Actor	**Niet-statelijk**	Statelijk	
Geraakt domein	**Alleen in ICT-domein**	Maatschappelijk belangrijke voorzieningen (niet-vitaal)	Vitale processen
Geraakt gebied	**Eén veiligheidsregio**	Meerdere veiligheidsregio's	Meerdere landen
Oplossingperspectief	**Technisch oplossings-perspectief aanwezig**	Technisch oplossings-perspectief onbekend	

Bron

Technisch falen buiten Nederland

In dit scenario is er sprake van een incident in Nederland als gevolg van technisch falen buiten Nederland.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Mogelijke verstoringen bedrijfsprocessen kunnen in omvang toenemen doordat bron buiten Nederland ligt.
	Attributie mogelijk lastiger in verband met bron buiten NL
Maatregelen	Afstemming en samenwerking rondom technische aspecten waaronder attributie met internationale netwerken
	Brede toolkit diplomatie
Betrokken partijen	Digitale dienstverleners getroffen partijen
	Aanbieders getroffen vitale processen
	Ministerie van Buitenlandse Zaken
	Openbaar Ministerie
	Internationaal netwerk via NCSC en NCC
	Andere ministeries, verantwoordelijk voor getroffen domeinen of partijen
	NCSC en NCTV

Dit scenario zal op zichzelf niet direct leiden tot opschaling naar (delen van) de nationale crisisstructuur, maar creëert dynamiek en samenhang met partijen buiten Nederland waardoor nauwere samenwerking met internationale partners misschien nodig is.

Het NCSC coördineert in veel voorkomende gevallen de samenwerking met internationale (cyber)partners. Het NCSC staat ook in contact met internationale samenwerkingsverbanden die geen actieve crisisrol hebben, maar wel ter ondersteuning benut worden voor hun (netwerk)kennis en expertise.

Afhankelijk van de situatie kan het ministerie van Buitenlandse Zaken een rol op zich nemen voor de diplomatieke afstemming met het land waar de bron van het incident zich bevindt. Inlichtingendiensten en politie kunnen onderzoek doen, eventueel in samenwerking met hun internationale counterparts om de bron van het incident te achterhalen.

Bouwsteen	Bouwsteenwaarde		
Oorzaak	**Niet-opzettelijk handelen**	Opzettelijk handelen	
Bron	**Binnen Nederland**	Buiten Nederland	
Actor	Niet-statelijk	**Statelijk**	
Geraakt domein	**Alleen in ICT-domein**	Maatschappelijk belangrijke voorzieningen (niet-vitaal)	Vitale processen
Geraakt gebied	**Eén veiligheidsregio**	Meerdere veiligheidsregio's	Meerdere landen
Oplossingperspectief	**Technisch oplossings-perspectief aanwezig**	Technisch oplossings-perspectief onbekend	

Actor

Statelijke actor

Bij dit scenario gaat het om een incident waarbij een statelijke actor is betrokken. Deze kan diverse doelen hebben: (economische) spionage, (voorbereiding op) sabotage, beïnvloeding als deel van een groter of internationaal conflict, vergelding, enz.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Verstoring vitale processen
	Aantasting integriteit systemen
	Diplomatieke/internationale onrust
	Maatschappelijke onrust
	Politiek onrust / druk
	Mogelijk meer risico's NL burgers in buitenland
Maatregelen	Opsporing en vervolging
	Relevante inlichtingenprocessen
	Afstemming en samenwerking internationale netwerken
	Diplomatiek responskader incl. mogelijke tegenreactie
	Uitroepen noodtoestand (in uiterste geval)
	Beroep op internationale verdragen (VN, NAVO, EU)
Betrokken partijen	Digitale dienstverleners getroffen partijen
	Aanbieders getroffen vitale processen
	Ministeries van AZ, BZ, BZK, DEF, JenV
	Politie
	AIVD, MIVD
	Openbaar Ministerie
	Internationaal netwerk via NCSC en NCC
	Andere ministeries, verantwoordelijk voor getroffen domeinen of partijen
	NCSC en NCTV

In ernstige gevallen waarbij slachtoffers vallen, ontwrichtende schade ontstaat of vitale processen van de overheid worden verstoord, kan er sprake zijn van een gewapende aanval en kan er een beroep worden gedaan op de Oorlogswet om de noodtoestand uit te roepen. Ook ontstaat dan het recht op nationale zelfverdediging onder art 51 van het VN Handvest. Verder kan een beroep worden gedaan op het NAVO-verdrag en EU-verdrag.

Zodra helder is dat een statelijke actor in het spel is, veranderen de rol en betrokkenheid van de inlichtingen- en veiligheidsdiensten, Defensie, Buitenlandse Zaken en Algemene Zaken. Al naar gelang de aard van de aanval, zullen sommige besluiten parallel aan de nationale crisisstructuur in andere gremia plaatsvinden (Raad Veiligheid en Inlichtingen, Raad Defensie en Internationale Aangelegenheden, Ministeriële Kerngroep Speciale Operaties, etc.). De kans is aanwezig dat de internationale dimensie ook een reactie vraagt van internationale organisaties zoals de EU, OVSE, NAVO of VN.

Bouwsteen	Bouwsteenwaarde		
Oorzaak	**Niet-opzettelijk handelen**	Opzettelijk handelen	
Bron	**Binnen Nederland**	Buiten Nederland	
Actor	**Niet-statelijk**	Statelijk	
Geraakt domein	Alleen in ICT-domein	**Maatschappelijk belangrijke voorzieningen (niet-vitaal)**	Vitale processen
Geraakt gebied	**Eén veiligheidsregio**	Meerdere veiligheidsregio's	Meerdere landen
Oplossingperspectief	**Technisch oplossings-perspectief aanwezig**	Technisch oplossings-perspectief onbekend	

Geraakt domein

Maatschappelijk belangrijke voorzieningen (niet-vitaal)[7]

Bij dit scenario gaat het om een incident waarbij maatschappelijk belangrijke, maar niet-vitale voorzieningen zijn getroffen, zoals openbaar vervoer (inclusief verkeerssignalering), zorg, supermarkten, tankstations, scholen, hulpverlening, bedrijven, gemeenten.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Verstoring bedrijfsprocessen getroffen bedrijven, instanties en organisaties
	Aantasting integriteit systemen
	Verstoring openbare orde en veiligheid
	Maatschappelijke onrust
	Politieke onrust / maatschappelijke ontwrichting
	Economische schade
	Reputatieschade en vertrouwensverlies
Maatregelen	BCM getroffen bedrijven, instanties en organisaties.
	Ondersteuning via CERT's Landelijk Dekkend Stelsel
	Verzoek aan NCSC om bijstand (art.16 Wbni)
	Maatregelen conform relevante crisisplannen
Betrokken partijen	Digitale dienstverleners getroffen partijen
	Aanbieders getroffen voorzieningen
	Digital Trust Center, sectorale CERT's Landelijk Dekkend Stelsel
	Ministeries, verantwoordelijk voor getroffen domeinen of partijen
	Veiligheidsregio's, LOCC c.q. LOCC-B
	Politie
	Openbaar Ministerie
	NCSC en NCTV

Wanneer niet-vitale voorzieningen getroffen worden hoeft dit niet per definitie te betekenen dat nationale of regionale crisisorganisaties betrokken raken. Bedrijven, instellingen en organisaties blijven zelf verantwoordelijk voor de continuïteit van hun eigen processen.

Daarnaast wordt binnen een landelijk dekkend stelsel van samenwerkingsverbanden, waaronder sectorale CERT's, op een snelle en efficiënte wijze informatie over incidenten en dreigingen gedeeld.

Wanneer maatschappelijke onrust/impact en effecten in de fysieke buitenwereld ontstaan kan dit echter wel leiden tot opschaling van crisisstructuren.

7 Conform de vitaliteitsbeoordeling, zoals door het rijk in 2017 vastgesteld. Zie overzicht vitale processen.

Bouwsteen	Bouwsteenwaarde	
Oorzaak	**Niet-opzettelijk handelen**	Opzettelijk handelen
Bron	**Binnen Nederland**	Buiten Nederland
Actor	**Niet-statelijk**	Statelijk
Geraakt domein	Alleen in ICT-domein	Maatschappelijk belangrijke voorzieningen (niet-vitaal)	**Vitale processen**
Geraakt gebied	**Eén veiligheidsregio**	Meerdere veiligheidsregio's	Meerdere landen
Oplossingperspectief	**Technisch oplossings-perspectief aanwezig**	Technisch oplossings-perspectief onbekend

Geraakt domein

Vitale processen

In dit scenario zijn een of meer vitale processen in Nederland getroffen.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Verstoring/uitval essentiële ICT-diensten voor de continuïteit van vitale processen
	Mogelijk doorwerking naar niet-vitale voorzieningen in verband met cascade-effecten
Maatregelen	BCM-maatregelen digitale dienstverleners getroffen bedrijven en organisaties
	Maatregelen conform relevante crisisplannen (o.a. bijstand NCSC)
	Specifieke maatregelen per getroffen vitaal proces
Betrokken partijen	Digitale dienstverleners getroffen partijen
	Aanbieders getroffen vitale processen
	Ministeries verantwoordelijk voor getroffen vitale processen (beleidsdirecties en DCC's)
	ICT Response Board
	Politie
	AIVD, MIVD
	Openbaar Ministerie
	Veiligheidsregio's, LOCC c.q. LOCC-B
	NCSC en NCTV

De vitale processen in Nederland zijn in toenemende mate afhankelijk van gedigitaliseerde processen, de onderliggende (informatie)systemen en ketenafhankelijkheden. Deze processen en systemen vormen het fundament van onze samenleving. Een dergelijk incident raakt al snel de nationale veiligheidsbelangen waarbij er sprake kan zijn van cascade effecten die kunnen leiden tot activering van de nationale crisisstructuur.

Een vitale aanbieder blijft altijd zelf verantwoordelijk voor de eigen continuïteit en dienstverlening. Het NCSC kan daarbij waar nodig ondersteunen.

Bijlage 1 bevat een overzicht van de Nederlandse vitale processen, conform de vitaliteitsbeoordeling zoals door het rijk in 2017 vastgesteld.

Bouwsteen	Bouwsteenwaarde		
Oorzaak	**Niet-opzettelijk handelen**	Opzettelijk handelen	
Bron	**Binnen Nederland**	Buiten Nederland	
Actor	**Niet-statelijk**	Statelijk	
Geraakt domein	**Alleen in ICT-domein**	Maatschappelijk belangrijke voorzieningen (niet-vitaal)	Vitale processen
Geraakt gebied	Eén veiligheidsregio	**Meerdere veiligheidsregio's**	Meerdere landen
Oplossingperspectief	**Technisch oplossings-perspectief aanwezig**	Technisch oplossings-perspectief onbekend	

Geraakt gebied

Regio-overstijgende effecten

In dit scenario leidt het incident tot gevolgen en effecten in meerdere veiligheidsregio's en/of andere regionaal ingedeelde sectoren of gebieden.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Effectgebied groter, waardoor kans op maatschappelijke onrust en/of ontwrichting toeneemt
	Complexiteit groter vanwege schaarste beschikbare middelen en verschillen tussen regio's
Maatregelen	BCM-maatregelen getroffen partijen
	Bovenregionale afstemming en informatie-uitwisseling
	Multidisciplinair landelijk operationeel beeld
	Maatregelen in het kader van opsporing en strafbaarstelling
Betrokken partijen	Digitale dienstverleners getroffen partijen
	Aanbieders getroffen vitale processen
	Veiligheidsregio's, LOCC c.q. LOCC-B
	Sectorale CERT's
	Politie
	Openbaar Ministerie
	Ministeries, verantwoordelijk voor getroffen domeinen of partijen
	NCSC en NCTV

Indien het incident meer dan één veiligheidsregio in Nederland beslaat (omdat bron en effecten in verschillende regio's liggen of omdat verschillende regio's geraakt worden), dient samenwerking gezocht te worden met en door de betrokkenen veiligheidsregio's voor de gevolgbestrijding van voornamelijk de fysieke effecten en mogelijke maatschappelijke onrust.

