Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Landelijk Crisisplan Digitaal

Omslagbeeld: IJtunnel Amsterdam

Vitale en niet-vitale processen zijn in hoge mate afhankelijk van netwerk- en informatiesystemen. Uitval en verstoring hiervan heeft vaak direct impact op onze samenleving. De controle- of meldkamer spelen een sleutelrol in zowel de voorbereiding als de reactie op incidenten en (potentiële) crises.

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

Het belang van digitale systemen voor onze samenleving is niet te overschatten. Of het nu gaat om wonen, werken, reizen, betalen, elkaar ontmoeten: we leven op een digitale infrastructuur. Een infrastructuur die een zee aan mogelijkheden biedt, maar die ook risico's met zich meebrengt. Want een crisis in het digitale domein beperkt zich niet tot de wereld van bits en bytes; die crisis is al heel snel merkbaar en voelbaar in de echte wereld waar binnen korte tijd ons maatschappelijk leven wordt verstoord.

Digitale dreigingen zijn inmiddels een permanente uitdaging voor de nationale veiligheid. Zoals blijkt uit het Cybersecuritybeeld Nederland 2022 is er sprake van scheefgroei tussen de toenemende dreiging en de ontwikkeling van onze weerbaarheid. Die scheefgroei vergroot het risico op ontwrichting. En ook als de kloof tussen weerbaarheid en dreiging wordt verkleind, is duidelijk dat honderd procent veiligheid niet bestaat. Digitale processen kunnen altijd uitvallen door technisch of menselijk falen. Om nog maar te zwijgen over de toenemende activiteiten van statelijke actoren en criminele organisaties in het digitale domein.

We zien in praktijk dat cyberaanvallen en –incidenten elkaar opvolgen en de gevolgen ingrijpender worden. Denk aan de Citrix-problematiek waarbij onder andere het Medisch Centrum Leeuwarden en de Rijksoverheid werden gedwongen verregaande maatregelen te nemen. Of de aanval op Veiligheidsregio Noord- en Oost-Gelderland waar cybercriminelen door middel van ransomware belangrijke systemen konden hacken en platleggen. En de kwetsbaarheden in Apache Log4J brachten de gevaren van ketenafhankelijkheid aan de oppervlakte. Dit zijn slechts enkele voorbeelden van digitale incidenten die doorwerkten in het fysieke domein. De gevolgen - hoe vervelend ook voor de betrokkenen – bleven relatief beperkt. Maar wat gebeurt er als de gevolgen de maatschappij ontwrichten en leiden tot grote maatschappelijke onrust? Dan is voor een adequate respons een sterke crisisaanpak meer dan noodzakelijk.

De Nederlandse Cybersecuritystrategie 2022-2028 benadrukt het belang van snel en adequaat reageren op cyberincidenten en –crises. Efficiënte samenwerking tussen overheidsorganisaties, het bedrijfsleven, de wetenschap en maatschappelijke organisaties is daarbij essentieel – ook over lokale, regionale en nationale grenzen heen. Dit Landelijk Crisisplan Digitaal biedt hiervoor de kaders. Om de landelijke crisisaanpak te vertalen naar operationeel uitgewerkte plannen voor specifieke organisaties in onze samenleving bevat dit plan veel informatie over de crisisbeheersing in het digitale domein en de koppeling met de fysieke gevolgbestrijding, op nationaal en regionaal niveau.

Effectieve crisisbeheersing vergt behalve gezamenlijke voorbereiding ook oefening. De flexibiliteit van de bouwstenenmethodiek in dit plan biedt u de kans om passende scenario's te creëren en hier met uw organisatie mee aan de slag te gaan. Het Landelijk Crisisplan Digitaal is daarmee uitstekend als basis te gebruiken voor de inrichting van de eigen planvorming en oefeningen. We nodigen u van harte uit dat ook te doen en zo bij te dragen aan een digitaal veilig Nederland.

Wij zijn trots dat dit Landelijk Crisisplan Digitaal is gerealiseerd in nauwe samenwerking van de Rijksoverheid en de veiligheidsregio's met private partners. Want het bewaken van onze nationale veiligheid in een snel veranderend digitaal landschap is een gedeelde en gezamenlijke verantwoordelijkheid.

Pieter-Jaap Aalbersberg
Nationaal Coördinator Terrorismebestrijding en Veiligheid

Gerhard van den Top
Burgemeester Hilversum, Portefeuillehouder Informatievoorziening in het Veiligheidsberaad

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Veiligheids
beraad

Het sluizencomplex bij Lelystad speelt een belangrijke rol in de waterverdeling vanuit het IJsselmeer.

1. Inleiding

De huidige samenleving is grotendeels afhankelijk geworden van digitale middelen. Het Cybersecuritybeeld Nederland (CSBN) biedt jaarlijks inzicht in de digitale dreigingen, de mogelijke aantasting van belangen, de weerbaarheid en tot slot risico's van de cybersecurity in Nederland. De toenemende dreiging zoals geschetst in meerdere edities van het CSBN toont het belang aan van een goede voorbereiding op een situatie waarbij sprake is van maatschappelijke ontwrichting veroorzaakt in het digitale domein.

De afhankelijkheid van gedigitaliseerde processen en systemen is zo groot dat aantasting hiervan kan leiden tot maatschappij-ontwrichtende schade. Vitale en niet-vitale processen zijn in hoge mate afhankelijk van netwerk- en informatiesystemen. Uitval en verstoring hiervan, of van belangrijke digitale processen in de samenwerkende keten(s), heeft zeer snel, binnen enkele uren, impact op een aantal vitale processen.

Doel

Het Landelijk Crisisplan Digitaal (LCP-Digitaal) is een leidraad om op hoofdlijnen inzicht en overzicht te creëren in de bestaande afspraken en wetgeving op landelijk niveau over de beheersing van incidenten en (potentiële) crises in de beveiliging van netwerk- en informatiesystemen met aanzienlijke maatschappelijke gevolgen.[1] Het plan beschrijft de gezamenlijke aanpak bij een digitale crisis op landelijk niveau, de samenwerking en aansluiting met betrokken publieke en private crisispartners en de samenwerking met netwerken op internationaal niveau. Het plan is daarmee een cyber-specifieke uitwerking van de generieke aanpak van crises door het Rijk zoals beschreven in het Instellingsbesluit Ministeriële Commissie Crisisbeheersing en het Nationaal Handboek Crisisbeheersing.

Het LCP-Digitaal kent zijn grootste meerwaarde in de voorbereiding op een crisis en is het overkoepelend en kaderstellend plan voor de individuele operationele plannen en draaiboeken van de betrokken actoren en organisaties. Het LCP-Digitaal vervangt deze plannen niet. De operationele plannen en draaiboeken van betrokken actoren en organisaties moeten waar relevant wel in overeenstemming worden gebracht met het LCP-Digitaal.

De informatie in dit plan geeft antwoord op de volgende vragen:

- Welke organisaties zijn en kunnen betrokken zijn bij een (dreigend) grootschalige cybercrisis en wat is ieders verantwoordelijkheid?
- Hoe verloopt de informatievoorziening in een cybercrisis en hoe worden de functionele en algemene crisisbeheersing aan elkaar verbonden?
- Wat zijn de belangrijkste onderscheidende elementen c.q. bouwstenen in de beheersing van een cybercrisis?
- Welke specifieke dilemma's en sleutelbesluiten zijn relevant voor bestuurders tijdens een (dreigend) grootschalige cybercrisis?

1. Incidenten kunnen, zodra deze aanzienlijke gevolgen hebben, een crisis worden of zijn. Volgens de Wet- beveiliging netwerk- en informatiesystemen (Wbni) is een incident elke gebeurtenis met een daadwerkelijk schadelijk effect op de beveiliging van netwerk- en informatiesystemen.

Doelgroepen

Doelgroepen van dit plan zijn de actoren en organisaties binnen of direct verbonden aan de opgeschaalde nationale en decentrale crisisstructuur die een rol hebben bij de beheersing van (potentiele) crises in netwerk- en informatiesystemen. Dit betreft onder andere medewerkers, CISO's, leidinggevenden en bestuurders van alle actoren en organisaties die binnen de opgeschaalde nationale en decentrale crisisorganisatie een rol kunnen hebben. Dit zijn onder andere de betrokken ministeries en organisaties actief in het digitale domein zoals het Nationaal Cyber Security Centrum (NCSC), het CIO-stelsel, de inlichtingen- en veiligheidsdiensten, de Politie en het Openbaar Ministerie (OM). Het plan is ook bestemd voor decentrale overheden zoals de veiligheidsregio's, waterschappen en een gemeentelijke CISO-organisatie. Daarnaast is het bedoeld voor instellingen in bijvoorbeeld de zorg en het onderwijs en private partners om hun eigen voorbereiding en planvorming daarop af te stemmen.

Vaststellings- en implementatieprocedure

- Naast een openbare versie kent het LCP-Digitaal ook een versie met de classificatie TLP:Amber (Oranje). Dit betekent dat deze publicatie bestemd is voor betrokken organisaties en dat de informatie binnen de organisatie uitsluitend mag worden verspreid op een need-to-know basis.
- Het Rijksbrede Directeurenoverleg Crisisbeheersing (DOCB), waarin ook de veiligheidsregio's en de aanbieders van vitale processen zijn vertegenwoordigd, is ambtelijk opdrachtgever van het LCP-Digitaal.
- Het LCP-Digitaal is opgesteld door een schrijfgroep met vertegenwoordigers van de NCTV, het NCSC, het NCC en de veiligheidsregio's in nauwe afstemming met de ministeries van BZ, BZK, DEF, EZK, FIN en IenW, politie, AIVD en OM. Het LCP-Digitaal is ter advisering voorgelegd aan de Commissie Vitale Infrastructuur en het Publiek-Privaat Directeurenoverleg Cyber Security.
- Het LCP-Digitaal is op regionaal niveau afgestemd met de Raad van Commandanten en Directeuren Veiligheidsregio (RCDV) en met de leden van het Veiligheidsberaad
- Het LCP-Digitaal is op Rijksniveau afgestemd door het Directeurenoverleg Crisisbeheersing (DOCB), het Directeurenoverleg Cybersecurity en daaraanvolgend vastgesteld in de Ministeriële Commissie Economie en Veiligheid en de ministerraad.

Beheercyclus

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de veiligheidsregio's verenigd in het Veiligheidsberaad zijn eigenaar van en verantwoordelijk voor beheer en actualisatie van het LCP-Digitaal. De NCTV beziet jaarlijks in overleg met de betrokken ministeries, veiligheidsregio's en andere betrokken actoren en organisaties of actualisering van het LCP-Digitaal of onderdelen daarvan nodig is.

De eerstvolgende (uitgebreide) actualisatie van dit plan zal naar verwachting volgen op de implementatie van stelselwijzigingen die aangekondigd zijn in de Nederlandse Cybersecurity Strategie (NLCS) en het daarbij behorende actieplan. In Hoofdstuk 2, Samenvattend Beeld, is een doorkijk opgenomen naar de ontwikkeling van het cybersecuritystelsel volgens de NLCS.

Gebruik

- Het LCP-Digitaal wordt gebruikt voor crisisvoorbereiding.
- Het LCP-Digitaal wordt gebruikt als basis voor cybercrisisoefeningen op regionaal en nationaal niveau, zoals ISIDOOR.
- Het LCP-Digitaal wordt gebruikt als informatiebron tijdens cybercrises.

De evaluaties die worden opgesteld naar aanleiding van (nationale) oefeningen en crises worden gebruikt als input voor volgende actualiseringen van het LCP-Digitaal.

2. Samenvattend beeld

Afbakening

Het domein waarop dit crisisplan van toepassing is, wordt in de Nationale Veiligheid Strategie uit 2019 (NVS) de digitale ruimte genoemd. Dit is het conglomeraat van digitale middelen en –diensten en bevat permanente, tijdelijke en plaatselijke (digitale) verbindingen en gegevens, waarbij geen geografische beperkingen zijn gesteld. Alle entiteiten in de samenleving kunnen in de digitale ruimte verbonden zijn.[2]

Binnen de digitale ruimte richt het LCP Digitaal zich op de beheersing van crises met betrekking tot de beveiliging van netwerken en informatiesystemen met aanzienlijke maatschappelijke gevolgen en daaraan gerelateerde cascade- en gevolgeffecten. Het plan ziet toe op crises waarbij de (veronderstelde) oorzaak zich eveneens in de digitale ruimte bevindt.

Er zijn verscheidene incidenttypen denkbaar die kunnen leiden tot een opschaling van de crisisstructuur zoals beschreven in dit plan. Het kan daarbij gaan om zowel hele merkbare situaties waarbij sprake is van uitval van netwerken en informatiesystemen met aanzienlijke maatschappelijke gevolgen, als om situaties die in de buitenwereld niet zichtbaar zijn maar van waaruit een grote (digitale) dreiging uitgaat.

Het CSBN 2022 onderkent vier risico's voor de nationale veiligheid die relevant kunnen zijn voor een dergelijke opschaling:

- Ongeautoriseerde inzage in informatie (en eventueel publicatie daarvan), in het bijzonder door spionage. Denk aan spionage van communicatie binnen de Rijksoverheid of de ontwikkeling van innovatieve technologieën.
- Ontoegankelijkheid van processen, als gevolg van (voorbereiding voor) sabotage en de inzet van ransomware. Denk aan de innesteling in processen die zorgdragen voor de distributie van elektriciteit.
- Schending van de (veiligheid van de) digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leverancierskketens.
- Grootschalige uitval: een situatie waarin één of meer processen zijn verstoord als gevolg van technische oorzaken of als gevolg van niet-moedwillig menselijk handelen.[3]

Wanneer een of meer van voorgaande risico's zich op grote schaal of in maatschappelijk belangrijke (digitale) processen en systemen 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.[4] In dat geval is er sprake van maatschappelijke ontwrichting.

2. Nationale Veiligheid Strategie 2019.
3. Het CSBN 2022 schrijft ook over natuurlijke oorzaken. Dit type oorzaak hoeft niet te leiden tot een activering van de crisisstructuur volgens het LCP Digitaal. Echter kunnen de organisaties die beschreven zijn in dit plan ook in dergelijk scenario een actieve of adviserende rol vervullen.
4. De nationale veiligheidsbelangen zoals beschreven in de NVS 2019 zijn de *territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, sociale en politieke stabiliteit*, en *internationale rechtsorde*.

Regionaal risicoprofiel

Naast de nationale risico's zijn ook regionaal gedefinieerde risico's relevant voor het LCP-Digitaal. Conform de Wet veiligheidsregio's (artikel 15) stelt het bestuur van een veiligheidsregio een regionaal risicoprofiel vast. Het regionaal risicoprofiel is een inventarisatie en analyse van de aanwezige risicovolle situaties en de soorten crises die zich daardoor kunnen voordoen, en wordt door veiligheidsregio's ten minste[5] eens per vier jaar vastgesteld. Mede op basis van deze risicoanalyse maakt het bestuur van de veiligheidsregio strategische beleidskeuzes over de ambities voor de risico- en crisisbeheersing. Deze ambities worden vastgelegd in het beleidsplan van de veiligheidsregio's.

Een gedeelte van de risicoprofielen van veiligheidsregio's richt zich op cyber-gerelateerde ontwikkelingen en risico's. Een toenemende mate van maatschappelijke afhankelijkheid en verwevenheid van digitale systemen en informatie wordt als een significant risico gezien. Hierin wordt zowel aangegeven dat een cybercrisis en/of digitale verstoring een risico is, maar dit wordt ook toegeschreven aan uitval en/of verstoring van ICT en telecommunicatie en/of spraak- en datacommunicatie. Tevens benadrukken vrijwel alle veiligheidsregio's het risico op zogenoemde cascade- en keteneffecten.

Kenmerken, risicoduiding en impact

Digitale crises verschillen in een aantal opzichten van andere typen crises:

- De snelheid waarmee dergelijke crises zich manifesteren. Een digitaal incident kan van het en 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 ketenafhankelijkheid kan een digitale crisis gevolgen hebben voor meerdere vitale processen tegelijkertijd. Dit kan snel leiden tot maatschappelijke ontwrichting zeker als de crisis langer aanhoudt.
- Door complexe ketenafhankelijkheden kan de bron van een digitale crisis soms lastig te achterhalen zijn, waardoor respons wordt bemoeilijkt. Organisaties werken samen in ketens waardoor problemen bij toeleveranciers of afnemers kunnen leiden tot maatschappelijke ontwrichting.
- Door het bespioneren van vertrouwelijke data en informatie, door deze te ontvreemden (data-extractie) of door deze te saboteren, kunnen de vitale belangen van Nederland en zijn bondgenoten worden aangetast.
- 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.
- Bij de bronbestrijding is de overheid mede afhankelijk van het handelen van private partijen, nauwe publiek-private samenwerking is van belang. Vrijwel alle digitale infrastructuur en digitale dienstverlening zijn in handen van private partijen.
- 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. Daarom wordt er door de betrokken opsporingsdiensten vanuit gegaan dat van opzet sprake is, totdat blijkt dat dat niet het geval is. Zowel statelijke als criminele actoren zijn actief in de digitale ruimte en kunnen verantwoordelijk zijn voor een crisis.
- Een crisis in de netwerk- en informatiesystemen treft zelden alleen het digitale domein. Veelal zullen er ook ongewenste effecten optreden in het fysieke domein.
- Netwerken en informatiesystemen zijn veelal grensoverschrijdend. Het is aannemelijk dat een crisis met betrekking tot netwerk- en informatiesystemen een internationaal karakter heeft, waarbij de oorzaak van de crisis in het buitenland kan liggen, in meerdere landen tegelijkertijd kan optreden, of waarbij de oorzaak mogelijk (mede) in Nederland ligt, maar het effect niet.
- Er bestaat 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 crisis in het digitale domein kan onderdeel zijn van hybride conflictvoering. Daarbij gaat het om een conflictvoering tussen staten, met geïntegreerd gebruik van middelen en actoren, met als doel bepaalde strategische doelstellingen te bereiken.

De gevolgen van een crisis 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 van een crisis in het digitale domein.

Overkoepelende vraagstukken

In een digitale crisis kan onderscheid worden gemaakt tussen acht overkoepelende vraagstukken ofwel 'Bouwstenen'. De bouwstenen van een digitale crisis zijn relevant voor het in kaart brengen van gevolgen en effecten, de inrichting en werkwijze van de crisisrespons en voor de betrokkenheid van verschillende actoren en organisaties. Bij een digitale crisis zijn de volgende bouwstenen altijd relevant:

- Of er sprake is van (on)opzettelijk handelen.
- Technisch falen binnen of buiten Nederland.
- De betrokkenheid van een statelijke of andere actor.
- Effect op maatschappelijk belangrijke voorzieningen (niet-vitaal).

5. Artikel 14 jo. 15 Wet veiligheidsregio's.

- Effect op vitale processen.
- Regio-overschrijdende effecten (ook fysieke).
- Effect van de crisis in het buitenland.
- De (on)bekendheid van een technisch oplossing perspectief.

In een crisissituatie zal het niet altijd mogelijk zijn om elk van deze vraagstukken te beantwoorden of hier zekerheid over te hebben. Herkenning van (een deel van) de bouwstenen tijdens een crisis zal alsnog direct bijdragen aan het inzichtelijk maken van de crisisbeheersing. Om de bouwstenen effectief te doorgronden is het van belang dat organisaties deze niet alleen refereren in een crisis, maar de bouwstenen met name gebruiken voor de inrichting van oefenscenario's en crisisprocessen in aansluiting op de nationale en decentrale crisisstructuren- en afspraken. In hoofdstuk 4: Bouwstenen is een uitgebreide uiteenzetting van ieder vraagstuk beschikbaar, met een overzicht van mogelijke gevolgen en effecten en de betrokken actoren en organisaties.

Digitale crisisbeheersing in vogelvlucht

Digitale crisisbeheersing onderscheidt zich door intensieve samenwerking tussen verschillende sectoren, netwerken en publieke en private actoren die parallel en gelijktijdig betrokken kunnen zijn bij de beheersing van de digitale en fysieke (gevolg) effecten van een crisis. Tussen al deze partners bestaat een omvangrijk web aan informatiestromen, ook over grenzen heen, waarin duiding, handelingsperspectieven, technische en niet-technische informatie, die van belang zijn voor de crisisbeheersing zo veel als mogelijk worden gedeeld.

Bij een (dreigende) crisis kan de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) via het Nationaal Crisis Centrum (NCC) de nationale crisisstructuur activeren. Hierin wordt afgestemd (en besloten) over de crisisbeheersing tussen alle betrokken ministeries, andere relevante bestuursorganen en private partners, zowel op het digitale als fysieke domein. De invulling van de overleggen binnen de nationale crisisorganisatie is maatwerk, waarbij de hierboven genoemde vraagstukken (bouwstenen) een indicatie leveren van betrokken actoren.

Het Nationaal Cyber Security Centrum (NCSC) is het nationale CERT die in het bijzonder bijstand verleend aan de Rijksoverheid en vitale aanbieders bij digitale dreigingen en incidenten. Ook is het NCSC de operationeel coördinerende organisatie in het kader van de beheersing van digitale crises. Het NCSC is aangesloten op het netwerk van computercrisisteams en andere schakelorganisaties in het Landelijk Dekkend Stelsel (LDS) die elk een sectorale verantwoordelijkheid dragen voor de beheersing van digitale crises. Belangrijke stelselpartners aan de overheidszijde als CIO Rijk, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) werken nauw samen met het NCSC en zijn vanuit de eigen functies en taken betrokken in de crisisbeheersing, evenals in de nationale crisisstructuur.

Het NCSC onderhoudt ten behoeve van zijn taken onder meer ook contacten met internationale partners en private security bedrijven die van betekenis kunnen zijn in de crisisbeheersing.

Vitale en niet-vitale bedrijven, instellingen en organisaties die getroffen worden door een digitale crisis blijven zelf verantwoordelijk voor de continuïteit van de eigen processen en dienstverlening. Er kan in bepaalde gevallen sprake zijn van een wettelijke meldplicht van een incident, daarnaast is het informeren van partners binnen de keten nuttig en nodig. Zie Hoofdstuk 3: Cyberstel en crisisprocessen, Sectie C – Crisisprocessen voor een visualisatie van de mogelijk van toepassing zijnde meldpunten.

Gevolgeffecten op de openbare orde en veiligheid worden bestreden vanuit de veiligheidsregio's en lokale driehoek, gebruikmakend van herkenbare structuren zoals GRIP. Verschillende uitvoeringsorganisaties (zoals Rijkswaterstaat), openbare lichamen en zelfstandige bestuursorganen kunnen vanuit de eigen beleidsverantwoordelijkheid direct betrokken zijn bij de fysieke crisisbeheersing. Het Nationaal Crisis Centrum en de nationale crisisstructuur vormen bij een digitale crisis waarbij nationaal is opgeschaald het koppelvlak tussen de fysieke en digitale crisisbeheersing.

De publieke communicatie over een digitale crisis wordt in de nationale crisisstructuur in of met het Nationaal Kernteam Crisiscommunicatie (NKC) afgestemd. De kern communicatie van het Nationaal Crisis Centrum kan communicatieadviseurs van lokaal of regionaal bevoegd gezag en betrokken departementale directies ondersteunen met adviezen, middelen en een netwerk van ervaringsdeskundigen.

Hoofdstuk 3: Cyberstelsel en crisisprocessen biedt daarnaast een uitgebreide beschrijving van alle betrokken organisaties en actoren, de crisisprocessen en communicatieafspraken- en richtlijnen tijdens een cybercrisis.

Dilemma's en sleutelbesluiten

Digitale crises kennen unieke uitdagingen en afwegingen die (overheids)organisaties, instellingen en bedrijven confronteren met verschillende dilemma's en moeilijke besluiten. Enkele voorbeelden:

- Het wel- of niet gedeeltelijk of volledig afschakelen van ICT-systemen.
- Het in stand houden van de verstoring om grondig forensisch onderzoek mogelijk te maken.
- De prioritering van de inzet van schaarse middelen voor de bestrijding van een digitale crisis of de (mogelijk fysieke) gevolgeffecten.
- Het wel- of niet toepassen van noodwet- en regelgeving bij een (zeer) ernstige crisis.

Een besluit op ieder van de bovenstaande punten kan grote gevolgen hebben voor de continuïteit van (vitale) processen en dienstverlening of delen daarvan, met mogelijke cascade-effecten binnen ketens tot gevolg, ook over grenzen heen. Daarnaast kan de maatschappelijke impact bij het toepassen van wettelijke noodbevoegdheden ook aanzienlijk zijn.

Nafase

In de nafase van een digitale crisis moet in ieder geval aandacht zijn voor o.a. herstel van de continuïteit van processen en dienstverlening, forensisch onderzoek, evaluatie van de crisis, en mogelijk psychische nazorg voor het betrokken personeel. Het dient benadrukt te worden dat na de initiële crisisbestrijding organisaties, instellingen en bedrijven zelf primair verantwoordelijkheid dragen voor de continuïteit van de dienstverlening en mogelijk noodzakelijk herstel of wederopbouw van digitale omgevingen. Zie Hoofdstuk 3: Cyberstelsel en crisisprocessen, Sectie C voor een toelichting op de nafase bij cybercrises.

Doorkijk Nationale Cybersecurity Strategie en het toekomstige stelsel

Op 10 oktober 2022 is de Nederlandse Cybersecurity Strategie 2022-2028 (NLCS) en het bijbehorende actieplan gepubliceerd.[6] In deze strategie zijn pijlers, doelen, subdoelen en acties opgenomen die onder andere effect zullen hebben op de beheersing van digitale crises in Nederland. Zoals in de NLCS weergegeven, is het van belang dat organisaties goed samenwerken in geval van (landelijke) digitale crises, passend bij (boven)regionale en (inter) nationale crisismechanismen.