Het NCC is voor veiligheidsregio's het 24/7 informatieloket en contactpunt van het rijk en legt de verbinding met de andere ministeries en het NCSC, in nauwe samenwerking met het LOCC.

Bouwsteen	Bouwsteenwaarde		
Oorzaak	**Niet-opzettelijk handelen**	Opzettelijk handelen	
Bron	**Binnen Nederland**	Buiten Nederland	
Actor	**Niet-statelijk**	Statelijk	
Geraakt domein	**Alleen in ICT-domein**	Maatschappelijk belangrijke voorzieningen (niet-vitaal)	Vitale processen
Geraakt gebied	Eén veiligheidsregio	Meerdere veiligheidsregio's	**Meerdere landen**
Oplossingperspectief	**Technisch oplossings-perspectief aanwezig**	Technisch oplossings-perspectief onbekend	

Geraakt gebied

Effecten in het buitenland

In dit scenario gaat het om een incident in Nederland met effecten in het buitenland.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Reputatieschade Nederland
	Internationale druk op Nederland
Maatregelen	BCM-maatregelen getroffen partijen
	Diplomatiek responskader
	Afstemming en samenwerking internationale netwerken o.a. over ondersteuning en bijstand
Betrokken partijen	Digitale dienstverleners getroffen partijen
	Aanbieders getroffen vitale processen
	Ministeries van AZ, BZ, DEF, JenV en evt. andere ministeries verantwoordelijk voor getroffen domeinen of partijen
	NCSC en NCC (Nationaal Contactpunt NL)
	Internationale netwerken
	Openbaar Ministerie
	NCSC en NCTV

In dit scenario wordt de internationale samenwerking geactiveerd om de bron en oorzaak van het incident te achterhalen en om de gevolgen zo beperkt mogelijk te houden (zie ook scenario 'bron buiten Nederland'). Het verschil zit hem in het feit dat in dit scenario de bron binnen Nederland kan liggen. Wanneer dat het geval is maakt het de bronbestrijding iets eenvoudiger, omdat geen rekening gehouden hoeft te worden met mandaten van andere landen.

Indien bevestigd wordt dat de bron in Nederland ligt met effecten merkbaar in meerdere landen zal de (internationale) druk op Nederland, en met name de Nederlandse overheid toenemen om tot een oplossing te komen. Dit kan ook leiden tot opschaling van (delen van) de nationale crisisstructuur.

Bouwsteen	Bouwsteenwaarde		
Oorzaak	**Niet-opzettelijk handelen**	Opzettelijk handelen	
Bron	**Binnen Nederland**	Buiten Nederland	
Actor	**Niet-statelijk**	Statelijk	
Geraakt domein	**Alleen in ICT-domein**	Maatschappelijk belangrijke voorzieningen (niet-vitaal)	Vitale processen
Geraakt gebied	**Eén veiligheidsregio**	Meerdere veiligheidsregio's	Meerdere landen
Oplossingperspectief	Technisch oplossings-perspectief aanwezig	**Technisch oplossings-perspectief onbekend**	

Oplossingperspectief

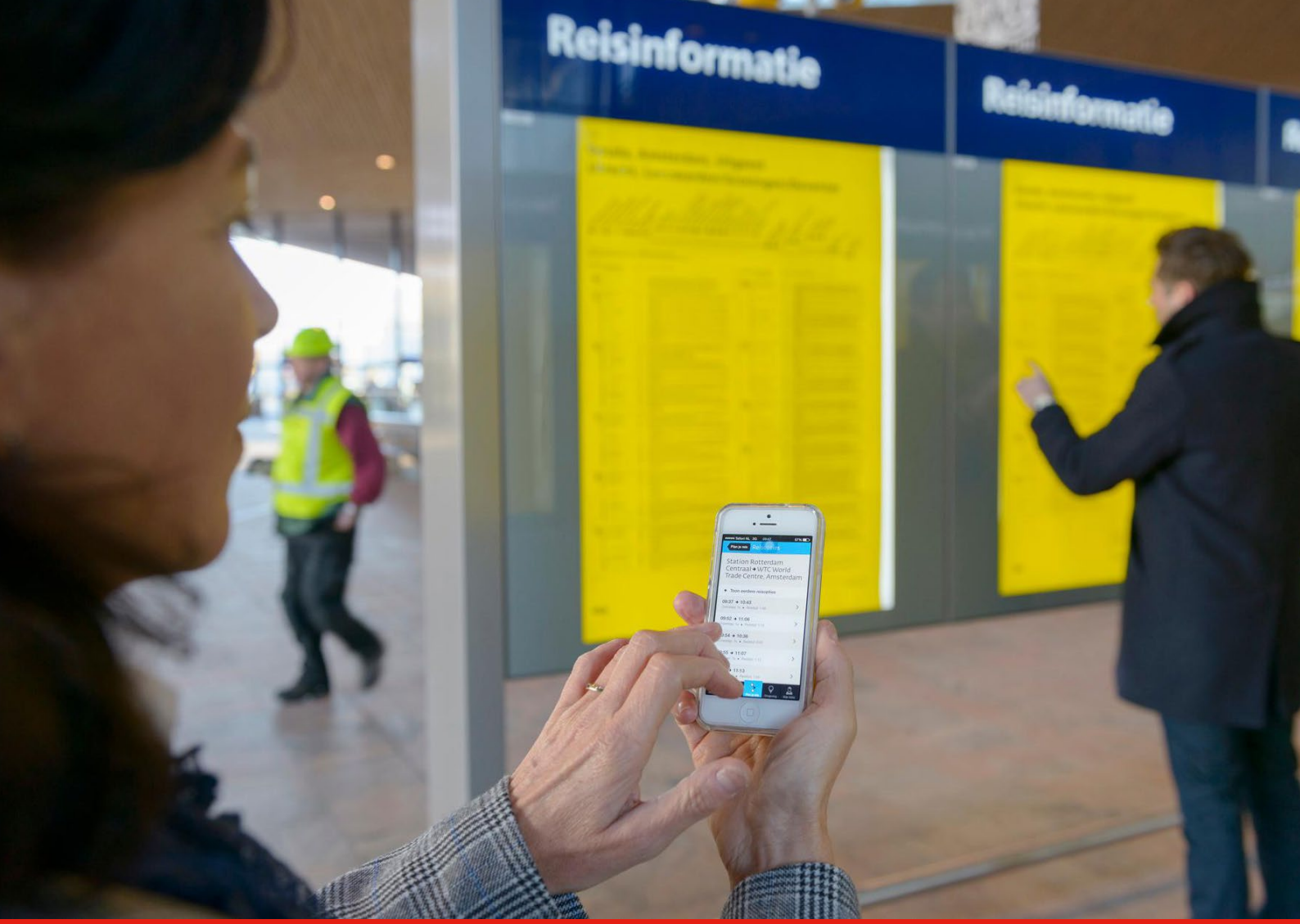
Technisch oplossingsperspectief langdurig onbekend

In dit scenario gaat het om een incident waar bij een technisch oplossings-perspectief langdurig onbekend is en de respons zich vooral op het mitigeren van effecten richt.

Gevolgen, maatregelen en respons

Gevolgen en effecten	Maatschappelijke onrust gevoed door ontbreken (zicht op) oplossing
	Onzekerheid
	Verschuiving van respons naar 'ermee omgaan'
Maatregelen	BCM-maatregelen getroffen partijen
	Zoveel mogelijk mitigeren effecten
	Stimuleren zelfredzaamheid burgers en bedrijven
	Monitoren (sociale) onrust
Betrokken partijen	ICT-dienstverleners getroffen partijen
	Aanbieders getroffen vitale processen
	Veiligheidsregio's, LOCC c.q. LOCC-B/N
	Ministeries verantwoordelijk voor getroffen domeinen of partijen
	NCSC en NCTV

De rol van het NCSC met betrekking tot onderzoek doen naar de oorzaak kan prominenter worden. Bezien zowel vanuit perspectief wettelijke taken (Wbni art. 3) als vrijwillige melding en mogelijke bijstand door NCSC (art. 16). Er wordt zoveel mogelijk conform reguliere afspraken en crisisbeheersingsstructuren gewerkt.


Reisinformatie
Reisinformatie
Station Rotterdam Centraal ➔ WTC World Trade Centre, Amsterdam

3. Processtappen en actoren

Dit hoofdstuk bevat een grafische weergave van de digitale- en generieke crisisstructuur. Daarnaast is een overzicht opgenomen van de rollen van de belangrijkste actoren tijdens een incident.

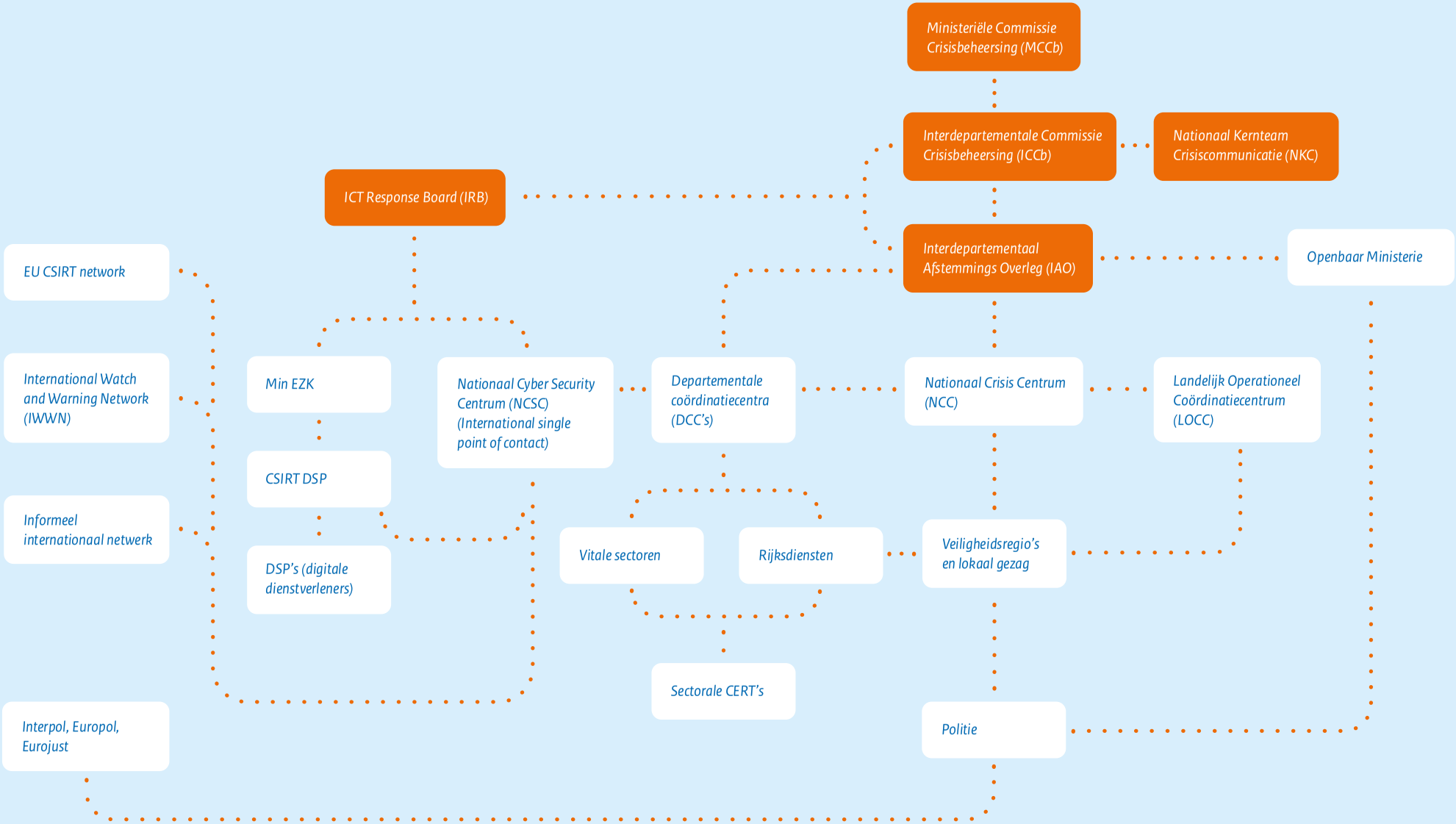
Bij ICT-incidenten doen alle CERT's en CSIRT's in de betrokken private bedrijven actief hun werk. Het NCSC en het NCC zijn hierbij het koppelvlak met de algemene en functionele ketens. Met name CERT's en CSIRT's van de Digitale Service Providers en de ICT-leveranciers zijn vanuit hun eigen bu*siness continuity management* (BCM) plannen hard aan de slag om ICT-oplossingen te maken en/of ICT-*workarounds*. Veel ICT van de overheid en van vitale aanbieders is afhankelijk van de Digitale Service Providers en de ICT-industrie.

In voorkomend geval kunnen deskundigen op uitnodiging van de voorzitter de vergaderingen van generieke crisisgremia tot aan de Ministeriële Commissie Crisisbeheersing bijwonen. Te denken valt aan deskundigen op een specifiek terrein, vertegenwoordigers van betrokken andere overheden of vitale sectoren.

Er bestaan veel informele netwerken die relevant zijn tijdens een ICT-incident. Deze netwerken, waarin private partijen veelal een rol spelen, kunnen een belangrijke functie vervullen bij verloop en aanpak van het incident. Bijvoorbeeld voor het verkrijgen van relevante informatie, maar ook kunnen zij via hun informatiepositie een belangrijke rol spelen bij het oplossen van het incident.

Een of meer betrokken actoren kunnen zelf getroffen worden door een ICT-incident, waardoor ze hun crisisbeheersingstaken niet of in mindere mate kunnen uitvoeren. Dit kan leiden tot *multiplier*-effecten.

Digitale- en generieke crisisstructuur



Belangrijkste actoren per processtap

Processtap	Betrokken actor
Incidentanalyse (oordeelsvorming, duiding)	Digitale dienstverleners getroffen partijen
	NCSC
	CSIRT DSP
	AIVD
	MIVD
	ICT Response Board
	ISAC's
	Ministerie van Buitenlande Zaken
	NCTV
	Internationale netwerken
Attributie en opsporing	Digitale dienstverleners getroffen partijen
	Politie
	KMAR
	AIVD
	MIVD
	Openbaar Ministerie
	Ministerie van Buitenlandse Zaken
	Internationale netwerken
Bestrijding oorzaak	Digitale dienstverleners getroffen partijen
	Politie
	Sectorale CERT's
	NCSC
	Internationale netwerken
Gevolgbestrijding	Digitale dienstverleners getroffen partijen
	Getroffen partijen
	Veiligheidsregio's
Besluitvorming	Aanbieders vitale processen
	Aanbieders getroffen voorzieningen
	Burgemeester
	Voorzitter veiligheidsregio
	Vakminister
	Ministeriële Commissie Crisisbeheersing

Processtap	Betrokken actor
Informatie-voorziening	Digitale dienstverleners getroffen partijen
	NCSC
	NCC, LOCC
	Internationale netwerken
	Sectorale CERT's
	OKTT's
Notificatie slachtoffers	Digitale dienstverleners getroffen partijen
	Politie
	NCSC
	Sectorale CERT's
	OKTT's
Cyberdiplomatie	Ministerie van Buitenlandse Zaken
Evt. offensieve reactie	Ministerie van Algemene Zaken
	Ministerie van Buitenlandse Zaken
	Ministerie van Defensie
	Ministerie van Justitie en Veiligheid
	AIVD
	MIVD
Communicatie	Digitale dienstverleners
	Getroffen partijen
	CSIRT DSP
	NCSC
	Hulpverleningsdiensten
	Burgemeester
	Voorzitter veiligheidsregio
	Vakminister
	Openbaar Ministerie
	NCTV/Nationaal Kernteam Crisiscommunicatie
Toezicht en handhaving	Sectorale toezichthouders
Vervolging	Openbaar Ministerie
	Europol
	Eurojust


32A

4. Crisiscommunicatie

Crisiscommunicatie is gericht op het beantwoorden van de maatschappelijke informatiebehoefte, op schadebeperking en op betekenisgeving. 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.

In geval van een (dreiging van een) incident in het digitale domein met aanzienlijke maatschappelijke gevolgen stemmen alle relevante partijen hun timing en inhoud van communicatie zoveel mogelijk met elkaar af. Meer dan ooit is zichtbaarheid en tijdigheid in de communicatie doorslaggevend.

De grote complexiteit van digitale incidenten en de verwevenheid van het digitale met het fysieke domein maken het tijdig bepalen van gevolgen van cyberincidenten lastig. Maatschappelijke ontwrichting als gevolg van incidenten in het digitale domein worden vaak gekenmerkt door een razendsnelle verspreiding en meerdere cascade-effecten. De crisis ontstaat los van geografische grenzen, is mogelijk langdurig en er bestaat vaak lang onzekerheid over oorzaak, omvang en impact.

Uitgangspunt is dat we bij maatschappelijke ontwrichting als gevolg van incidenten in het digitale domein vasthouden aan bestaande structuren, rollen en werkwijzen, met oog voor het bijzondere dat een incident in het digitale domein met zich meebrengt.

Nationaal

Indien nodig ondersteunt de Eenheid Communicatie van het NCC het lokaal of regionaal bevoegd gezag en de betrokken departementale directies Communicatie met adviezen, middelen en een netwerk van ervaringsdeskundigen. De mogelijkheid bestaat om tussen rijk en veiligheidsregio/gemeente communicatie-liaisons uit te wisselen. Afstemming tussen nationaal en lokaal/regionaal niveau vindt dan plaats door middel van de liaison ter plaatse.

Zodra de nationale crisisorganisatie is geactiveerd, coördineert het NKC (Nationaal Kernteam Crisiscommunicatie) de pers- en publieksvoorlichting vanuit de rijksoverheid. Het NKC adviseert de crisisgremia op rijksniveau over de te volgen communicatiestrategie en de communicatieve gevolgen van (voor)genomen besluiten. Het NKC communiceert over zichtbare maatregelen en geeft procesinformatie over wat de overheid doet en waarom. Daarnaast formuleert het communicatiekaders en kernboodschappen, daar waar het de nationale bevoegdheden betreft en stemt deze af met de veiligheidsregio/direct betrokken gemeente(n).

Regionaal

De Wet op de veiligheidsregio's bepaalt dat het bestuur van de veiligheidsregio de verantwoordelijkheid heeft voor de informatievoorziening aan burgers over rampen en crises en over de maatregelen die de overheid heeft getroffen ter voorkoming en bestrijding ervan. Binnen gemeenten is de eindverantwoordelijkheid voor de crisiscommunicatie lokaal belegd bij de burgemeester van een getroffen gemeente, of de voorzitter van de veiligheidsregio. Dit laat onverlet de verantwoordelijkheden van een vakminister om binnen zijn domein specifieke informatie over mogelijke crises te geven.

De voorzitter van de veiligheidsregio of de burgemeester richt zich bij de communicatie op zijn/haar eigen regio/gemeente, daarbij rekening houdend met wat er in de eventuele buurgemeente/regio gecommuniceerd wordt.

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.

Verantwoordelijkheden

Crisiscommunicatie bij incidenten in het digitale domein volgt de reguliere bevoegdheden en verantwoordelijkheden. Uitgangspunt is dat we vasthouden aan bestaande structuren, rollen en werkwijzen, met oog voor het bijzondere dat een cyberincident met zich meebrengt. Iedere betrokken partij communiceert vanuit eigen verantwoordelijkheid over eigen onderwerpen, maar stemt centraal 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[8] 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.

Onderwerp	Organisatie
Feiten lokaal	Hulpverleningsdiensten
Duiding en handelingsperspectieven lokaal	Burgemeester binnen driehoek/ Voorzitter veiligheidsregio (bij opzettelijk handelen scenario)
Handhaving openbare orde en veiligheid	Burgemeester/Voorzitter veiligheidsregio
Veiligheidsmaatregelen lokaal	Burgemeester/Voorzitter veiligheidsregio (maatregelen over openbare orde) en OM (maatregelen in het kader van opsporing)
Duiding nationale veiligheid en veiligheidsmaatregelen algemeen	NCTV
Duiding en maatregelen technisch operationeel	CSIRT DSP (in ieder geval in eerste instantie)
	NCSC
	NCTV – NCC communiceert deze duiding met de betrokken veiligheidsregio's
Opsporingsonderzoek	Openbaar Ministerie
Feiten en duiding, handelingsperspectieven nationaal	Betrokken vakminister
Gevolgen voor eigen organisatie en medewerkers, directe gevolgen voor klanten of leveranciers	Publieke en private partijen

8 Dit overzicht geeft de hoofdlijnen weer. Per situatie zal in overleg met elkaar bepaald worden wie wanneer en hoe communiceert.

Algemene uitgangspunten voor de crisiscommunicatie

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

Aandachtspunten voor crisiscommunicatie bij een digitaal incident

- Zolang niet zeker is of een incident opzettelijk handelen is, vermijden we verwijzingen naar mogelijke oorzaken, duur en omvang;
- Verminder aantal (digitale) middelen dat kan worden ingezet bij uitval;
- Wanneer vanuit veiligheidsoverwegingen communicatie over 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 appelleert aan de veerkracht van individuele burgers en van de Nederlandse samenleving als geheel;
- Houd bij de communicatie rekening met het BIV-principe: betrouwbaarheid (continuïteit), integriteit (manipulatie) en verantwoordelijkheid (lekken).
- Crisispreparatie: vanwege de complexiteit en onvoorspelbaarheid van incidenten in het digitale domein is het van belang om vooraf per scenario het netwerk van communicatiepartners in kaart te brengen en afspraken te maken.

In de communicatienotitie 'Communicatie bij incidenten in het digitale domein' (NCTV 2020) wordt de communicatiestrategie op nationaal niveau en de rolverdeling in de communicatie tussen partners op (inter)nationaal en regionaal niveau beschreven, rekening houdend met bovenstaande aandachtspunten.

Bijlagen

1. Overzicht vitale processen
2. Meest relevante wet- en regelgeving
3. Rolbeschrijvingen
4. Relevante bronnen en literatuur
5. Afkortingen

Bijlage 1

Overzicht vitale processen

Deze bijlage bevat een overzicht van de Nederlandse vitale processen, conform de vitaliteitsbeoordeling zoals door het rijk in 2017 vastgesteld.

Er is onderscheid gemaakt tussen de categorie A en de categorie B om recht te doen aan de diversiteit binnen de vitale infrastructuur, om te kunnen prioriteren bij onder andere incidenten en om maatwerk bij weerbaarheidsverhogende maatregelen mogelijk te maken. De processen hiernaast zijn als vitaal geïdentificeerd in Nederland. Categorie A vitale processen hebben grotere gevolgen bij uitval dan categorie B vitale processen.

Categorie A

In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria (economisch, fysiek of sociaal maatschappelijk) voor categorie A raakt en daarnaast ook voldoet aan het criterium van cascade gevolgen:

- Economische gevolgen: > ca. 50 miljard euro schade of ca. 5,0 % daling reëel inkomen
- Fysieke gevolgen: meer dan 10.000 personen dood, ernstig gewond of chronisch ziek
- Sociaal maatschappelijke gevolgen: meer dan 1 miljoen personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen
- Cascade gevolgen: uitval heeft als gevolg dat minimaal twee andere sectoren uitvallen.