Eén van de belangrijkste stelselwijzigingen betreft de doorontwikkeling van het Nationaal Cyber Security Centrum tot het nationale CERT. Het NCSC, het Digital Trust Center (DTC) en het CSIRT voor digitale diensten (CSIRT-DSP) zullen daarvoor worden samengevoegd tot één nationale cybersecurityautoriteit, zoals in de NLCS beschreven en in september 2022 aangekondigd in een Kamerbrief over dit onderwerp.[7] Daarnaast wordt meer samenhang gecreëerd tussen andere schakelorganisaties door integratie, waar nuttig, te stimuleren. Dit betekent onder andere dat verkend zal worden of samenvoeging van andere sectorale computercrisisteams met het NCSC toegevoegde waarde heeft.

In aanvulling op de vorming van één nationale CERT zal de overheid samen met het bedrijfsleven een routekaart opstellen voor de implementatie van een publiek-privaat platform voor wederkerige cybersecurity informatie- en kennisdeling om alle betrokken partijen tijdig te voorzien van relevante technische en niet-technische informatie, duiding en handelingsperspectief. Hiervoor zal worden aangesloten bij het volwassenheidsniveau en de behoeften van diverse doelgroepen.

Daarnaast worden in de tweede helft van 2024 de Europese Netwerk en Informatiebeveiliging richtlijn 2 (NIB2) en de richtlijn voor weerbaarheid van kritieke entiteiten (CER) omgezet in nationale wetgeving. Als gevolg van de NIB2 krijgen veel meer sectoren en organisaties binnen de EU te maken met wettelijke verplichtingen voor de beveiliging van netwerk- en informatiesystemen. De taken van organisaties zoals het NCSC en sectorale toezichthouders zullen als gevolg van de implementatie ook flink worden uitgebreid. De CER richt zich op de fysieke veiligheid en beveiliging van vitale processen. Samen bieden de NIS en de CER een kader voor digitale en fysieke weerbaarheid van vitale aanbieders.

Op het gebied van incident response zal het Nationaal Response Netwerk (NRN) doorontwikkeld worden tot een nationaal incident responsnetwerk. Ook zal worden onderzocht of het huidige wettelijke instrumentarium voor ingrijpen bij nationale crises (o.a. noodwetgeving) voldoende is voor een crisis met digitale elementen, met aandacht voor een verdringingsreeks.

Tot slot zal intensiever ingezet worden op een gezamenlijke voorbereiding, oefeningen en aanpak van crises door de Rijksoverheid, interdepartementaal, met de veiligheidsregio's en private partners. Een eerste stap hiertoe is de publicatie van dit Landelijk Crisisplan Digitaal, wat zal worden gebruikt voor de voorbereiding van de landelijke cyberoefening ISIDOOR IV. Ook wordt als actie van de NLCS een bestuurlijk convenant opgesteld met de VNG en de gemeenten ten aanzien van digitale veiligheid waarin de gezamenlijke inzet op het gebied van cybersecurity voor gemeenten nader zal worden uitgewerkt.

Gedurende de levensduur van de NLCS zal jaarlijks worden bezien of het Landelijk Crisisplan Digitaal actualisaties behoeft, aan de hand van nieuwe geleerde lessen en de implementatie van verschillende nieuwe structuren, afspraken en stelselwijzigingen.

6. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028
7. https://open.overheid.nl/repository/ronl-b7f91c5d3699f71604720c497fde8110e343a48c/1/pdf/tk-uitvoerder-programmaplan-sporen-integratie-csirt-dsp-dtc-ncsc.pdf

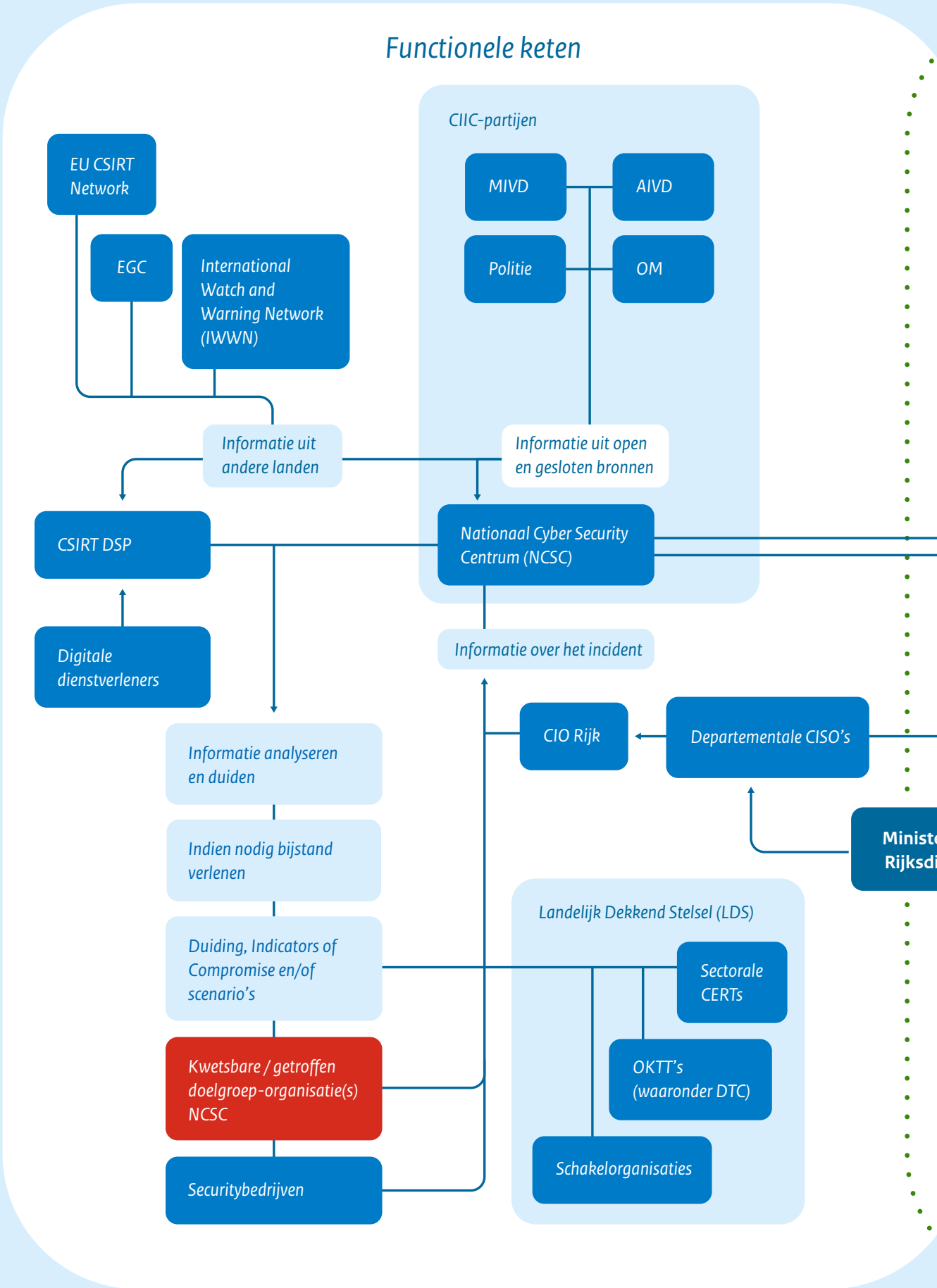
De Eemshavencentrale is de grootste en een van de drie nieuwste kolencentrales van Nederland.

3. Cyberstelsel en crisisprocessen

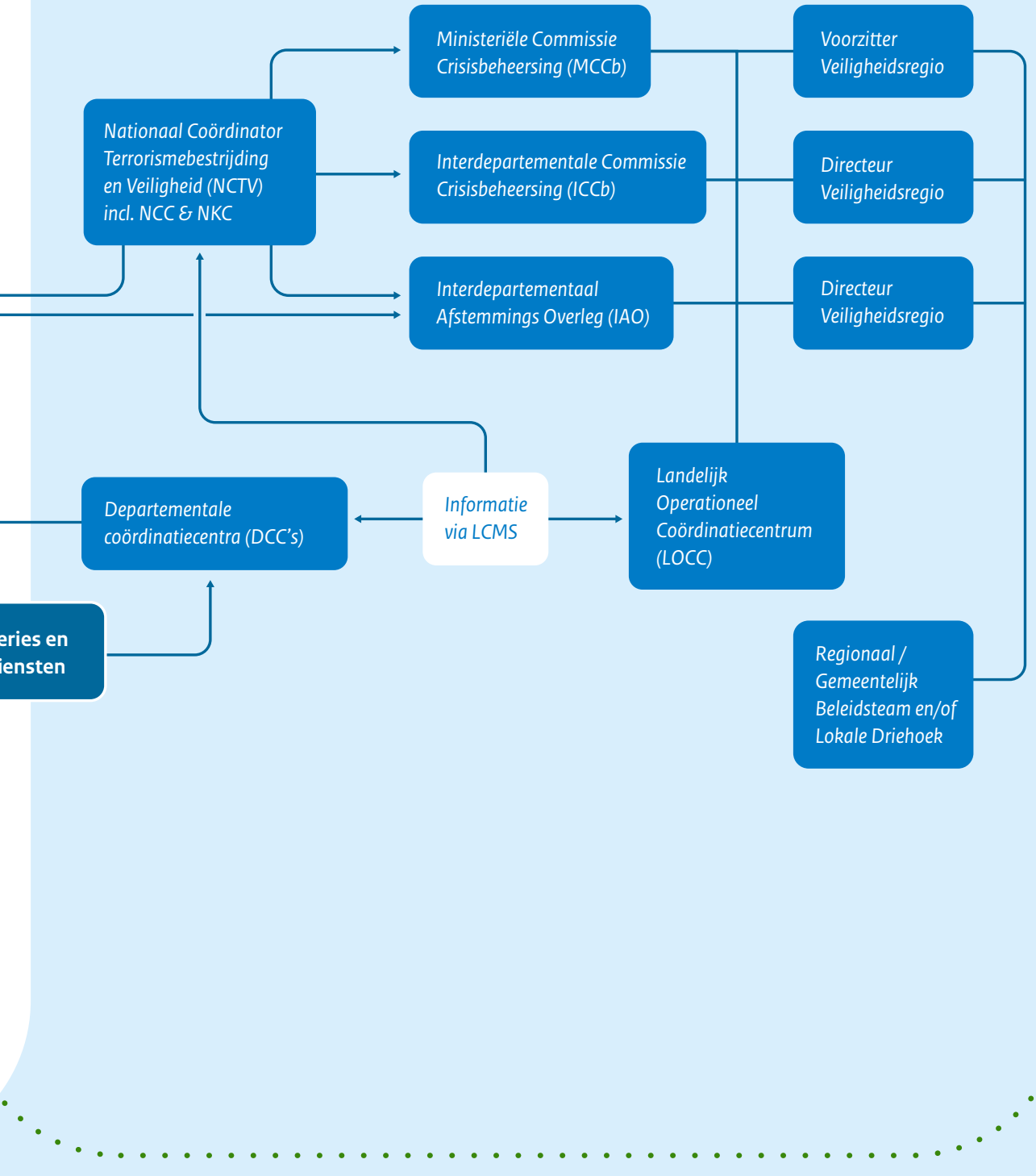
Een digitale crisis is vaak niet opzichzelfstaand en raakt veel facetten binnen onze samenleving. Bij de beheersing van een digitale crisis zijn veel actoren betrokken, zowel in het digitale domein als in het fysieke domein. Daarnaast zijn er zowel publieke-als private partijen betrokken, die allemaal hun eigen verantwoordelijkheid hebben tijdens een digitale crisis maar daarbij ook nauw samenwerken. Vandaar dat het belangrijk is om goed inzichtelijk te hebben op welke manier al deze partijen op elkaar aangesloten zijn, welke taken zij uitvoeren en op welke manier zij met elkaar interacteren.