Categorie B

In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:

- Economische gevolgen: > ca. 5 miljard euro schade of ca. 1,0 % daling reëel inkomen
- Fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek
- Sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen

Vitale processen	Categorie	Sector	Ministerie
Landelijk transport en distributie elektriciteit	A	Energie	EZK
Regionale distributie elektriciteit	B		
Gasproductie, landelijk transport en distributie gas	A		
Regionale distributie gas	B		
Olievoorziening	A		
Internet en datadiensten	B	ICT/Telecom	EZK
Internettoegang en dataverkeer	B		
Spraakdienst en SMS*	B		
Plaats- en tijdsbepaling middels GNSS	B		IenW
Drinkwatervoorziening	A	Drinkwater	IenW
Keren en beheren waterkwantiteit	A	Water	IenW
Vlucht- en vliegtuigafhandeling	B	Transport	IenW
Scheepvaartafwikkeling	B		
Grootschalige productie/verwerking en/of opslag (petro) chemische stoffen	B	Chemie	IenW
Opslag, productie en verwerking nucleair materiaal	A	Nucleair	IenW
Toonbankbetalingsverkeer	B	Financieel	FIN
Massaal giraal betalingsverkeer	B		
Hoogwaardig betalingsverkeer tussen banken	B		
Effectenverkeer	B		
Communicatie met en tussen hulpdiensten middels 112 en C2000	B	OOV	JenV
Inzet politie	B		
Basisregistraties personen en organisaties	B	Digitale overheidsprocessen	BZK
Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)	B		
Elektronisch berichtenverkeer en informatie-verschaffing aan burgers	B		
Identificatie en authenticatie van burgers en bedrijven	B		
Inzet defensie	B	Defensie	DEF

* Voor alle ICT/Telecomprocessen geldt dat deze zowel via vaste als mobiele aansluitingen en infrastructuur worden verzorgd, met uitzondering van SMS, hier geldt alleen dat deze via mobiele aansluitingen en infrastructuur worden verzorgd.

Bijlage 2

Meest relevante wet- en regelgeving

Deze bijlage bevat een beknopt overzicht van de meest relevante wet- en regelgeving om de veiligheid van netwerken en informatiesystemen te waarborgen.

Wet beveiliging netwerk- en informatiesystemen

De Wet beveiliging netwerk- en informatiesystemen (Wbni)[9] streeft ernaar digitale weerbaarheid van vitale aanbieders, de rijksoverheid en digitale dienstverleners te vergroten. De Wbni regelt een meldplicht van incidenten en een zorgplicht voor het treffen van de juiste beveiligingsmaatregelen en is erop gericht de gevolgen van cyberincidenten te beperken en maatschappelijke ontwrichting te voorkomen. In de Wbni is nader bepaald wanneer er sprake is van een meldplichtig incident en welke drempelwaardes daartoe zijn gespecificeerd.

Alle vitale aanbieders hebben op grond van de Wbni recht op informatie, adviezen en bijstand van het Nationaal Cyber Security Centrum (NCSC) waarmee zij de continuïteit van de door hen geleverde diensten kunnen borgen. Het NCSC vervult daarmee de CSIRT functie voor vitale aanbieders.

Naast het recht op bijstand hebben de meeste vitale partijen ook plichten onder de Wbni. Daarbij wordt onderscheid gemaakt tussen twee soorten aanbieders 'aanbieders van een essentiële dienst' (AED's) en 'andere aangewezen vitale aanbieders' (AAVA's):

1. AED's hebben de plicht om incidenten met aanzienlijke gevolgen voor continuïteit van de dienstverlening te melden bij de sectorale toezichthouder. AED's hebben de (zorg)plicht om passende technische en organisatorische maatregelen te nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. Ook hebben deze partijen de plicht om passende maatregelen te treffen om incidenten te voorkomen die de beveiliging aantasten van de voor de verlening van de dienst gebruikte netwerk- en informatiesystemen. Daarnaast hebben ze de plicht de gevolgen van dergelijke incidenten zo veel mogelijk te beperken. De verschillende sectorale toezichthouders zien er op toe dat AED's zo veel mogelijk aan deze zorgplicht proberen te voldoen. Deze zorgplicht is nader uitgewerkt in het Besluit beveiliging netwerk- en informatiesystemen (Bbni)[10].

2. AAVA's zijn vitale aanbieders die niet zijn opgenomen in de Europese Netwerk en Informatie Beveiliging (NIB) richtlijn maar die wij in Nederland wel vitaal achten of vitale aanbieders die al Europese wetgeving hebben die een zorgplicht voorschrijft van vergelijkbaar of hoger niveau. Deze partijen hebben de plicht om incidenten met directe gevolgen voor de continuïteit van hun dienst te melden bij het NCSC.

Een belangrijke rol is daarnaast middels de Wbni toebedeeld aan de sectorale toezichthouders. Zij houden toezicht op de invulling van de zorgplicht, waarvan onderdeel is dat de vitale aanbieders maatregelen nemen om incidenten te voorkomen en om de continuïteit van een essentiële dienst zo snel mogelijk te herstellen. Als organisaties onvoldoende maatregelen nemen, waardoor er mogelijk een gevaar voor de nationale veiligheid bestaat, kan een toezichthouder ingrijpen door middel van bestuursdwang of boetes.

9 De Wbni implementeert de netwerk- en informatieveiligheid richtlijn van de Europese Unie.

10 Samen met de Wbni is ook het Besluit beveiliging netwerk- en informatiesystemen (Bbni) in werking getreden. In het Bbni worden vitale aanbieders aangewezen, die daarmee vallen onder de verplichtingen van de Wbni.

Autoriteit en toezichthouder per AED-sector

AED-sector	Bevoegde autoriteit	Toezichthouder dienst
Energie	Minister van Economische Zaken en Klimaat	Agentschap Telecom
Digitale infrastructuur	Minister van Economische Zaken en Klimaat	Agentschap Telecom
Bankwezen	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Infrastructuur voor de financiële markt	De Nederlandsche Bank N.V.	De Nederlandsche Bank N.V.
Vervoer	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Levering en distributie van drinkwater	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport
Gezondheidszorg	Minister voor Medische zorg en Sport	Inspectie Gezondheidszorg en Jeugd

Telecommunicatiewet

De belangrijkste wettelijke bepalingen ten aanzien van telecommunicatie die een rol spelen bij de crisisbeheersing zijn opgenomen in hoofdstuk 11a en in hoofdstuk 14 van de Telecommunicatiewet.

Risico- en crisisbeheersingsmaatregelen (hoofdstuk 11a)

In algemene zin hebben aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten de plicht passende technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid en de integriteit van hun netwerken en diensten te beheersen. Daarnaast moeten zij alle noodzakelijke maatregelen nemen om de beschikbaarheid van de openbare telefoondiensten over de openbare elektronische communicatienetwerken zo volledig mogelijk te waarborgen in geval van een technische storing of uitval van het elektriciteitsnetwerk.

Verder zijn aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten verplicht de minister onverwijld in kennis te stellen van een inbreuk op de veiligheid, of een verlies van integriteit, waardoor de continuïteit van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten in belangrijke mate werd onderbroken

Buitengewone omstandigheden (Hoofdstuk 14)

Als er buitengewone omstandigheden zijn afgekondigd, heeft de minister van EZK uitgebreide bevoegdheden om aanwijzingen aan iedere aanbieder van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten op te leggen. De aanwijzingen die in buitengewone omstandigheden gegeven kunnen worden liggen op het vlak van:

- de instandhouding en exploitatie van openbare telecommunicatienetwerken en -diensten, hieronder vallen bijvoorbeeld prioritering of juist beperking van communicatie; het eventueel uitschakelen van diensten of een gewijzigde vorm van levering (bijvoorbeeld tijdelijk gratis bellen of het toelaten van anderen dan de eigen abonnees, maar denk ook aan het prioriteren of limiteren van bepaalde vormen van communicatie);
- de instandhouding en exploitatie dan wel beperking of beëindiging van het gebruik van radiozendapparaten (bijv. in- of uitschakelen van zenders of straalverbindingen);
- De bereikbaarheid van het alarmnummer 112 zo goed mogelijk waarborgen via de verplichting om een voorziening te installeren ter voorkoming van congestie in de bereikbaarheid van 112.

Ten behoeve van de voorbereiding op buitengewone omstandigheden kan de minister van EZK aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten aanwijzen die verplicht zijn voorbereidingen te treffen om aanwijzingen tijdens buitengewone omstandigheden te kunnen uitvoeren. Deze voorbereidingen liggen op het vlak van:

- deelname aan oefeningen en/of overleggen. Het NCO-T is een overleg dat hieronder valt;
- implementeren van continuïteitsplanning en crisismanagement;
- rapportage over de voorbereidingen.

Tijdens een crisis of incident, waarbij geen buitengewone omstandigheden zijn afgekondigd, kan de minister van EZK in overleg treden met de vitale spelers uit het proces, dat wil zeggen, via het NCO-T. De als lid daarvan aangewezen bedrijven kunnen verzocht worden mee te werken aan eventuele responsacties.

Aanwijzingsbevoegdheid (Hoofdstuk 18)

In hoofdstuk 18 staan aanvullende bepalingen voor de Telecommunicatiewet, inclusief bepalingen met betrekking tot de aanwijzingsbevoegdheid van de minister van EZK om inlichtingen te vorderen (18.7) en ook aanwijzingen met betrekking tot de instandhouding en exploitatie van communicatienetwerken en het verzorgen en gebruiken van hun openbare elektronische communicatiediensten, wanneer dit noodzakelijk is ter beëindiging van strafbaar gedrag jegens een persoon (in overeenstemming met de minister van JenV) of wanneer dit noodzakelijk is in het belang van de veiligheid van de staat (in overeenstemming met de minister van Binnenlandse Zaken en Koninkrijksrelaties) (18.9).

Wet computercriminaliteit

Met de Wet computercriminaliteit, in werking getreden op 1 maart 1993, is het Wetboek van Strafvordering aangevuld met bevoegdheden op het gebied van onderzoek van geautomatiseerde werken en zijn specifieke strafbepalingen, zoals computervredebreuk toegevoegd aan het Wetboek van Strafrecht. Voorbeelden van computercriminaliteit zijn:

- Computervredebreuk: ongeoorloofd toegang verschaffen tot een computersysteem;
- Het kopiëren van vertrouwelijke gegevens;
- Ongeoorloofd computerdata verwijderen of aanpassen;
- Ongeoorloofd computersystemen uitschakelen of onbruikbaar maken;
- Het versturen van virussen;
- Fraude: met behulp van computers en valsheid in geschrifte met betrekking tot computerdata, bijvoorbeeld door berichten te onderscheppen en te veranderen zoals met een *man-in-the-middle-attack*;
- Het valselijk beschuldigen of bedreigen via een sociaal netwerk of e-mail.

Deze wetgeving is inmiddels enige keren aangescherpt, het meest recent door middel van de Wet Computercriminaliteit III, die op 1 maart 2019 in werking is getreden. Deze wet geeft Justitie en politie nieuwe bevoegdheden om computercriminaliteit beter te bestrijden. Zo is onder andere een bevoegdheid gecreëerd om heimelijk en op afstand ('online') computers binnen te gaan voor de opsporing van ernstige delicten, zoals kinderpornografie, drugshandel of liquidaties. Verder wordt onder meer heling van computergegevens als zelfstandig delict strafbaar. Daarmee kan iemand worden aangepakt die over gegevens van anderen beschikt, ook als niet bewezen kan worden dat hij zelf die gegevens heeft overgenomen.

Bestuurlijke Netwerkkaarten Crisisbeheersing

Naast de hiervoor opgenomen wet- en regelgeving bieden de Bestuurlijke Netwerkkaarten Crisisbeheersing en de bijbehorende bevoegdhedenschema's een nader inzicht van relevante wetgeving inclusief bevoegdheden en crisispartners. De netwerkkaarten zijn bedoeld als handvat, oriëntatiepunt en naslagwerk tijdens de respons. De schema's bieden een breed overzicht van crisisbevoegdheden en -verplichtingen.[11]

Coordinated vulnerability disclosure beleid

Naast wet en regelgeving kennen steeds meer private partijen een eigen *coordinated vulnerability disclosure* beleid waarmee zij onderzoekers en hackers aanmoedigen om kwetsbaarheden op een verantwoorde wijze te melden.

11 https://www.ifv.nl/kennisplein/Paginas/bestuurlijke-netwerkkaarten-crisisbeheersing.aspx

Bijlage 3

Rolbeschrijvingen

A. Cybernetwerk

Nationaal Cyber Security Centrum (NCSC)

Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland en nationaal contactpunt voor digitale dreigingen en incidenten. Het NCSC verricht als het Computer Security Incident Response Team (CSIRT) voor de Rijksoverheid en vitale aanbieders, waaronder aanbieders van essentiële diensten, de operationele coördinatie bij een grote uitval of verstoring. Het NCSC is onderdeel van het ministerie van JenV en verricht zijn activiteiten binnen de in de Wbni genoemde taken ook namens de minister. Wettelijke kerntaken zijn in het bijzonder:

Met het oog op het voorkomen en beperken van maatschappelijke ontwrichting door cyberdreigingen en –incidenten en het versterken van de digitale weerbaarheid in de samenleving:

- Het bijstaan van Rijksoverheid en vitale aanbieders bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen;
- Het informeren en adviseren van deze aanbieders en anderen in en buiten Nederland over dreigingen en incidenten met betrekking tot informatiesystemen van de Rijksoverheid en vitale aanbieders;
- Het verrichten van analyses en technisch onderzoek ten behoeve van de hierboven genoemde taken naar aanleiding van (aanwijzingen voor) dreigingen en incidenten bij de Rijksoverheid en vitale aanbieders;
- Centraal contactpunt voor buitenlandse CSIRT's;
- De CSIRT-taken voor AED's zoals genoemd in de NIB-richtlijn.

Het NCSC heeft verder tot taak, ter voorkoming van nadelige maatschappelijke gevolgen in en buiten Nederland, om bepaalde, in de Wbni genoemde, organisaties te informeren over dreigingen en incidenten betreffende andere informatiesystemen dan die van Rijk en vitaal, voor zover die informatie is verkregen bij de uitoefening van bovenstaande taken. Ook kan het NCSC bijvoorbeeld publiek in algemene zin adviseren, op het gebied van digitale dreigingen en incidenten.

Het NCSC heeft daarnaast in geval van een opschaling van de nationale crisisstructuur tot taak een gemeenschappelijk beeld en duiding van de ICT-verstoring te geven op basis van de informatie die zij ontvangt van haar partners. Het NCSC coördineert het pubiek-privaat Nationaal Respons Netwerk (NRN). Dit netwerk is opgericht om de gezamenlijke respons op cybersecurity-incidenten te versterken. Verder is het NCSC nationaal contactpunt voor het EU CSIRT netwerk en het IWWN.

Digital Trust Center (DTC) en CSIRT DSP

Het Ministerie van Economische Zaken en Klimaat draagt bij aan het verhogen van de cybersecurity bij het (MKB) bedrijfsleven door de inzet van het Digital Trust Center (DTC) en het CSIRT DSP. Daarnaast dienen digitale dienstverleners op grond van de Wbni sinds 1 januari 2019 incidenten (incident = iedere gebeurtenis met een schadelijk effect op de beveiliging van netwerk- en informatiesystemen) niet alleen te melden bij het Agentschap Telecom maar ook bij het CSIRT DSP. Hierbij gaat het om incidenten met aanzienlijke gevolgen.

Dit doen het DTC en het CSIRT DSP door:
- Bewustwording cyber security (DTC)
- Monitoring (CSIRT DSP)
- Proactieve ondersteuning bij preventie (DTC en CSIRT-DSP)
- Actieve en reactieve ondersteuning als het misgaat (CSIRT-DSP)

Het DTC en het CSIRT DSP liggen voor wat betreft hun functies dicht bij elkaar. Belangrijke verschillen liggen in hun doelgroepen en doelgroep-benadering en de inkadering van hun taken, als volgt:
- DTC richt zich op het niet-vitale bedrijfsleven en daarmee dus op een enorm brede doelgroep. Het CSIRT DSP richt zich heel specifiek op een deelverzameling, namelijk de digital service providers (DSP's);
- Het DTC benadert haar doelgroep via brede communicatiekanalen en draagt daarop de generieke boodschap uit met betrekking tot verhogen van de weerbaarheid/ cyber security. Het CSIRT DSP draagt specifiekere boodschappen uit sterk gericht op ICT en concrete oplossingen voor cybersecurity;
- Het DTC heeft als taak algemene voorlichting. Het CSIRT DSP heeft de wettelijke taak van aannemen, registreren en reageren van/op incidentmeldingen bij haar specifieke doelgroep.

Het CSIRT DSP zorgt voor de sector van DSP's voor:
- Het kunnen aannemen en registeren van meldingen over incidenten bij DSP's;
- Het daarop reageren bij voorkeur door middel van directe hulp en het verspreiden van dreigingsinformatie aan DSP's en ten minste het bevestigen van de gedane incidentmelding.
- 24/7 ondersteuning vanuit een beveiligde fysieke werkplek en met behulp van robuuste beveiligde systemen en infrastructuur.

Zowel DTC als CSIRT DSP werken nauw samen met het NCSC.

Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden

Om snel dreigingen te kunnen herkennen is het uitwisselen van kennis, informatie en expertise van belang. In de Nederlandse Cyber Security Agenda (NCSA) is daarom de ambitie geformuleerd om te komen tot een landelijk dekkend stelsel van cybersecurity samenwerkingsverbanden zodat er breder, efficiënter en effectiever informatie wordt gedeeld tussen publieke en private partijen. In Nederland wordt al door een groot aantal organisaties, samenwerkingsverbanden en informatieknooppunten informatie uitgewisseld. In het stelsel wordt door het NCSC informatie uitgewisseld met de op dit moment verschillende aangewezen CERT/CSIRT organisaties:
- De Informatiebeveiligingsdienst (IBD): De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en onderdeel van de Vereniging Nederlandse Gemeenten.
- SURFcert: SURFcert is het incident response team voor bij SURF aangesloten instellingen. In SURF werken onderwijs- en onderzoeksinstellingen samen aan ICT-voorzieningen en -innovatie om de kansen van digitalisering ten volle te benutten.
- CERT Waterschapsmanagement (CERT-WM): Het CERT-WM is de CERT voor de Waterschappen en een samenwerking tussen RWS en de Waterschappen.
- Zorg-CERT (Z-CERT): Z-CERT is ontstaan vanuit de zorg zelf (geïnitieerd vanuit de academische ziekenhuizen, als stichting), dat wordt ondersteund vanuit het ministerie van VWS (en de Directie Informatiebeleid) om uit te bouwen in diensten en aangesloten instellingen uit de zorg. Vrijwel alle ziekenhuizen zijn aangesloten en een toenemend aantal andere instellingen.[12]

In sommige gevallen kan het NCSC informatie uitwisselen met niet aangewezen CERT/CSIRT organisaties. De aanwijzing tot een CERT/CSIRT maakt vooral dat tot personen herleidbare gegevens kunnen worden gedeeld (bijvoorbeeld IP-adressen) en onder extra voorwaarden vertrouwelijke, tot een aanbieder herleidbare informatie. Bij een ernstige crisis kan onder voorwaarden zelfs vertrouwelijke informatie gedeeld worden met niet-aangewezen CERT's (en andere organisaties), als dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken.

Naast computercrisisteams, kan het NCSC ook informatie delen met organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren op het gebied van cybersecurity. Door aanwijzing in het kader van de Wbni kan met deze organisaties, zogenaamde OKTT's, onder voorwaarden, informatie over dreigingen, incidenten en kwetsbaarheden, inclusief persoonsgegevens, worden gedeeld.

12 Per 24 januari 2020 zijn IBD, SURFCert, CERT-WM en Z-CERT bij ministeriële regeling aangewezen als computercrisisteams als bedoeld in de Wbni.

ICT Response Board

De ICT Response Board (IRB) adviseert de nationale crisisstructuur over mogelijke ICT-gerelateerde maatregelen voor de instandhouding van vitale processen. De IRB fungeert als schakelpunt tussen het technische en het bestuurlijke niveau. Aanbieders van vitale processen worden bijeen geroepen, wisselen informatie uit en maken met elkaar een analyse. Deelnemers zijn sectoren (bijvoorbeeld telecom/ICT, energie en financiële instellingen) of betrokken vitale overheidsdiensten. De samenstelling is flexibel. Experts worden naar behoefte uitgenodigd om uitleg te geven over het specifieke probleem dat zich voordoet. De IRB wordt gefaciliteerd door het NCSC en het ministerie van EZK. EZK levert de voorzitter, het NCSC de informatiecoördinator en de secretaris.

Information Sharing and Analysis Centres

Op structurele basis wordt er via een stelsel van Information Sharing and Analysis Centres (ISACs) overleg gevoerd. Een Information Sharing and Analysis Centre (ISAC) is een middel om met organisaties in dezelfde sector samen te werken om de digitale weerbaarheid van deze organisaties te vergroten. Een ISAC is een sectoraal overleg over cybersecurity. In een ISAC wordt een vertrouwde omgeving gecreëerd met organisaties uit dezelfde sector om gevoelige en vertrouwelijke informatie over incidenten, dreigingen, kwetsbaarheden, maatregelen en leerpunten op het gebied van cybersecurity te delen. Er is geen 'standaardvorm' van een ISAC. Een samenwerking in een ISAC kan formeel of informeel zijn; gestructureerd of flexibel; met fysieke vergaderingen, teleconferenties, via een digitaal platform of een mix van deze drie. De sectoren kiezen zelf de best passende vorm en zijn zelf eigenaar van de ISAC. Het NCSC en de ISAC's staan in nauw contact met elkaar.

Cyber Security Raad

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en bedrijfsleven (via het kabinet) en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen. De CSR stelt zich o.a. de volgende taken:

1. gevraagd en ongevraagd verstrekken van advies aan de regering en private partijen;
2. adviseren over de implementatie van de nationale cybersecurity strategie;
3. het leveren van een bijdrage aan de Nationale Cyber Security Research Agenda;
4. adviseren van de crisisorganisatie in Nederland tijdens grootschalige cyberincidenten.

B. Generieke crisisgremia

De **Ministeriële Commissie Crisisbeheersing** (MCCb) is verantwoordelijk voor de coördinatie en besluitvorming op politiek-bestuurlijk niveau over de treffen maatregelen waaronder de toepassing van bevoegdheden. De uitvoering van de maatregelen inclusief de toepassing van bevoegdheden geschiedt in overeenstemming met de in het MCCb genomen besluiten. De besluiten van de MCCb vormen het kader voor de uitvoering daarvan door publieke en private partners.

De **Interdepartementale Commissie Crisisbeheersing** (ICCb) is een coördinerend en besluitvormend orgaan op hoog-ambtelijk niveau (directeur, DG), onder voorzitterschap van de NCTV. De door de ICCb genomen besluiten worden zo nodig ter goedkeuring voorgelegd aan de MCCb. MCCb en ICCb worden ondersteund en geadviseerd door een **Inter-departementaal Afstemmingsoverleg** (IAO).

Het **Nationaal Crisiscentrum** (NCC) is het interdepartementaal coördinatiecentrum en knooppunt van en voor de bestuurlijke informatievoorziening en de crisiscommunicatie. Het NCC is de ondersteunende c.q. uitvoerende staf en het facilitair bedrijf ten dienste van de (voorbereiding van de) interdepartementale crisisbesluitvorming, zowel op ambtelijk als op politiek-bestuurlijk niveau.

- De rolverdeling tussen het lokale/regionale en nationale niveau ligt bij incidenten met een digitale component in lijn met de reguliere verantwoordelijkheden en structuren;
- Uitgangspunt is om zoveel mogelijk aan te sluiten en gebruik te maken van de reguliere structuren, indien nodig aangevuld met specifieke kennis of expertise op het gebied van cyber en het digitale domein in relatie tot crisisbeheersing;
- Basis zijn op nationaal niveau de afspraken en structuren van het Nationaal Handboek Crisisbesluitvorming (NHC, 2016).

Het NCC blijft te allen tijde het 24/7 Informatieknooppunt en contactpunt van het rijk en staat tijdens incidenten met een digitale component met impact op lokale gezagen of veiligheidsregio's in rechtstreekse verbinding met het NCSC en LOCC, bijvoorbeeld ten aanzien van onderwerpen als informatievoorziening en crisiscommunicatie.