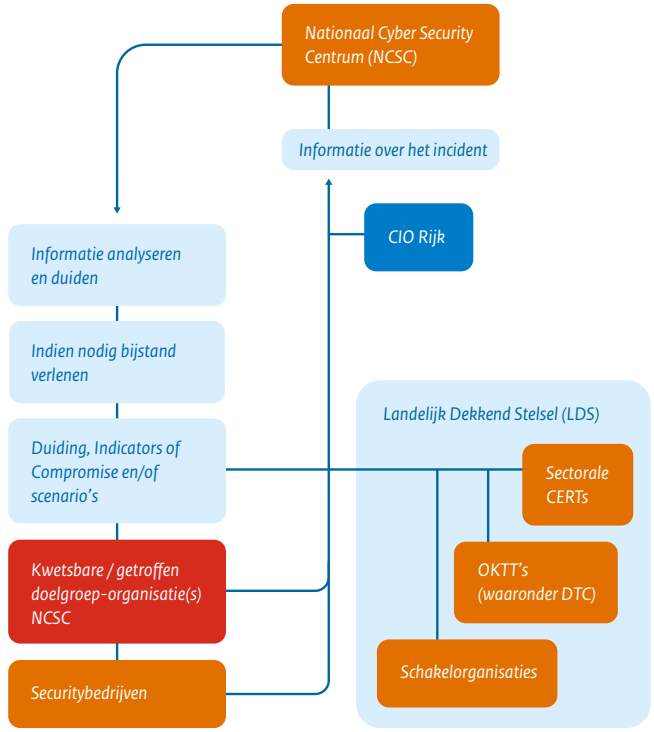
In dit hoofdstuk wordt in meerdere visuele weergaven uitgebeeld op welke manier de cyber-specifieke crisisstructuur aansluit op de reguliere crisisstructuren in Nederland. Hierbij wordt onderscheid gemaakt tussen sectorale crisisstructuren en de aansluiting van deze structuren op zowel landelijk als op regionaal niveau. Er wordt dieper in gegaan op de cyber-specifieke crisisstructuur (sectie A) waarin de operationele coördinatie, incidentanalyse, attributie en opsporing, het bestrijden van de oorzaak en de internationale samenwerking aan bod komt. In het volgende deel wordt de aansluiting van de cyber-specifieke crisisstructuur op de algemene keten (sectie B) geschetst, waarbij wordt ingegaan op bestuurlijke coördinatie, gevolg- en effectbestrijding en informatiemanagement. Tevens bevat dit hoofdstuk rolbeschrijvingen van organisaties die betrokken zijn in digitale crisisbeheersing. Ook bevat dit hoofdstuk informatie over relevante crisisprocessen waaronder melden, alarmeren en opschalen en crisiscommunicatie (Sectie C).

Informatiestromen tijdens (dreigende) crisis



Algemene keten





A. Functionele Keten (Het cyber-specifieke stelsel)

Nationaal Cyber Security Centrum (NCSC)

Het NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC is het nationale CERT, dat in het bijzonder bijstand verleent aan de Rijksoverheid en vitale aanbieders bij digitale dreigingen en incidenten. Bij (dreiging van) grootschalige digitale crises heeft het NCSC een operationeel coördinerende rol. Het NCSC beschikt ten behoeve van zijn taken over een actueel situationeel beeld, staat in nauw contact met (doelgroep)organisaties, legt verbindingen tussen partijen in het cyberstelsel en geeft zo veel als mogelijk adviezen en handelingsperspectief om een digitaal incident tegen te gaan of te voorkomen. Het NCSC levert waar nodig zelf bijstand, bijvoorbeeld door het leveren van incident responscapaciteit.

NCSC vormt de operationele spil in het cyberstelsel van Nederland. De taken van het NCSC bestaan onder meer uit:

- Rijksoverheidsorganisaties en vitale aanbieders bijstaan bij het treffen van maatregelen om de continuïteit van diensten te waarborgen of te herstellen.
- Deze organisaties en aanbieders informeren en adviseren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen.
- Het verrichten van analyses en technisch onderzoek naar aanleiding van digitale dreigingen en incidenten om deze aanbieders bij te staan, te informeren of te adviseren.
- Andere organisaties informeren of adviseren over dreigingen en incidenten bij deze aanbieders
- Schakelorganisaties (krachtens de Wbni aangewezen CERTs en OKTTs), of in bepaalde gevallen individuele andere aanbieders, informeren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen.
- Om cyberincidenten te voorkomen en de weerbaarheid te verhogen, geeft het NCSC weerbaarheidsadvies over cybersecurityrisico's en te treffen maatregelen.
- Het brede publiek in algemene zin adviseren over digitale dreigingen en incidenten.
- Krachtens de Wbni aangewezen vitale aanbieders zijn verplicht incidenten met aanzienlijke gevolgen voor hun dienstverlening bij het NCSC te melden.
- Andere aanbieders en organisaties buiten de Rijksoverheid kunnen eveneens vrijwillig melding doen bij het NCSC in het geval van een incident met aanzienlijke gevolgen voor hun dienstverlening. Hierbij wordt per melding bezien in hoeverre bijstand kan worden geleverd.
- Het NCSC is conform de Wbni het centrale contactpunt (SPOC) voor de beveiliging van netwerk- en informatiesystemen als bedoeld in de Europese NIB-richtlijn. Hiertoe staat het NCSC in nauw contact met nationale autoriteiten en autoriteiten in andere lidstaten.
- Daarnaast neemt het NCSC deel aan internationale samenwerkingsverbanden. Binnen al deze samenwerkingsverbanden bestaan crisisplannen (standard operating procedures) die in werking treden bij (dreiging van) grootschalige grensoverschrijdende incidenten.

Om voorgaande taken te vervullen werkt het NCSC intensief samen met een groot aantal (inter)nationale organisaties en samenwerkingsverbanden, waaronder:

- Het Nationaal Respons Netwerk (NRN). Het NRN is een samenwerkingsverband tussen de Belastingdienst, Rijkswaterstaat, SURFcert, de IBD, Defensie, Z-CERT en het NCSC. Het doel van het NRN is om gezamenlijk de digitale weerbaarheid van de Nederlandse samenleving in het algemeen en de netwerk- en informatiesystemen van partijen in het bijzonder te vergroten. Tevens leidt het NRN tot gezamenlijke bijdrage tijdens grootschalige cybersecurity incidenten in de vorm van het bundelen van de capaciteiten om zodoende de respons op incidenten te versterken. Tenslotte draagt het NRN bij aan het versterken van de kennis- en informatiepositie van de deelnemende organisaties en het voorkomen dan wel tijdig en adequaat pareren van cyberdreigingen.
- In het kader van het Nationaal Detectie Netwerk (NDN) deelt het NCSC, net als de AIVD en de MIVD (acute) dreigingsinformatie met hierop aangesloten organisaties om deze organisaties tegen cyberdreigingen te kunnen beschermen.
- In de Cyber Intel Info Cel (CIIC) brengen NCSC, AIVD, MIVD, Nationale Politie en OM informatie over cyberincidenten en -dreigingen bijeen om hiermee onder meer tot een beter landelijk situationeel beeld en snel handelingsperspectief te komen.
- Voor het NCSC is het van belang om goed samen te werken met security bedrijven. De wijze van samenwerking verschilt per casus, bijvoorbeeld met als doel te komen tot een landelijk situationeel beeld of gecoördineerde incident respons.
- Het NCSC stimuleert en faciliteert samenwerking binnen de vitale infrastructuur en Rijksoverheid in 'Information Sharing and Analysis Centers' (ISAC's), waarbinnen organisaties informatie over incidenten, dreigingen en maatregelen kunnen uitwisselen.
- Onder coördinatie van het NCSC wordt binnen een landelijk dekkend stelsel van samenwerkingsverbanden, bestaand uit sectorale CERT's en andere schakelorganisaties, informatie over incidenten en dreigingen gedeeld.

Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden

Om snel dreigingen te kunnen herkennen is het uitwisselen van kennis, informatie en expertise van belang. Het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden (LDS) voorziet in deze behoefte doordat breder, efficiënter en effectiever informatie wordt gedeeld tussen publieke en private partijen. Door het NCSC kan informatie worden uitgewisseld met schakelorganisaties die krachtens de Wbni aangewezen zijn als CERT's en OKTTs.

De aanwijzing van een schakelorganisatie krachtens de Wbni als computercrisisteam of OKTT maakt het mogelijk voor het NCSC om dreigings- en incidentinformatie met betrekking tot de systemen van aanbieders in de doelgroep van die schakelorganisatie te delen, met inbegrip van tot personen herleidbare gegevens (bijvoorbeeld IP-adressen) en onder extra voorwaarden vertrouwelijke tot een aanbieder herleidbare informatie.

Op de website van het NCSC staat een actueel overzicht van de CERT's en OKTTs in het Landelijk Dekkend Stelsel.[8]

Digital Trust Center (DTC)

Het Ministerie van Economische Zaken en Klimaat draagt bij aan het verhogen van de cybersecurity van het niet-vitale bedrijfsleven door de inzet van het Digital Trust Center (DTC). Het DTC heeft onder meer proactieve ondersteuning bij preventie tot taak. Het DTC richt zich op het niet-vitale bedrijfsleven, draagt een generieke boodschap uit met betrekking tot het verhogen van de weerbaarheid / cyber security en heeft als taak algemene voorlichting.

Het DTC werkt nauw samen met het NCSC.

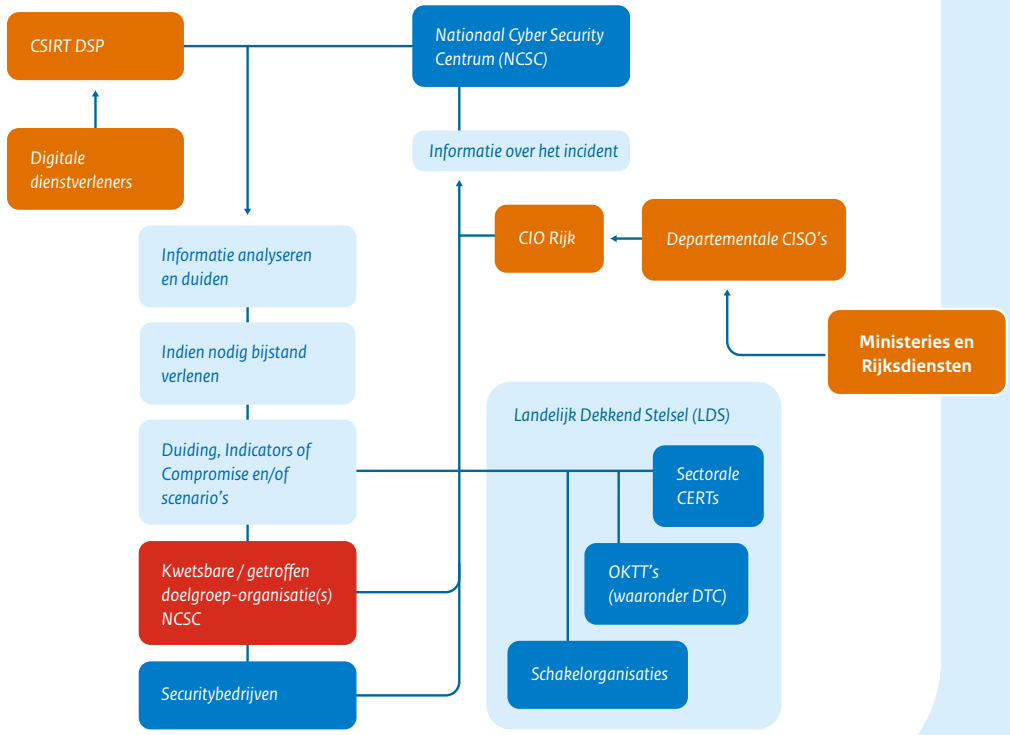
Vitale aanbieders

Vitale aanbieders zijn partijen die een dienst exploiteren, beheren of beschikbaar stellen waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Vitale aanbieders hebben primair zelf een verantwoordelijkheid voor het ongestoord verlopen van hun dienstverlening binnen als vitaal aangemerkte processen (bijvoorbeeld elektriciteit, internettoegang, drinkwater en betalingsverkeer). Deze processen vormen tezamen de vitale infrastructuur.

Vitale aanbieders behoren (naast de Rijksoverheid) tot de doelgroep van het NCSC en hebben op grond van de Wbni recht op bijstand, informatie en adviezen van het NCSC. Verschillende vitale aanbieders hebben een meldplicht bij hun toezichthouder van incidenten met aanzienlijke gevolgen voor hun dienstverlening en bij het NCSC van inbreuken op de beveiliging op netwerk- en informatiesystemen die dergelijke aanzienlijke gevolgen kunnen hebben. Specifieke vitale aanbieders (AEDs) hebben ook een zorgplicht voor de eigen netwerk- en informatiesystemen.

Vitale aanbieders hebben veelal een eigen CISO-organisatie en/of worden ondersteund door private security bedrijven voor de beveiliging van de eigen (digitale) organisatie en de beheersing van incidenten in IT/OT-systemen.

8. Aansluiting op het Landelijk Dekkend Stelsel (LDS) | Samenwerkingspartner worden | Nationaal Cyber Security Centrum (ncsc.nl).