Het **Landelijk Operationeel Coördinatie Centrum** (LOCC) voert informatiemanagement voor operationele vraagstukken uit, voert regie over bijstand en (schaarse, nationale) capaciteiten. Verder levert het LOCC operationeel advies ten behoeve van bestuurlijke besluitvorming op bovenregionaal en nationaal niveau. Het LOCC faciliteert tevens het LOCC-Bovenregionaal en/of het LOCC-Nationaal (resp. LOCC-B of LOCC-N). Dit is een adviesgremium op strategisch niveau, specifiek bedoeld om bestuurlijk draagvlak voor genomen (of te nemen) bestuurlijke besluiten over de operationele crisisbeheersing te creëren en om de voortgang te volgen opdat bijstelling van advies mogelijk is. Het LOCC B/N wordt geactiveerd op verzoek van (één of meerdere) voorzitters Veiligheidsregio's (LOCC-B), of op verzoek van de NCTV (LOCC-N).

Het **Nationaal Kernteam Crisiscommunicatie** (NKC) adviseert ICCb en MCCb over de te volgen communicatiestrategie en de communicatieve gevolgen van (voor)genomen besluiten. Het NKC ontwikkelt en coördineert de communicatie van het rijk en de rijksoverheid en stemt deze waar nodig af met de betrokken andere publieke en private partners.

C. Ministeries en organisaties

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Departementale Chief Information Officers (CIO's) en de CIO Rijk

De CIO-Rijk heeft binnen het Rijk een belangrijke rol op het gebied van informatiebeveiliging. De CIO-Rijk stelt kaders en richtlijnen voor het niveau van digitale beveiliging via de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast kan de CIO-Rijk vragen om beveiligingsadviezen op te volgen door middel van het 'comply or explain' principe. De CIO Rijk is voorzitter van het CIO Beraad, waaraan de CIO's van de ministeries en enkele grote uitvoeringsorganisaties deel nemen.

Bij een (dreigend) ICT-incident is/zijn de departementale crisisorganisatie(s) aanspreekpunt voor de NCTV. Daar waar een (dreigend) ICT-incident meerdere departementen raakt is en inhoudelijke coördinatie nodig is, dan is de CIO Rijk hiervoor het aanspreekpunt, als voorzitter van het CIO Beraad. De CIO Rijk kan, gehoord hebbende het CIO-beraad, escaleren naar de ambtelijke/politieke top van BZK. De CIO Rijk kan bij een departement-overstijgend incident deelnemen aan een interdepartementaal crisisteam.

Departementale BVA's en RijksBVA

De RijksBVA is belast met het bewaken van het integrale karakter en de consistentie van de rijksbrede kaders voor beveiliging en het toezicht op de werking van de integrale beveiliging van de Rijksdienst. De BVA is de departementale adviseur en toezichthouder op de implementatie van de kaders voor integrale beveiliging. Departementaal werken de CIO en BVA hiertoe samen, ieder vanuit zijn specifieke rol en verantwoordelijkheid. Op departementaal niveau wordt de BVA geïnformeerd door de CIO bij ernstige incidenten en –crises in het digitale domein. De CIO Rijk informeert de RijksBVA over ernstige dreigingen, -incidenten en -crises. De RijksBVA kan namens zijn secretaris-generaal, na instemming van de departementale secretaris-generaal, in het geval van een (mogelijke) ernstige inbreuk op de beveiliging van departement overstijgende systemen of diensten – of een risico daarop – aanwijzingen geven aan iedere ambtenaar om eventuele gevolgen van een inbreuk op de beveiliging te beperken.

Directie Informatiesamenleving en Overheid (I&O)

Taak van deze directie is het concretiseren van de visie op de rol van de overheid in de informatiesamenleving. I&O neemt de regie op de interbestuurlijke uitwerking en uitvoering hiervan daar waar dat de publieke belangen en de maatschappelijke orde in de digitale samenleving dient en zo nodig versterkt.

Verschillende Computer Emergency Response Teams (CERT's) vallen onder verantwoordelijkheid van BZK. Provincies hebben de CERT-functie op dit moment individueel geregeld en verkennen de mogelijkheid van aansluiting bij een overheidsbrede CERT. De waterschappen hebben sinds april 2017 samen met Rijkswaterstaat een CERT Watermanagement en de gemeenten hebben sinds 2013 een eigen CERT, de Informatiebeveiligingsdienst (IBD).

Algemene Inlichtingen- en Veiligheidsdienst

De AIVD verricht onderzoek naar digitale aanvallen die een potentiële bedreiging vormen voor de nationale veiligheid. Hierdoor kan de AIVD dergelijke aanvallen detecteren en mitigeren, slachtoffers informeren en bewustwordingspresentaties geven aan mogelijke doelwitten. Daarnaast verstrekt de AIVD informatiebeveiligingsadviezen op maat aan de Rijksoverheid en andere belanghebbenden, zoals vitale bedrijven. Het doel van deze adviezen is de weerstand tegen digitale aanvallen te verhogen en (digitale) schade te beperken of te voorkomen. Door de toegang tot geheime informatie geeft de AIVD uniek en gedegen beveiligingsadvies en stelt anderen in staat te handelen.

Nauwe samenwerking met de MIVD is cruciaal bij het uitvoeren van deze taken. Daarnaast werkt de AIVD intensief samen met andere nationale en internationale partners. Zo delen de AIVD, MIVD en het NCSC binnen het Nationaal Detectie Netwerk (NDN) relevante dreigingsinformatie waardoor deze organisaties binnen hun eigen verantwoordelijkheden maatregelen kunnen treffen.

Ministerie van Buitenlandse Zaken

Als gevolg van een exponentiële toename in de digitale dreiging vanuit statelijke actoren neemt de politieke wil om onverantwoordelijk gedrag in cyberspace aan de kaak te stellen toe. De minister van BZ is verantwoordelijk voor de diplomatie en politieke respons op cyberaanvallen en coördineert voor Nederland de diplomatieke en politieke respons in like-minded-, EU-, OVSE- en NAVO-verband.

Daarnaast heeft het ministerie van Buitenlandse Zaken en de ambassades in bijzonder een belangrijke monitoring- en signaleringsfunctie ter bevordering van het situationeel bewustzijn.

In voorkomende gevallen is de Directie Veiligheidsbeleid het eerste aanspreekpunt bij internationale incidenten in het digitale domein. Als de nationale crisisstructuur in werking is getreden, is de crisiscoördinator van Buitenlandse Zaken het eerste aanspreekpunt.

Ministerie van Defensie

Op verzoek van de civiele autoriteiten kan het Ministerie van Defensie in het kader van zijn derde hoofdtaak ondersteuning leveren bij rampenbestrijding en crisisbeheersing alsmede bij rechtshandhaving in Nederland of in internationaal verband.
In de Catalogus Nationale Operaties zijn verschillende Defensie capaciteiten en hun beschikbaarheid voor inzet in het civiele domein opgenomen. Deze capaciteiten zijn in voorkomend geval ook beschikbaar voor de beheersing van incidenten in het digitale domein.

De **Hoofddirectie Bedrijfsvoering** (HDBV) vervult binnen Defensie de rol van CIO (Chief Information Officer) en is daarmee de vertegenwoordiger in het (reguliere) interdepartementale ICT overleg tussen CIO's. Gelet op haar taken op het gebied van bedrijfsvoering is de HDBV (eind)verantwoordelijk voor de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de Defensie ICT systemen.

In het geval van opschaling van de nationale crisisstructuur neemt de **Bestuursstaf** (Directie Operaties) deel aan het Informatieteam, IAO en ICCb ter voorbereiding op het MCCb. Bij een specifiek incident in het digitale domein kan hierdoor een combinatie van DOPS / HDBV (al dan niet gesteund door materie deskundige specialisten zoals het DCC en/of DCSC) betrokken zijn bij de opschaling van de nationale crisisstructuur (mandaat in fysieke operaties versus CIO rol).

Het **Defensie Cyber Security Centre** (DCSC) heeft tot taak het onderkennen, analyseren en gecoördineerd mitigeren dan wel opheffen van cyberdreigingen tegen en/of verstoringen van Defensie IT middelen. Daarnaast richt het DCSC zich op samenwerkingsverbanden met andere departementen in het kader van het in rijks breed verband mitigeren van cyberdreigingen. DCSC voert deze taken zowel proactief als reactief uit, enerzijds door middel van informatie-uitwisseling alsmede het bijhouden van technologische ontwikkelingen, anderzijds door het (op aanvraag van civiele autoriteiten) uitvoeren van reviews op architectuur/ ontwerpen/infrastructuur en het uitvoeren van testen teneinde een hoger beveiligingsniveau tegen digitale dreigingen en aanvallen te realiseren.

Het **Defensie Cybercommando** (DCC) is verantwoordelijk voor de ontwikkeling en inzet van militaire offensieve cyber capaciteit. Het DCC beschikt hiertoe over teams van cyberadviseurs/-operators . Door deels generieke cyberkennis kan het DCC bij cyberincidenten eventueel gevraagd worden uitvoering te geven aan militaire bijstand aan civiele autoriteiten . Het DCC heeft voor zijn reguliere taken contacten en samenwerkingsverbanden (interdepartementaal) met partners en actoren binnen en buiten Defensie in het kader van informatievoorziening rondom cyberincidenten en personele uitwisselingen voor kennisopbouw. Daarnaast beschikt het DCC over een groot aantal cyberreservisten die in het dagelijks leven werkzaam zijn bij andere publieke of private organisaties maar eventueel kunnen worden opgeroepen als de nood hoog is.

Het DCSC werkt nauw samen met andere organisaties zoals het NCSC, de NATO Computer Incident Response Capability (NCIRC) en CERT-organisaties van over de gehele wereld. Met het NCSC zijn afspraken gemaakt over wederzijdse ondersteuning en bijstand in het cyberdomein in het belang van een gezamenlijk beeld van digitale dreigingen en de optimale coördinatie van operationele activiteiten. Bij incidenten verlenen zij elkaar (personele) assistentie en technische middelen (reguliere samenwerking).

Koninklijke Marechaussee

Bij het optreden van een (cyber) incident/verstoring in een van de toegewezen taakgebieden voert de Marechaussee het onderzoek naar eventueel strafbare feiten onder gezag van het Openbaar Ministerie uit. Hiertoe beschikt de Marechaussee over cybermiddelen om in eigen onderzoek te kunnen voorzien dan wel werkt samen met de politie. In voorkomend geval kan de Marechaussee (op aanvraag via DJZ) bijstand verzoeken aan Defensie.

Militaire Inlichtingen- en Veiligheidsdienst

De MIVD verricht onderzoek naar actoren die een potentiële bedreiging vormen voor de nationale veiligheid, in het bijzonder gericht op Defensie belangen. Hierdoor kan de MIVD aanvallen van deze actoren detecteren en mitigeren, (potentiële) slachtoffers informeren en bewustwordingspresentaties geven aan mogelijke doelwitten. Een bijzondere relatie heeft de MIVD in dit kader met de Defensie Industrie. Daarnaast kan de MIVD door zijn inlichtingenpositie bijdragen aan attributie van digitale aanvallen.

Daarbovenop voert de MIVD in opdracht van de BA de Algemene Beveiligingseisen voor Defensie Opdrachten (ABDO) uit door hierover te adviseren en toe te zien op de handhaving en toezicht van dit kader.

Ministerie van Economische Zaken en Klimaat

Het Ministerie van Economische Zaken en Klimaat (EZK) heeft als stelselverantwoordelijke voor de telecomsector een verantwoordelijkheid voor de instandhouding van de nationale ICT-infrastructuur. Tijdens een incident in het digitale domein is het primair aan de partijen in de sector zelf om maatregelen te treffen die de crisis helpen oplossen; de staatssecretaris draagt géén operationele verantwoordelijkheid. Alleen onder buitengewone omstandigheden kan de minister/staatssecretaris op grond van artikel 14 van de Telecomwet aanwijzingen geven aan de aanbieders van elektronische communicatiediensten en –netwerken.

De Telecommunicatiewet geeft de mogelijkheid aanbieders van openbare telecommunicatiediensten en/of -infrastructuur aan te wijzen die voorbereidingen moeten treffen om de telecommunicatie in stand te houden tijdens buitengewone omstandigheden. Eén van de voorbereidingen is het deelnemen aan het door de overheid ingesteld overleg, het Nationaal Continuïteitsoverleg Telecom (NCO-T). Het doel van het NCO-T is dat de overheid samen met de aanbieders:

- preventieve maatregelen opstelt om ernstige verstoring of uitval van openbare communicatienetwerken en -diensten te voorkomen;
- maatregelen te treffen om een eventuele verstoring of uitval zo snel mogelijk en met zo weinig mogelijk schade aan vitale belangen te verhelpen.

In het NCO-T worden afspraken gemaakt over de verplichtingen die voor deze aanbieders volgen uit de Telecommunicatiewet, met name uit artikel 14.6. Dit zijn verplichtingen op het gebied van

continuïteitsplanning en crisismanagement. Daarbij wordt zo veel als mogelijk en wenselijk aangesloten bij de maatregelen die de bedrijven zelf vanuit de strategie met betrekking tot hun bedrijfscontinuïteit reeds getroffen hebben.

De minister van EZK is in Nederland ook beleidsverantwoordelijk voor het onderdeel vertrouwensdiensten van de eIDAS-verordening. Vertrouwensdiensten zijn diensten waarmee de integere uitwisseling van gegevens via internet kan worden geborgd. Voorbeelden zijn elektronische handtekeningen, -zegels, -tijdstempels, diensten voor aangetekende elektronische bezorging en certificaten voor de authenticatie van websites.

Door gebruik van vertrouwensdiensten weet de ontvanger van informatie wie deze aanbiedt of verzonden heeft en wanneer dit is gebeurd. Vertrouwensdiensten worden aangeboden door commerciële partijen maar ook gebruikt binnen de overheid zelf. Zij behoren tot de vitale infrastructuur Telecom.

Bij een crisis met vertrouwensdiensten kunnen burgers, bedrijven en de overheid niet meer vertrouwen op integere informatie-uitwisseling. Dit verlies van vertrouwen kan leiden tot stagnatie van elektronische communicatie en daarmee tot aanzienlijke maatschappelijke en economische schade.

Agentschap Telecom

Het Agentschap Telecom houdt zich bezig met het verruimen, verdelen en optimaliseren van het elektronische communicatiedomein. Het accent ligt daarbij op het frequentiespectrum, maar verder ziet het Agentschap, naast de Autoriteit Consument en Markt, ook op de naleving van vele bepalingen in de Telecommunicatiewet, zoals de verplichtingen die rusten op aanbieders van openbare telefoniediensten om continue toegang te bieden tot het alarmnummer 112. Ook is het Agentschap de organisatie waar de storingsmelding in het kader van de Telecomwet dient plaats te vinden.

Taken van het Agentschap Telecom tijdens crises omvatten onder meer:

- proactief toezicht houden en adviseren op locatie. Dit is ten behoeve van de continuïteit van de netwerken en diensten en ter ondersteuning van de crisisbeheersing;
- het beoordelen van de directe en lange termijn effecten;
- het beoordelen van andere processen in relatie tot het Elektronisch Communicatie Domein, zoals bijvoorbeeld:
  - het adviseren ten behoeve van de continuïteit van de netwerken;
  - het beëindigen van (bijvoorbeeld illegale) radioverbindingen;
  - het in beslag nemen en/ of uitschakelen van (zend)apparatuur;
  - vorderen van apparatuur en informatie;
  - toepassen van bestuursdwang;
  - voorbereiden maatregelen toewijzen frequenties tijdens bijzondere omstandigheden.

Ministerie van Justitie en Veiligheid

De Minister van Justitie en Veiligheid is coördinerend minister voor crisisbeheersing en voor cybersecurity. De NCTV is stelselverantwoordelijk voor de nationale crisisbeheersing en voert het beheer van de hierboven genoemde nationale crisisgremia. De NCTV is daarnaast opdrachtgever van het NCSC dat als uitvoeringsorganisatie onder de verantwoordelijkheid van de minister van Justitie en Veiligheid valt. Verder is de minister verantwoordelijk voor de vitale communicatiediensten 112, C2000 en NL-Alert.

Openbaar Ministerie

Het OM is bij een (dreigend) incident in het digitale domein verantwoordelijk voor de strafrechtelijke handhaving van de rechtsorde. Dit betekent dat het OM:

- Het gezag voert over het opsporingsonderzoek naar de toedracht van de calamiteit of crisis, het veiligstellen van (digitaal) bewijs of betrokken is bij het uitwisselen van relevante informatie (bijvoorbeeld van/naar private partijen, of de inlichtingen- en veiligheidsdiensten);
- Zich inzet om het plegen van strafbare feiten te voorkomen of doen stoppen door middel van het strafrecht en/of door het laten treffen van maatregelen in het kader van bewaken en beveiligen (persoonsbeveiliging);
- De rechtsorde handhaaft door diverse interventiemethoden zoals preventie, notificatie, verstoring, attributie/opsporing, laten aanhouden en vervolgen van burgers of rechtspersonen die zich schuldig maken aan het overtreden van wet- en regelgeving.

Politie

De politie is verantwoordelijk voor handhaving van de rechtsorde (dit omvat tevens de opsporing) en hulp aan hen die dat behoeven. Indien noodzakelijk kan de politie haar (crisis) organisatie opschalen bij incidenten met grote impact volgens het (N) SGBO-model: (Nationale) Staf Grootschalig Bijzonder Optreden. De taken worden verdeeld over diverse hoofdprocessen, te weten handhaving mobiliteit, ordehandhaving, opsporing (en expertise op dat terrein), interventie, handhaven netwerken, bewaking en beveiliging. Op het niveau van de veiligheidsregio fungeert een SGBO als actiecentrum van de politie en richt zij zich op crisisbeheersing, gevolgbestrijding en het wegnemen van de bron van het incident. Voor het uitvoeren van de landelijke taken van de Landelijke Eenheid, waaronder de landelijk informatievoorziening en -inschatting, het contact en de coördinatie met partners als NCSC en Europol kan een SGBO Landelijke Eenheid gestart worden. Tevens is het mogelijk om een nationaal SGBO (NSGBO) op te starten, met als taak richting te geven of te sturen op de politieoperaties. Deze wordt via de reguliere bestuurlijke lijnen aangehaakt aan de nationale en regionale crisisstructuur. Het niveau van opschaling hangt af van de impact van de ontwrichting op de samenleving, zowel qua ernst als regionale spreiding.

Het gezag over politie-inzet is in beginsel territoriaal georiënteerd (burgemeester, bij crisis opschalend via GRIP model). Voor de opsporing met betrekking tot een strafbaar feit vallen de politie en ook de Koninklijke Marechaussée onder het bevoegd gezag van het Openbaar Ministerie (OM). Bijzondere opsporingsbevoegdheden kunnen ingezet worden om eventuele verdachten van (tot crisis leidende) cybercrime te traceren, strafbare feiten te stoppen en te voorkomen (waar mogelijk) en criminele infrastructuren te ontmantelen. Dit kan leiden tot het verhinderen/verstoren van de criminele activiteiten en/of het aanhouden van verdachten in binnen- of buitenland. Op die manier kan de dreiging en verstoring mogelijk worden weggenomen en controle over de situatie verkregen worden. Aanvankelijk zal onzekerheid bestaan over het type dader (crimineel of statelijke actor). Afhankelijk van o.a. mogelijkheden en context wordt de meest passende aanpak (één of meer interventiemethoden) gekozen: preventie, notificatie, verstoring en opsporing (en vervolging). Indien sprake is van neveneffecten en gevolgen in het fysieke domein (zoals maatschappelijke onrust, rellen en plunderingen) heeft de politie ook daar een (handhavende) taak. Naast de cybercrimeteams in de eenheden en het Team High Tech Crime (THTC) wordt ook een beroep gedaan op andere teams (zoals de basisteams, het real-time intelligence team en de ME).

Op het internationale vlak kan de politie schakelen via INTERPOL, Europol en diverse 24/7 netwerken. Sommige van deze kanalen kunnen vervallen indien de crisis (met zekerheid) militair van karakter is of door een statelijke actor wordt veroorzaakt. Er kan dan in beginsel niet opgespoord worden via bijvoorbeeld INTERPOL. Ook is de politie vertegenwoordigd in bijna alle Information Sharing and Analysis Centres (ISAC's).

Ministerie van Financiën

Tripartiet crisismanagement operationeel (TCO)

Indien er informatie is over (dreigende) operationele verstoringen in het betalings- en effectenverkeer bij de Financiële Kerninfrastructuur, bijvoorbeeld als gevolg van een cyberaanval, wordt het TCO operationeel. Het TCO dient als besluitvormend orgaan en heeft als taken:

- maatregelen te nemen in geval van een dreigende, instelling-overschrijdende verstoring van het betalings- en effectenverkeer;
- te communiceren met stakeholders.

Deelnemers aan het TCO zijn het Ministerie van Financiën, de Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB). Deze partijen hebben alle drie een rol ten aanzien van het functioneren van het betalings- en effectverkeer. De Minister van Financiën is in dit kader politiek verantwoordelijk voor het financiële stelsel. De AFM is gedragstoezichthouder en houdt toezicht op het effectenverkeer. DNB is prudentieel toezichthouder en centrale bank, en bevordert onder meer de goede werking van het betalingsverkeer. DNB is de voorzitter van het TCO.

Ministerie van Infrastructuur en Waterstaat

In 2019 heeft IenW een actuele Cyberstrategie vastgesteld. Deze strategie schetst de ambities van IenW (bestuurskern, agentschappen en ZBO's) op het gebied van cybersecurity en geeft richting aan de aanpak van IenW. IenW is beleidsverantwoordelijk voor een groot aantal sectoren waarvan er op dit moment zeven zijn geclassificeerd als nationaal-vitaal (waaronder drinkwater en mainports). De strategie is gericht op het inzichtelijk krijgen en beheersen van cyberrisico's bij de ICT van IenW zelf en bij de ICT van de IenW sectoren (vitaal en niet-vitaal), én op de organisatie en governance van cybersecurity bij IenW.

Bij de uitvoeringsorganisatie RWS is voor de drie netwerken hoofdwatersysteem, hoofdwegen én hoofdvaarwegen een Security Centre operationeel. Het Security Centre heeft een breed takenpakket: van adviezen aan projecten om de juiste beveiligingseisen te implementeren, tot het inrichten van de besturing van informatiebeveiliging bij RWS. Dit gebeurt zowel voor de Industriële Automatisering als voor de kantooromgeving. Ook organiseert het Security Centre toezicht op de implementatie van beveiligingseisen, wordt dagelijks het netwerkverkeer gemonitord en wordt geacteerd wanneer belangrijke afwijkingen worden gesignaleerd.

Het Security Centre werkt dagelijks samen met andere overheidsorganisaties, zoals het Nationaal Cybersecurity Centrum (NCSC), Joint- SOC (J-SOC, samenwerking van de Belastingdienst, SSC-ICT en SOC RWS), de AIVD en waterschappen.

Voor de Wbni heeft de minister van IenW de Inspectie Leefomgeving en Transport als toezichthouder aangewezen op de naleving van de wet bij de Aanbieders van Essentiële Diensten. Het piketnummer van het Departementaal Coördinatiecentrum Crisisbeheersing IenW (DCC-IenW) doet dienst als 24/7 Wbni-meldpunt voor de ILT.

Voor IenW betreft het de volgende AED's:

- Voor vervoer over water: de Divisie Havenmeester van het Havenbedrijf Rotterdam N.V.
- Voor vervoer door de lucht: Royal Schiphol Group N.V., Luchtverkeersleiding Nederland, Maastricht Upper Area Control Centre (MUAC), Aircraft Fuel Supply B.V., Koninklijke Marechaussee en elke luchtvaartmaatschappij met minimaal 25% van het totaal aantal vliegbewegingen op Schiphol in een kalenderjaar. Nu is dat Air France-KLM.
- Voor drinkwater: de drinkwaterbedrijven.