CSIRT-DSP

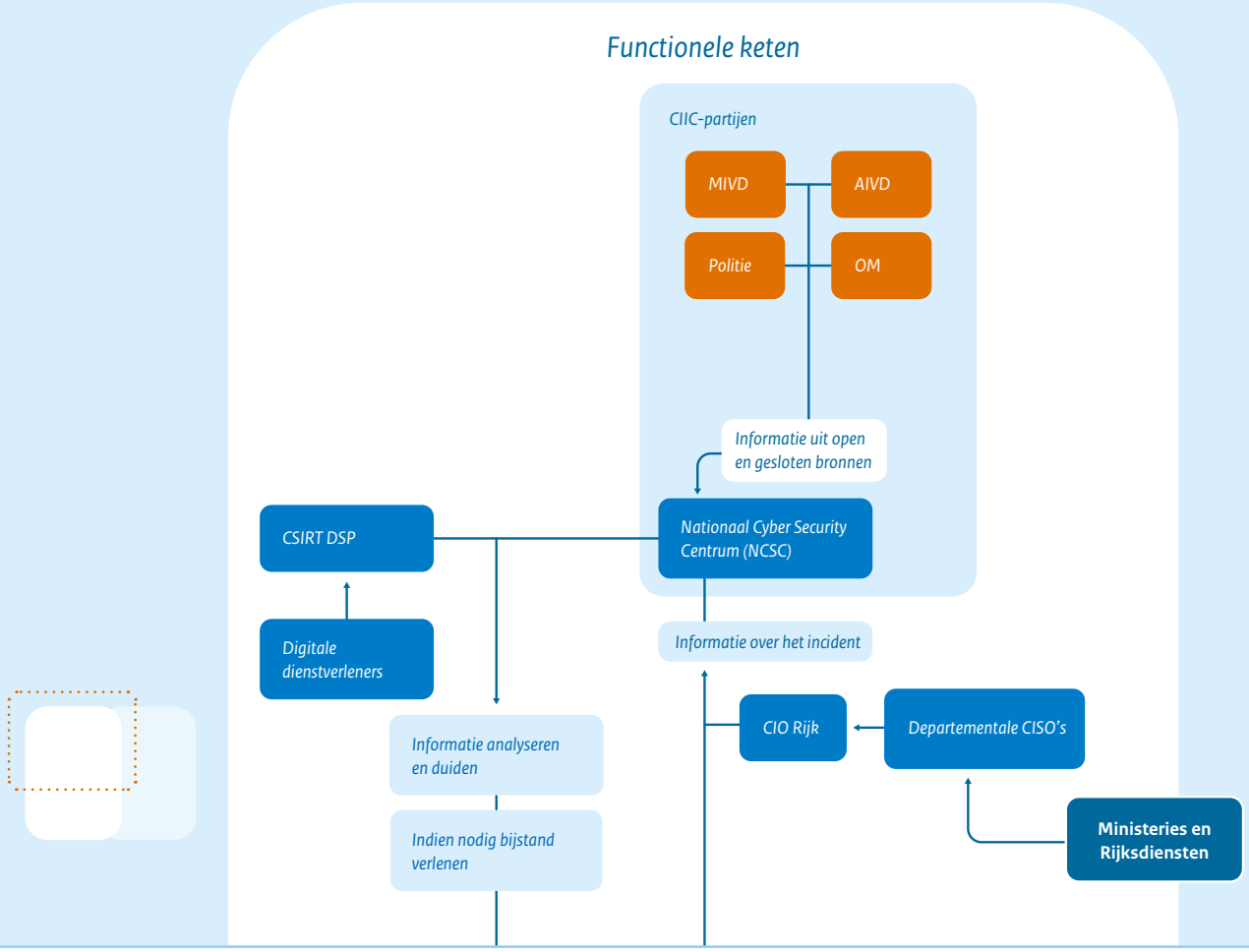
Het CSIRT-DSP is het nationale Computer Security Incident Response Team voor digitale dienstverleners. De taken van het CSIRT-DSP zijn, vanwege de implementatie van de Europese NIB-richtlijn, geregeld in de Wet beveiliging netwerk- en informatiesystemen (Wbni).

Digitale dienstverleners hebben een meldplicht voor incidenten met aanzienlijke gevolgen voor hun netwerk- en informatiesystemen en een zorgplicht (het treffen van beveiligingsmaatregelen ten aanzien van hun netwerk- en informatiesystemen). Deze digitale dienstverleners zijn onlinemarktplaatsen, onlinezoekmachines en cloud-computerdiensten. Naast dit meldpunt ondersteunt het CSIRT-DSP haar doelgroep door het monitoren van incidenten op nationaal niveau, het voorzien van relevante informatie over risico's en incidenten, het bijstand verlenen bij incidenten en het zorgen voor risico- en incidentanalyses. Zo waarschuwt het CSIRT-DSP haar doelgroep onder andere als het bekend is dat er kwetsbare systemen draaien en over kwetsbaarheden in software. Het CSIRT-DSP probeert samen met digitale dienstverleners Nederland digitaal weerbaarder te maken. Hiervoor wordt nauw samengewerkt met het NCSC, het DTC en het EU CSIRT-netwerk.

Departementale CIO's, CISO's, CIO Rijk, CISO Rijk en beveiligingsautoriteit Rijk

Onder coördinatie van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties hebben departementale CIO's en CIO Rijk op grond van het besluit CIO Stelsel een belangrijke rol op het gebied van informatiebeveiliging. De departementale CISO kan namens de secretaris-generaal en de departementale CIO en in afstemming met de beveiligingsautoriteit van het ministerie, aanwijzingen geven aan iedere ambtenaar, externe medewerkers en bezoekers, voor zover dat noodzakelijk is voor de uitvoering van het departementale informatiebeveiligingsbeleid en de naleving van de informatiebeveiligingsvoorschriften. De CISO Rijk heeft een interdepartementale coördinatierol bij Rijksbrede informatiebeveiligingsincidenten en -calamiteiten. De CISO Rijk kan, na afstemming met de betreffende departementale CISO, in het geval van een, mogelijke, ernstige, acute, departement-overstijgende inbreuk op de beveiliging van informatiesystemen of een risico daarop, namens de secretaris-generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onder meer aanwijzingen geven en maatregelen (laten) treffen. De CISO Rijk stemt onverwijld af met de CIO Rijk, de beveiligingsautoriteit Rijk en betrokken departementen over een (mogelijke) inbreuk of het risico daarop en de genomen maatregelen en heeft daarbij in afstemming met de departementale CISO's indien nodig direct toegang tot de secretaris-generaal van ministeries.

Bij een (dreigend) cyberincident zijn de departementale crisisorganisaties aanspreekpunt voor het NCC. Daar waar een (dreigend) cyberincident meerdere departementen raakt en inhoudelijke coördinatie nodig is, dan is de CIO Rijk hiervoor het aanspreekpunt, als voorzitter van de CISO-raad. De CISO Rijk kan, gehoord hebbende de CISO-raad, escaleren naar de ambtelijke/politieke top van BZK. Bij activering van de crisisstructuur neemt CISO Rijk deel aan het IAO. De directeur-generaal Digitalisering en Overheidsorganisatie (DGDOO) ,waar CISO Rijk onder valt, neemt dan deel aan de ICCb.



Algemene Inlichtingen- en Veiligheidsdienst (AIVD)

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. Dat doet de dienst in direct contact met slachtoffer en doelwitorganisaties, maar ook in samenwerking en afstemming met het NCSC, overige CIIC-deelnemers en andere partijen binnen de Rijksoverheid. Bovendien is een belangrijke taak voor de AIVD om beleidsmedewerkers en bestuurders te informeren, zodat zij in staat gesteld worden tot het voeren van effectief ICT-veiligheidsbeleid. Daarnaast verstrekt de AIVD informatiebeveiligingsadviezen op maat, gericht op statelijke actoren, aan de Rijksoverheid en andere belanghebbenden, zoals vitale aanbieders. Het doel van deze adviezen is de weerstand tegen digitale aanvallen van statelijke actoren te verhogen en (digitale) schade te beperken of te voorkomen. Hierbij werkt de AIVD nauw samen met het NCSC. 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 hierop aangesloten organisaties binnen hun eigen verantwoordelijkheden maatregelen kunnen treffen.

Militaire Inlichtingen- en Veiligheidsdienst (MIVD)

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 statelijke actoren detecteren en mitigeren en (potentiële) slachtoffers informeren. Hierbij wordt nauw samengewerkt met het NCSC. Tevens worden bewustwordingspresentaties gegeven 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 beveiligingsautoriteit de Algemene Beveiligingseisen voor Defensie Opdrachten (ABDO) uit door hierover te adviseren en toe te zien op de handhaving en toezicht van dit kader.

Openbaar Ministerie (OM)

Het OM is bij een (dreigend) incident en/of crisis 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 strafbare feiten te voorkomen of doen stoppen door middel van het strafrecht of door het laten treffen van maatregelen in het kader van bewaken en beveiligen;
- de rechtsorde strafrechtelijk handhaaft door het leiden van opsporingsonderzoeken en de vervolging van (rechts)personen voor strafbare feiten, en daarbij ook alternatieve interventie-methoden gebruikt zoals het notificeren van slachtoffers, het verstoren van criminele activiteiten of het voorkomen van nieuw slachtoffer- of daderschap. Het OM werkt daarbij nauw samen met internationale en private partners.

Politie

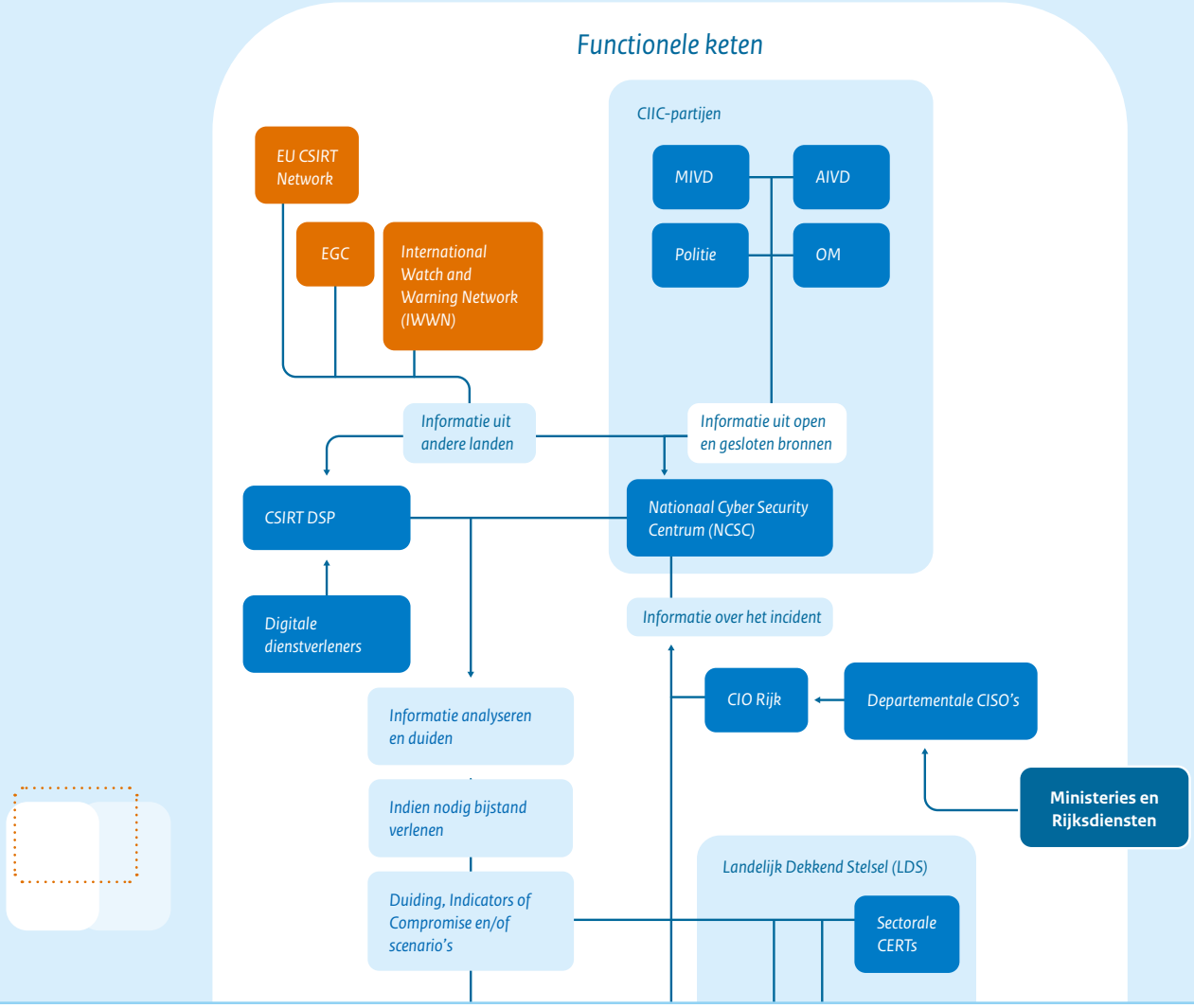
Bijzondere opsporingsbevoegdheden kunnen ingezet worden om eventuele verdachten van (tot crisis leidende) cybercrime te traceren, strafbare feiten te stoppen en te voorkomen (waar mogelijk) en criminele infrastructuren te ontmantelen. Dit kan leiden tot het verhinderen/verstoren van de criminele activiteiten en/of het aanhouden van verdachten in binnen- of buitenland. 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 informatie uitwisselen 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 verantwoordelijk voor het technisch beheer van de 112-meldkamers.

Cyber Intel/Info Cel (CIIC)

AIVD, MIVD, Politie, NCSC en OM werken samen in de Cyber Intel/Info Cel als bedoeld in het Convenant samenwerking CIIC[9]. Het doel van de Cyber Intel/Info Cel is het versterken van een landelijk situationeel beeld ten aanzien van cyberdreigingen en -incidenten, het op basis daarvan door partijen in relatie tot die dreigingen en incidenten beter kunnen uitoefenen van hun wettelijke taken, het meer en sneller bieden van handelingsperspectief aan andere belanghebbende organisaties inzake cyberdreigingen, en het hierdoor vergroten van de digitale slagkracht van genoemde organisaties en versterken van de veiligheid in het digitale domein. Hiertoe brengen de deelnemende organisaties informatie over cyberdreigingen en –incidenten bijeen, wordt die informatie door medewerkers van de deelnemende organisaties gezamenlijk beoordeeld, en kan van hieruit relevante informatie aan belang-hebbende organisaties worden verstrekt.

9. Staatscourant 2020, 30702 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)



Internationale partners en samenwerkingsverbanden

Europese Unie

In de Europese Netwerk en informatiebeveiligingsrichtlijn (NIB) uit 2016 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 informatie-systemen. 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 respons-organisatie voor incidenten in het digitale domein.

Op Europees niveau is een blauwdruk[10] 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.

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. Voor specifieke cyber-expertise binnen het justitiële domein kan Eurojust een beroep doen op het Europees Justitieel Cybercrime Netwerk (EJCN).

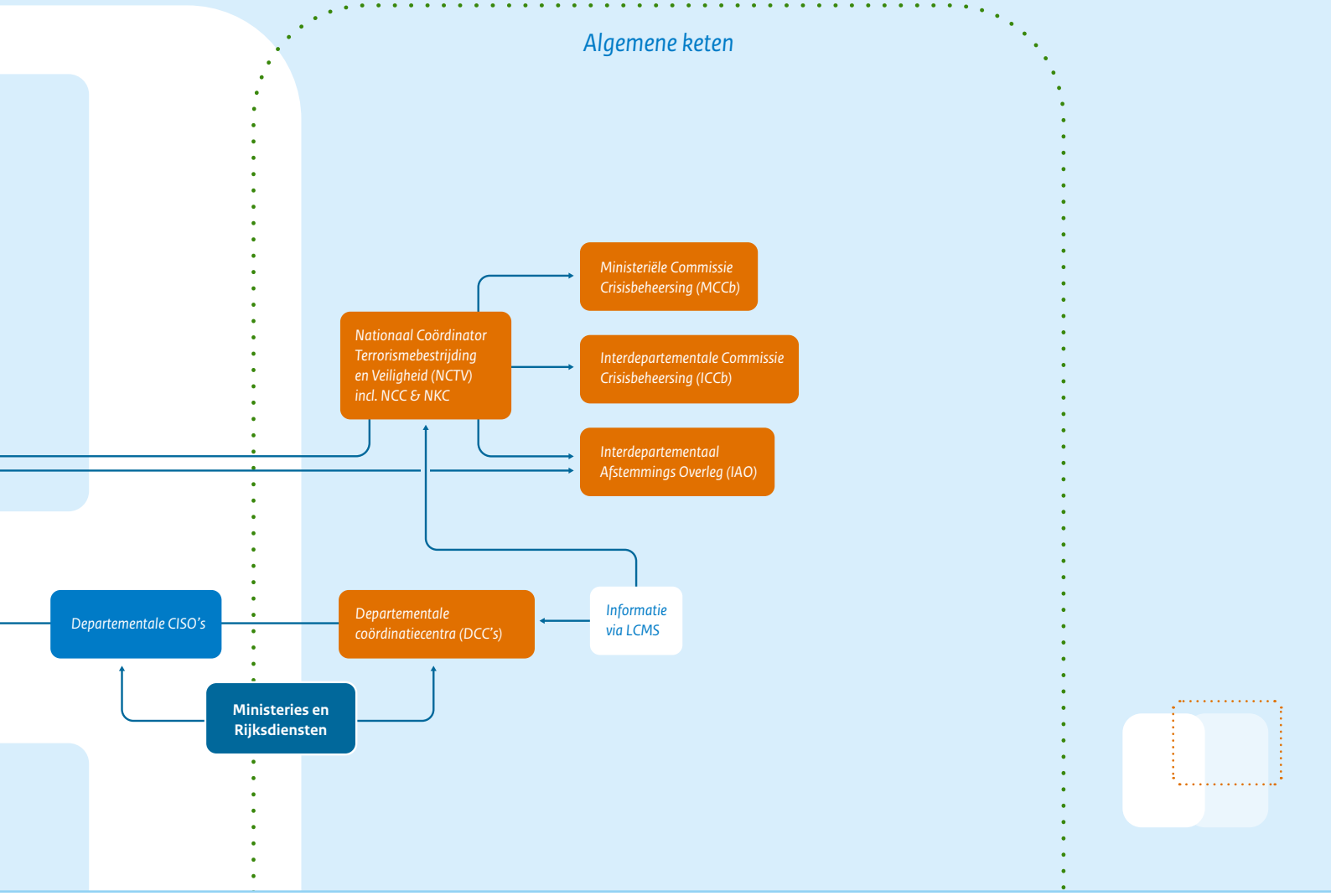
10. Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises, 13 September 2017 (L239/36).

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 CERT's 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.



B. Algemene Keten (Nationale crisisstructuur)

Nationaal Coördinator Terrorismebestrijding en Veiligheid

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), onderdeel van het Ministerie van Justitie en Veiligheid, beschermt Nederland tegen maatschappelijk ontwrichtende dreigingen en coördineert cybersecuritybeleid in Nederland, waaronder de inrichting van het cybersecuritystelsel. De NCTV is opdrachtgever van het NCSC en voorziet de Minister van Justitie en Veiligheid van strategische duiding en advies bij een (dreigende) cybercrisis. Ook heeft de NCTV een overkoepelende bestuurlijke en coördinerende rol bij nationale crisisopschaling en is zodoende betrokken in zowel de functionele als algemene ketens. De NCTV faciliteert en ondersteunt interdepartementaal op ambtelijk en politiek-bestuurlijk niveau de crisisbesluitvorming via het Nationaal Crisis Centrum (NCC). De Minister van Justitie en Veiligheid is coördinerend minister voor crisisbeheersing en cybersecurity.

Wanneer de nationale crisisstructuur, of onderdelen daarvan, opgeschaald wordt vanwege een (dreigende) cybercrisis, dienen de functionele keten (cyber-specifiek) en de algemene keten (nationale crisisstructuur) met elkaar in verbinding gebracht te worden. Bij een (dreigende) nationale cybercrisis wordt er gewerkt vanuit bestaande afspraken conform het Instellingsbesluit Ministeriële Commissie Crisisbeheersing en het Nationaal Handboek Crisisbeheersing. Voor de organisatie, inrichting en werkwijze van de nationale crisisstructuur is optimale flexibiliteit het uitgangspunt. Voor alle onderdelen en overleggen binnen die structuur geldt dat deze naar behoefte worden ingezet en flexibel ingericht en samengesteld zijn. Er is sprake van maatwerk per situatie en zo nodig per bijeenkomst.

De **Ministeriële Commissie Crisisbeheersing** (MCCb) is verantwoordelijk voor de coördinatie en besluitvorming op politiek-bestuurlijk niveau over de te 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 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.

De MCCb en ICCb worden ondersteund en geadviseerd door een **Interdepartementaal Afstemmingsoverleg** (IAO) onder voorzitterschap van de NCTV. In een (dreigende) nationale cybercrisis zullen vertegenwoordigers van de beleidsverantwoordelijke departementen, betrokken departementale crisiscentra, het NCSC en andere betrokken partners in het cybernetwerk deelnemen aan het IAO. In het IAO wordt een landelijk situationeel beeld verzameld, mogelijke maatregelen afgestemd en besluiten voor het ICCb en MCCb voorbereid.

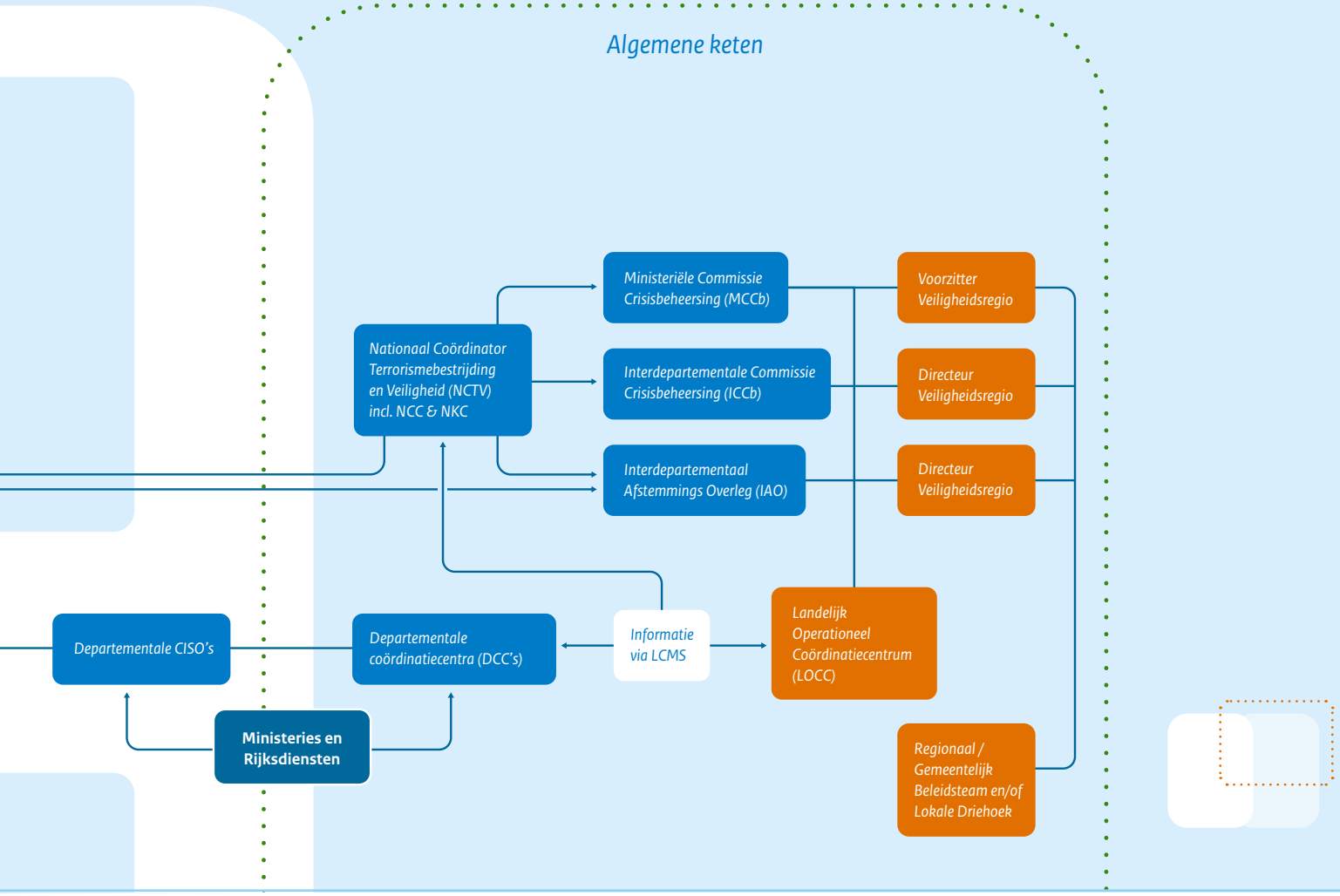
Het **Nationaal Crisiscentrum** (NCC) is onderdeel van de NCTV en het interdepartementaal coördinatiecentrum en knooppunt van en voor de bestuurlijke informatievoorziening en de crisiscommunicatie. Het NCC is de ondersteunende c.q. uitvoerende staf en het facilitair bedrijf ten dienste van de (voorbereiding 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 op nationaal niveau de afspraken en structuren van het Nationaal Handboek Crisisbeheersing (NHC, 2022).

Het NCC is 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 het Landelijk Operationeel Coördinatie Centrum (LOCC), bijvoorbeeld ten aanzien van onderwerpen als informatievoorziening en crisiscommunicatie.

De **Departementale Coördinatiecentra** (DCCs), of een ander daartoe aangewezen onderdeel binnen het verantwoordelijk ministerie, zijn verantwoordelijk voor de uitvoering en coördinatie van de departementale responsactiviteiten binnen de eigen sector. Dit geldt ook bij een digitale crisis/crisis met een digitaal component, hierin zijn zij de schakel tussen het getroffen of betrokken vakdepartement, de eigen sector en de nationale crisisstructuur.

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.



Het **Landelijk Operationeel Coördinatie Centrum** (LOCC) is onderdeel van het Ministerie van Justitie en Veiligheid, maakt deel uit van de nationale crisisstructuur en neemt deel aan het IAO. Bij het LOCC werken ervaren medewerkers vanuit de verschillende organisaties binnen het veiligheidsdomein zoals de veiligheidsregio's, de nationale politie, de brandweer, het ministerie van Defensie, GGD/GHOR, RIVM en het Rode Kruis. Het LOCC is daarmee organisatorisch en in de uitvoering een multidisciplinaire organisatie.