Veiligheidsregio's

Wanneer een incident in het digitale domein gevolgen heeft voor de openbare orde en veiligheid hebben de veiligheidsregio als taak te zorgen voor continuïteit van de samenleving en inwoners een goede hulpverlening te bieden. Daarbij gaat het om bevolkingszorg, brandweerzorg, geneeskundige zorg, leiding en coördinatie, informatiemanagement en crisisbeheersing in de zin van de Wet veiligheidsregio's (Wvr).

Conform het Besluit Veiligheidsregio's en de daarop gebaseerde Basisvereisten Crisismanagement moet de crisisorganisatie van de veiligheidsregio 72 uur continu zelfstandig kunnen functioneren.

Veiligheidsregio's maken samen met hun partners een globale inventarisatie van de mogelijke (fysieke) cascade-effecten van een digitaal incident in hun regio. Inzicht in het incident en de mogelijke risico's en cascade-effecten is essentieel voor de realisatie van de gehele veiligheidsketen: risicobeheersing, incident- en rampenbestrijding en crisisbeheersing, risico- en crisiscommunicatie richting burgers en deelnemende organisaties, en normalisering van de samenleving na een incident.

Door de kenmerken van digitale verstoringen zijn deze complex en moeilijk vooraf in kaart te brengen, daarom investeren veiligheidsregio's samen met hun partners in universele instrumenten zoals een goede informatiepositie, duiding, bewustwording en scenario-denken bij digitale verstoringen. Daarnaast bevorderen veiligheidsregio's dat risicovolle objecten en partners in haar regio zelf zorg dragen voor een goede digitale weerbaarheid en herstelvermogen.

Het NCC is voor de veiligheidsregio's nationaal contactpunt voor het rijk.

De focus van de veiligheidsregio ligt bij de gevolgbestrijding van maatschappelijke ontwrichting en op het beschermen en voorlichten van burgers en deelnemende organisaties en instellingen. Coördinatie is nodig om tot een gedeeld situatiebeeld en prioritering te komen.

D. Internationale partners en samenwerkingsverbanden

Bij internationale partners en samenwerkingsverbanden wordt een onderscheid gemaakt tussen operationele samenwerking en tactisch-strategische samenwerking.

Operationele samenwerking

Europese Unie

In de Europese Netwerk en informatiebeveiligingsrichtlijn (NIB) uit 2016, die voor zover het Nederland betreft is geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen, is de instelling van een Europees netwerk van nationale CSIRTs en CERT-EU (het CSIRT-netwerk) vastgelegd. Binnen dit CSIRT-netwerk kunnen de CSIRTs snel en effectief operationele informatie met elkaar uitwisselen. Het CSIRT-netwerk wordt actief ondersteund door het European Network and Information Security Agency (ENISA).

ENISA richt zich op de Europese Commissie en de lidstaten rond het onderwerp netwerk- en informatiebeveiliging, en ondersteunt deze partijen daarin. Doelstelling van ENISA is het vergroten van de veiligheid en weerbaarheid van communicatie- en informatiesystemen. ENISA organiseert een tweejaarlijkse oefencyclus onder de naam Cyber Europe. In deze oefening wordt de opzet van een zogeheten Standard Operating Procedure (SOP) getest. Dit is een hulpmiddel voor de CERT's in Europa om op een veilige en effectieve wijze informatie uit te wisselen bij een internationale crisis in het digitale domein.

Voor de Europese instellingen fungeert CERT-EU als responsorganisatie voor incidenten in het digitale domein. Met de invoering van de zogeheten NIB-richtlijn in Europa in de komende jaren zal de verdere uitbouw van de samenwerking van de lidstaten vooral gestalte krijgen via het netwerk van *Cyber Security and Incident Response Teams*.

Op Europees niveau is een blauwdruk[13] gepubliceerd die lidstaten helpt bij het omgaan met digitale incidenten. Deze blauwdruk is van toepassing bij incidenten die dusdanige ontwrichting veroorzaken dat lidstaten deze zelf niet kunnen afhandelen of als het incident gevolgen heeft voor meerdere lidstaten of EU instellingen. Daarbij kan sprake zijn van dusdanig grootschalige of significante impact, of technische of politieke relevantie, dat tijdige coördinatie en respons op Europees politiek niveau nodig is.

13 Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises, 13 September 2017 (L239/36).

Ook Europol (EC3) krijgt via het responsprotocol meer een operationele taak bij grootschalige, grensoverschrijdende incidenten en crises. Hierin richten zij zich op hun opsporingstaak en werken zij op het gebied van informatiedeling met name samen met politiediensten en ENISA.

Wanneer de aanpak van een grensoverschrijdende crisis een strafrechtelijke component heeft, is ook voorzien in een rol voor Eurojust (het agentschap voor samenwerking tussen justitiële autoriteiten). Het betrekken van Eurojust geschiedt op initiatief van Europol (EC3). Voor specifieke cyber-expertise binnen het justitiële domein kan Eurojust een beroep doen op het Europees Justitieel Cybercrime Netwerk (EJCN).

International Watch and Warning Network

Het International Watch and Warning Network (IWWN) is een (informeel) wereldwijd netwerk van overheidsvertegenwoordigers uit vijftien landen (waaronder Nederland) rond operationele samenwerking en crisisbeheersing op het gebied van cybersecurity. Het IWWN onderhoudt de banden tussen de functionele 'points-of-contact' met een nationale verantwoordelijkheid, heeft voor grote dreigingen en crises Standard Operational Procedures (SOP) ontwikkeld, organiseert oefeningen, bevordert samenwerking en stimuleert informatiedeling.

European Government CERTs group

De European Government CERT group (EGC) is een hoog vertrouwd, informeel verband van overheids-CERT's in Europa. De deelnemers werken samen op basis van wederzijds vertrouwen en begrip. Gezamenlijk wordt gewerkt aan maatregelen, informatiedeling in relatie tot incidenten, kennisontwikkeling en gezamenlijke standpunten. EGC is een operationele groep met een technische focus, gericht op incidentrespons en informatiedeling.

Tactisch-strategische samenwerking

Like-minded

Like-minded en Europese lidstaten coördineren in toenemende mate de publieke reactie op cyberoperaties. Dit kan het Nederlandse belang dienen. Dit moet dan zorgvuldig worden ingebed in de bredere buitenlandpolitieke agenda en de drijfveren van de staat waartegen wordt opgetreden en de like-minded waarmee wordt opgetrokken. Nederland heeft belang bij een brede coalitie. Daartoe dient ruimte te bestaan voor flexibiliteit c.q. verschillende vormen van deelname.

Europese Unie

Kwaadwillige cyberactiviteiten kunnen aanleiding geven tot een gezamenlijke EU-respons. Om tot een effectieve EU-respons te komen kan ten volle gebruik worden gemaakt van maatregelen in het kader van het Gemeenschappelijk Buitenlands- en Veiligheidsbeleid, waaronder beperkende maatregelen (sancties).

Internationale Europese samenwerking vindt ook plaats onder Permanent Structured Cooperation (PESCO). Zo is er voor cyber een project dat ziet op snelle reactieteams. Dit door Litouwen geleide project beoogt de responscapaciteit van deelnemende lidstaten te bundelen en in te zetten ter ondersteuning van EU-lidstaten ten tijde van cyber crises. Nederland is deelnemer aan dit project. Op deze manier draagt het project bij aan betere samenwerking op het gebied van cybersecurity tussen de lidstaten en daarmee aan een digitaal veiliger Europa.

Organisatie voor Veiligheid en Samenwerking in Europa (OVSE)

In OVSE-verband zijn zestien vertrouwenwekkende maatregelen overeen gekomen met als doel om de risico's van conflict te verminderen die kunnen ontstaan door het gebruik van ICT. De maatregelen variëren van het vrijwillig uitwisselen van informatie tot het aangaan van formele consultaties met andere deelnemende staten.

Noord-Atlantische Verdragsorganisatie

Het NAVO-bondgenootschap moet in staat zijn om zich te weren tegen het volledige brede spectrum aan vijandige cyberoperaties. Dit betreft niet alleen cyberoperaties die beschouwd kunnen worden als een gewapende aanval, maar ook operaties die onderdeel zijn van een hybride campagne in het lagere gedeelte van het geweldsspectrum. Het bondgenootschap werkt aan een breed keuzemenu bestaande uit diplomatieke en politieke responsopties van verschillende intensiteit. Hier dient ook een zekere afschrikwekkende werking vanuit te gaan.

Bijlage 4

Relevante bronnen en literatuur

Agenda Risico- en Crisisbeheersing 2018-2021, TK-brief 12 november 2018.
AIV en CAVV, Digitale oorlogvoering (advies) en kabinetsreactie, 2012.
Algemene Rekenkamer, Digitale dijkverzwaring: cyber security en vitale waterwerken, 2019 en reactie minister Infrastructuur en Waterstaat, 25 februari 2019.
Cyber Security Beeld Nederland, 2019.
Cyberstorm III, Evaluatie interdepartementale ICT-crisisoefening, 17 februari 2011.
Defensie Cyber Strategie 2018
M. van Eeten, Blussen met nullen en enen (Van Slingerlandtlezing 31 oktober 2019).
Geïntegreerde risicoanalyse in het kader van de Nationale Veiligheid Strategie 2019.
Handboek ICT Response Board.
Inspectie JenV, Evaluatie rijkscrisisorganisatie tijdens de DigiNotar-crisis, juli 2012.
Instellingsbesluit NCO-T, 2007.
Instellingsbesluit Ministeriële Commissie Crisisbeheersing 2016.
IFV, Bestuurlijke Netwerkkaarten Crisisbeheersing en bijbehorende bevoegdhedenschema's, 2019.
IFV, Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoring), april 2019.
IFV, Crisiscommunicatietips voor uitval van vitale voorzieningen, december 2018.
IFV, Verbinden van werelden? Een analyse van de aanpak van zeven bovenregionale crisistypen, Arnhem 2019.
Landelijk convenant voor samenwerkingsafspraken tussen Veiligheidsregio's, Politie en Telecom.
H. Modderkolk, Het is oorlog, maar niemand die het ziet, 2019.
Nationaal Handboek Crisisbesluitvorming 2016.
Nationale Risicobeoordeling, Bevindingenrapportage 2010, 30 november 2010.
Nationaal Veiligheidsprofiel 2016.
Nederlandse Cyber Security Agenda (NCSA) 2018.
Cyber Security Beeld Nederland, 2019.
Nationale Veiligheid Strategie 2019.
Recommentation EU on coordinated response to largescale cyber security incidents and crises, 13 September 2017 (L239/36).
Resultaten self-assessment intersectorale afhankelijkheden eindrapportage, 6 maart 2019.
Veiligheidsberaad, Bestuurlijk routeboek digitale ontwrichting, september 2019.
WRR, Voorbereiden op digitale ontwrichting, 2019.

Bijlage 5

Afkortingen

AED	Aanbieder van Essentiële Diensten
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
DDoS	Distributed Denial of Service
DOCB	Directeurenoverleg Crisisbeheersing
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
MCCb	Ministeriële Commissie Crisisbeheersing
NAVO	Noord-Atlantische Verdragsorganisatie
NCC	Nationaal Crisiscentrum
NCO-T	Nationaal Continuïteitsoverleg Telecommunicatie
NCSA	Nederlandse Cybersecurity Agenda
NCSC	Nationaal Cyber Security Centrum
NCSS	Nationale Cyber Security Strategie
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NCV	Noodcommunicatievoorziening
NHC	Nationaal Handboek Crisisbesluitvorming
NKC	Nationaal Kernteam Communicatie
NRN	Nationaal Respons Netwerk
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
TCO	Tripartiet Crisismanagement Operationeel
THTC	Team High Tech Crime van de Politie
VNG	Vereniging Nederlandse Gemeenten
VR	Veiligheidsregio

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minjenv.nl
@nctv_nl

Februari 2020