Taken van het LOCC zijn:

- Het zorg dragen voor het aanleveren van het multidisciplinair Landelijk Operationeel Beeld en het operationeel advies bij nationale en internationale incidenten, crises, rampen en grootschalige evenementen;
- het coördineren van regionale, nationale en internationale bijstand, met inbegrip van de bijstand, bedoeld in de Wet veiligheidsregio's en de Politiewet 2012;
- het op verzoek van betrokken partners ondersteunen bij regionale en bovenregionale incidenten, crises, rampen en grootschalige evenementen; en
- het, als zijnde de National Training Coördinator, zorgdragen voor de coördinatie, opleiding en inzet van de Nederlandse experts in het kader van het EU Civil Protection Mechanism.

Veiligheidsregio's (regionale crisisorganisatie)

De **regionale crisisorganisatie** binnen een veiligheidsregio wordt in de basis gevormd door de hulpverleningsdiensten (brandweer, politie en geneeskundige hulpverlening) en de gemeenten, onder het gezag van de burgemeester of de voorzitter veiligheidsregio. Veiligheidsregio's dienen zorg te dragen voor de inrichting van de regionale crisisorganisatie inclusief de mogelijkheid tot aanhaken van benodigde crisispartners gegeven de situatie.

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 door openbare orde en veiligheidseffecten te beperken en inwoners te voorzien van handelingsperspectief. De focus van de veiligheidsregio ligt bij de gevolgbestrijding van de (fysieke) effecten in de samenleving, van maatschappelijke ontwrichting en op het beschermen en voorlichten van burgers en deelnemende organisaties en instellingen. Daarbij gaat het om bevolkingszorg, brandweerzorg, geneeskundige zorg, leiding en coördinatie, informatiemanagement en crisisbeheersing in de zin van de Wet veiligheidsregio's (Wvr).

In samenwerking met partners duiden de veiligheidsregio's de mogelijke maatschappelijke impact van een digitaal incident in hun regio. Hierbij wordt gekeken naar mogelijke cascade-effecten. Inzicht in het incident en de mogelijke risico's en cascade-effecten is essentieel voor de crisisbeheersing, de communicatie richting burgers en getroffen organisaties, en ten behoeve van de normalisering van de samenleving na een incident.

De veiligheidsregio's investeren 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.[11] Het NCC is voor de veiligheidsregio's nationaal contactpunt voor het Rijk.

Bij een cybercrisis in het geografisch gebied van de gemeente kan de burgemeester, of voorzitter veiligheidsregio, als bevoegd gezag gebruik maken van de crisisbeheersingsstructuur. Er kan dan binnen de GRIP-structuur worden opgeschaald om snel een crisisteam te formeren en heldere informatie-besluitvormingslijnen te creëren. De burgemeester, of voorzitter veiligheidsregio, laat zich in het Gemeentelijk Beleidsteam (GBT), of Regionaal Beleidsteam (RBT), adviseren over de consequenties van de digitale verstoring op het maatschappelijk leven en de te nemen maatregelen omtrent de effectbestrijding. Deze opschaling vindt onder meer plaats als de effecten van deze cybercrisis leiden tot brede maatschappelijke impact en (grootschalige) inzet van de hulpverleningsdiensten. Indien blijkt dat de crisis ook (grote) effecten heeft op de openbare orde en veiligheid, of dat er behoefte is aan extra opsporingsbevoegdheden om de actor te achterhalen, komt de *driehoek* bij elkaar.[12] De politie staat onder duaal gezag: voor de handhaving van de openbare orde en voor de hulpverlening ligt het gezag bij de burgemeester en voor de strafrechtelijke handhaving ligt het gezag bij de officier van justitie. Dit overleg tussen politie, burgemeester en OM is de lokale gezagsdriehoek. De informatie uit het driehoeksoverleg wordt waar relevant voor de crisisbeheersing gedeeld met het beleidsteam op basis van *need-to-know*.

11. Artikel 7, 3e lid Wet veiligheidsregio's wetten.nl - Regeling - Wet veiligheidsregio's - BWBR0027466 (overheid.nl)
12. Artikel 13 Politiewet 2012. wetten.nl - Regeling - Politiewet 2012 - BWBR0031788 (overheid.nl).

C. Crisisprocessen

Deze paragraaf bevat een beschrijving van de relevante crisisprocessen bij een digitaal incident waaronder melden, alarmeren en opschalen en crisiscommunicatie. Deze omschrijving is algemeen van aard. Afhankelijk van de sector waarin een organisatie zich bevindt, kunnen nog sectorspecifieke dynamieken of afspraken geldend zijn waarvan het belangrijk is dat deze inzichtelijk zijn in de eigen operationeel uitgewerkte crisisplannen.

1. Melden, alarmeren en opschalen

Bij incidenten in digitale processen en systemen doorloopt het proces van melden, alarmeren en opschalen verschillende organisaties, afhankelijk van de aard en omvang van een incident en wettelijke rollen en taken. Bij melding van een incident dient rekening gehouden te worden met effecten op de digitale organisatie, effect op de continuïteit van de dienstverlening en mogelijke effecten op de fysieke veiligheid en openbare orde.

Op grond van de Wbni hebben de meeste vitale aanbieders als plicht om incidenten die aanzienlijke gevolgen hebben of kunnen hebben voor de continuïteit van de door hen verleende dienst te melden aan het NCSC. Vitale aanbieders die zijn aangewezen als aanbieders van een essentiële dienst hebben daarnaast tot plicht om incidenten met aanzienlijke gevolgen te melden bij hun sectorale toezichthouders. Digitale dienstverleners hebben ook een meldplicht bij zowel het CSIRT-DSP als het Agentschap Telecom.

Andere aanbieders kunnen een digitaal incident melden bij hun sectoraal computercrisisteam dat deel uitmaakt van het LDS, als ze tot de doelgroep daarvan behoren.

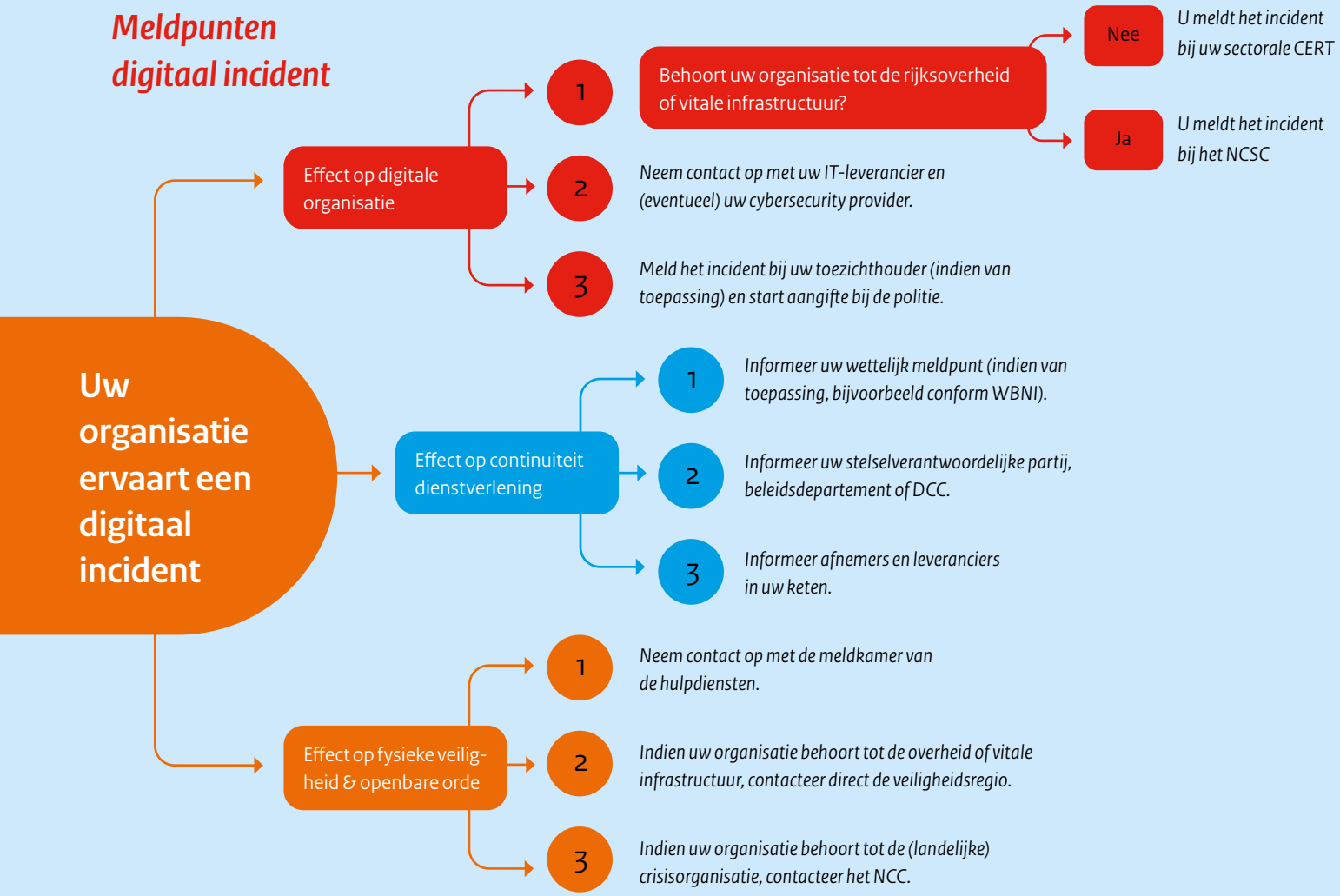
Afhankelijk van de aard en omvang van een incident kan een sectoraal computercrisisteam, betrokken crisisorganisatie en/of het NCSC besluiten intern op te schalen. Bij een (dreigend) grootschalig digitaal incident adviseert het NCSC de NCTV over mogelijke inzet van de nationale crisisstructuur of onderdelen daarvan. Het opschalen van (onderdelen van) de nationale crisisstructuur gebeurt conform het Nationaal Handboek Crisisbeheersing.

Als een incident gevolgen heeft voor de continuïteit van de dienstverlening dient de getroffen organisatie zijn wettelijk meldpunt (indien van toepassing) en stelselverantwoordelijke partij of departementale crisiscentrum in te lichten en op de hoogte te houden. Ook is het van belang ketenpartners en leveranciers op de hoogte te stellen.

Vanwege de (potentiële) impact van een digitaal incident kan ook sprake zijn van gevolgen voor de fysieke veiligheid en openbare orde. Het NCC informeert bij grootschalige (dreigende) crises de betrokken veiligheidsregio('s) en/of lokaal bevoegd gezag over het incident met mogelijke cascade- en gevolgeffecten, indien hier aanleiding toe is. Daarnaast kunnen incidenten met gevolgen voor de fysieke veiligheid en openbare orde, direct gemeld worden bij de betrokken (hulp)diensten en/of regionale of lokale overheden, waaronder de veiligheidsregio. Informatie over een incident met (mogelijke) fysieke gevolgen binnen het regionaal of lokaal domein kan door de veiligheidsregio gecommuniceerd worden aan andere medeoverheden (gemeenten, provincies en waterschappen). Voor de fysieke gevolgbestrijding kan er door de veiligheidsregio worden opgeschaald vanuit bestaande en herkenbare structuren, bijvoorbeeld binnen de GRIP-structuur op regionaal niveau.

In het geval van een (dreigende) cybercrisis zijn getroffen organisaties zelf primair verantwoordelijk voor het oplossen van de digitale verstoring binnen hun eigen organisaties. Het NCSC ondersteunt de Rijksoverheid en vitale aanbieders bij het treffen van maatregelen om de continuïteit van de dienstverlening te waarborgen of (in geval van incidenten) te herstellen.

Voor een overzicht van meldpunten bij een digitaal incident kunt het figuur op de volgende pagina raadplegen.



2. Crisiscommunicatie

Crisiscommunicatie is gericht op het beantwoorden van de maatschappelijke informatiebehoefte, op schadebeperking en op betekenisgeving. In een tijd waarin door sociale media informatie (of die nu waar is of niet) binnen enkele minuten massaal gedeeld kan worden, zijn heldere uitgangspunten over communicatie van groot belang.

De grote complexiteit van digitale incidenten en de verwevenheid van het digitale met het fysieke domein maken het tijdig bepalen van gevolgen van potentiële cybercrises lastig. Maatschappelijke ontwrichting als gevolg van incidenten in het digitale domein wordt 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. Bij een cybercrisis ligt de kern bij het vertalen van complexe technische problematiek naar begrijpelijke algemene communicatie. Het bij elkaar brengen van de functionele en algemene ketens vindt ook plaats bij het NKC, met een belangrijke rol vanuit het NCSC. Ook de verbinding publiek-privaat vindt hier plaats.

Deze onzekerheid moet partijen er niet van weerhouden te communiceren. Integendeel, tijdens een crisis is zichtbaarheid, eenduidigheid en tijdigheid in de communicatie van doorslaggevend belang. In geval van een (dreiging van een) crisis in het digitale domein met aanzienlijke maatschappelijke gevolgen stemmen alle relevante partijen daarom hun timing en inhoud van communicatie zoveel mogelijk met elkaar af. Uitgangspunt is dat wordt vastgehouden aan bestaande structuren, rollen en werkwijzen, met oog voor het bijzondere dat het digitale domein met zich meebrengt.

In de geactualiseerde *Koepelnotitie Crisiscommunicatie in het digitale domein* (NCTV 2022) zijn verantwoordelijkheden, uitgangspunten voor de communicatie en wijze van afstemming verder uitgewerkt. Ook de rolverdeling in de communicatie tussen partners op (inter) nationaal en regionaal niveau en kernboodschappen zijn opgenomen. Daarbij ligt de focus overigens niet alleen op crisiscommunicatie bij een digitale crisis met maatschappij-ontwrichtende effecten; ook bij een digitale dreiging of een digitaal incident met beperkte (regionale) gevolgen is crisiscommunicatie en landelijke afstemming vaak snel aan de orde. De Koepelnotitie is in samenwerking met diverse partners tot stand gekomen: NCSC, BZK, EZK, IenW, Politie en vertegenwoordigers van de Veiligheidsregio's en het OM.[13]

13. De Koepelnotitie is te vinden op www.nctv.nl.

Nationaal

Zodra de nationale crisisstructuur is geactiveerd, wordt het NKC ingesteld, met communicatieprofessionals van het NCC en de meest betrokken departementen. Het NKC coördineert de pers- en publieksvoorlichting vanuit de Rijksoverheid, adviseert de crisisoverleggen op Rijksniveau over de te volgen communicatiestrategie en de communicatieve gevolgen van (voor)genomen besluiten. Het NKC communiceert over zichtbare maatregelen of over de dreiging die nog niet zichtbaar is 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 partners buiten de Rijksoverheid, zoals veiligheidsregio/direct betrokken gemeente(n), organisaties en instellingen.

Ook als de nationale crisisstructuur (nog) niet is geactiveerd bij een dreiging of incident in het digitale domein, is het vaak raadzaam om interdepartementaal en tussen Rijk en regio's af te stemmen over communicatie. De Afdeling Communicatie van het NCC organiseert deze afstemming en ondersteunt indien nodig communicatieadviseurs van het lokaal of regionaal bevoegd gezag en de betrokken departementale directies Communicatie met adviezen, middelen en een netwerk van ervaringsdeskundigen.

Regionaal

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

Bij een cybercrisis richt de voorzitter van de veiligheidsregio of de burgemeester zich bij de communicatie op zijn/haar eigen regio/gemeente, daarbij rekening houdend met wat er in de eventuele buurgemeente/regio of door het Rijk gecommuniceerd wordt. Hierbij zal veel afstemming moeten plaatsvinden met de betrokken partijen in zowel de functionele als algemene keten. Het NKC is een belangrijke partner bij crises met bovenregionale effecten. Daarnaast zal er altijd met het OM afstemming moeten plaatsvinden over de wijze van communiceren rondom het opsporingsproces. Dit wijkt niet af van andere type crises waar sprake is van moedwilligheid of schuldvraag.

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 met het Benelux Crisis Centre Communication.

Verantwoordelijkheden

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

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

Aandachtspunten voor crisiscommunicatie bij een digitaal incident

Het doel van crisiscommunicatie is eenduidige en tijdige (publieks) communicatie. Dat vraagt om een proactieve manier van communiceren: omgevingsbewust, open, tijdig en consistent – ook als er nog weinig informatie bekend is. In dat geval ligt de focus op procescommunicatie: vertellen wat wel en niet bekend is en welke stappen worden gezet. Zo blijft de overheid zichtbaar. Communicatie van bestuurders verbindt de samenleving en appelleert aan de veerkracht van individuele burgers en van de Nederlandse samenleving als geheel.

Zolang niet zeker is of een crisis het gevolg is van opzettelijk handelen, worden verwijzingen naar mogelijke oorzaken, duur en omvang zoveel mogelijk vermeden. Zodra dat kan, wordt het publiek geïnformeerd over zichtbare maatregelen en indien wenselijk/mogelijk over onzichtbare maatregelen. Belangrijk in elke fase is waar mogelijk antwoord te geven op de vraag: wat kunnen mensen doen? Hoe kan men zelf handelen en anderen helpen? Zo wordt de (zelf)redzaamheid van getroffenen en betrokkenen bevorderd.

Bij een crisis wordt veel en vaak informatie verspreid – ook onjuiste informatie. Het is belangrijk alert te zijn op desinformatie, te bevestigen wat waar is en tegelijkertijd onjuiste geruchten te ontkrachten of te laten weten dat geruchten bekend zijn en onderzocht worden.

Onderwerp	Organisatie
Nationaal Kernteam Crisiscommunicatie	Coördineren van pers- en publiekscommunicatie over het digitaal incident en de zichtbare gevolgen
Hulpverleningsdiensten (politie, brandweer)	Lokale/regionale effecten Handelingsperspectief voor burgers in fysieke ruimte
Burgemeester, voorzitter veiligheidsregio	Handhaving openbare orde en veiligheid Veiligheidsmaatregelen en duiding lokaal/regionaal
Publieke en private partijen	Gevolgen voor eigen organisatie en medewerkers, directe gevolgen voor klanten of leveranciers
NCSC	Duiding, maatregelen en handelingsperspectief
DTC, CERTs en SOC-organisaties	Maatregelen technisch/ operationeel voor de eigen doelgroepen
NCTV, MinJenV als coördinerend minister cybersecurity en verantwoordelijk voor crisisbeheersing	Duiding en attributie van activiteiten en dreigingen door statelijke actoren
Politie/KMAr	Fysieke veiligheidsmaatregelen algemeen
AIVD/MIVD	Duiding activiteiten en dreigingen door statelijke actoren
Openbaar Ministerie, Landelijk Parket	Opsporingsonderzoek (bij opzettelijk handelen)
Betrokken vakminister	Feiten en duiding Handelingsperspectieven nationaal (in afstemming met andere betrokken departementen)

3. Nafase (nazorg en herstel)

De nafase van een (dreigende) digitale crisis brengt verschillende uitdagingen met zich mee. Zo zal het lastig te duiden zijn wanneer een cyberverstoring echt over is; het is wellicht niet helder of systemen weer 'schoon' zijn. Ook is het lastig te bepalen of en wanneer systemen weer naar behoren en verantwoord werken. Dit maakt het in de nafase extra ingewikkeld om te toetsen of alle problemen (en bijbehorende effecten) verholpen zijn en welke kosten gemaakt zijn en te verhalen zijn.

In ieder geval zal er aandacht moeten zijn voor:

- Op landelijk niveau duiden van de maatschappelijke en psychologische impact van het incident.
- Herstel van continuïteit daar waar deze verstoord is geraakt. Herstel kan intensief en langdurig zijn indien er grote schade aan de IT is aangericht of grote delen van systemen vervangen moeten worden. Ook herstel van uitval van vitale processen kan intensief zijn, inclusief schaarste in benodigde expertise of andere middelen.
- Monitoring van de situatie, ontwikkelingen in de dreiging en nieuwe gerelateerde incidenten
- Forensisch en strafrechtelijk onderzoek, om o.a. de dader, toedracht en omvang van de digitale crisis zo accuraat mogelijk te bepalen. Wees bewust dat (technische) forensische expertise veelal privaat ingekocht moet worden. Het is verstandig om vóór een crisis al contact te leggen met security bedrijven die deze dienstverlening aanbieden en hier eventueel contracten mee te sluiten.
- Evaluatie van zowel de (technische) aanpak van de verstoring als de procesmatige aanpak van crisismanagement (kritische processen van crisismanagement).
- Borging van de leerpunten in planvorming (crisisplannen, handreiking en continuïteitsplannen).
- Nazorg voor betrokken personeel. Ondanks dat er geen fysieke slachtoffers zijn kan de impact op eigen personeel groot zijn.
- Forensisch en strafrechtelijk onderzoek, om o.a. de dader en toedracht van de verstoring te bepalen. Wees bewust dat (technische) forensische expertise veelal privaat ingekocht wordt. Het kan nuttig zijn om vóór een crisis al contact te leggen met security bedrijven die deze dienstverlening aanbieden en hier eventueel contracten mee te sluiten.
- Bij een cybercrisis met grote maatschappelijke impact moeten keuzes worden gemaakt in de wijze van organiseren. Mogelijk gaat de nationale crisisorganisatie over in een specifieke crisisorganisatie of een projectorganisatie. Ook daar kan samenwerking tussen verschillende sectoren aan de orde zijn. Dit is onderdeel van de besluitvorming tijdens de crisis.

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).

4. Bouwstenen

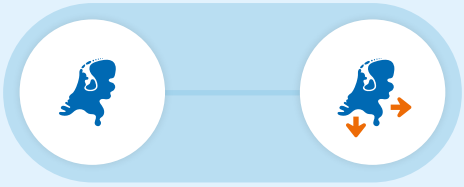
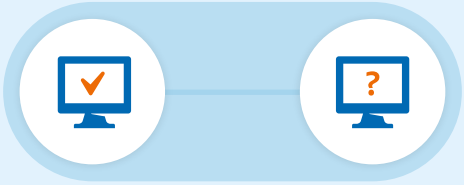
Omdat er talloze situaties denkbaar zijn als het gaat om incidenten en dreigende crises in het digitale domein, zeker in combinatie met een mogelijke doorwerking naar het fysieke domein, is in dit crisisplan gekozen voor een aanpak gebaseerd op bouwstenen. Bij de definiëring van de bouwstenen is geredeneerd vanuit voor de crisisrespons betekenisvolle verschillen. Het gaat om de volgende bouwstenen: oorzaak, bron, actor, geraakt domein, geraakt gebied en technisch oplossingsperspectief. In het volgende hoofdstuk zijn acht mogelijke situaties verder uitgewerkt: 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.

In de praktijk zal veelal een combinatie van verschillende bouwstenen 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 aan de slag kunnen. Door na te gaan welke bouwstenen aan de orde zijn of kunnen zijn, kan zo een inschatting worden gemaakt van de opgave en kunnen keuzes worden gemaakt in wijze van organiseren en de betrokkenheid van partners.

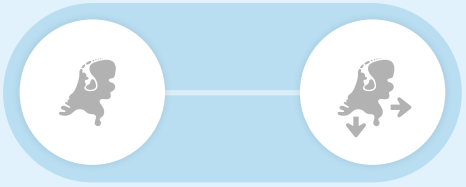
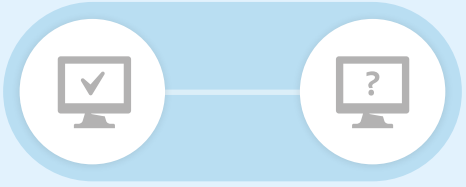
Situational awareness, monitoring en informatievoorziening zijn op 24/7-basis reguliere taken van het NCSC, de NCTV (NCC) en de veiligheidsregio's. Alle organisaties zijn derhalve bij alle situaties betrokken.

Politie, inlichtingen- en veiligheidsdiensten en het OM zijn vanaf het begin betrokken omdat lang onduidelijk kan zijn of de bouwstenen "opzettelijk handelen" en "statelijke actor" van toepassing zijn. Het ministerie van Buitenlandse Zaken en Defensie zijn vanaf het begin betrokken zolang onduidelijk is of de bouwsteen "statelijke actor" van toepassing is. Daarnaast kunnen verschillende ministeries betrokken zijn afhankelijk van de aard van het incident en de daarbij behorende departementale beleidsverantwoordelijkheid.

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 en essentiële diensten
Geraakt gebied		Eén veiligheidsregio	Regio-overstijgende effecten / Effecten in het buitenland
Oplossingperspectief		Technisch oplossings-perspectief aanwezig	Technisch oplossings-perspectief onbekend

Bouwsteenwaarden

Op basis van de gedefinieerde bouwstenen en bouwsteenwaarden kan een situatie worden geschetst. Door na te gaan welke bouwstenen aan de orde zijn of kunnen zijn, kan zo een inschatting worden gemaakt van de opgave en kunnen keuzes worden gemaakt in de wijze van organiseren. Ook kan inzicht worden verkregen in de betrokkenheid van partners.

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 en essentiële diensten
Geraakt gebied	 Eén veiligheidsregio; Regio-overstijgende effecten; Effecten in het buitenland
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, effecten en betrokken partijen

Gevolgen en effecten	Mensen en instanties worden gedupeerd (bijvoorbeeld financieel, chantage, laster, imagoschade)
	Afname vertrouwen aangeboden digitale diensten
	Integriteit van informatie wordt aangetast
	Maatschappelijke onrust, verstoring openbare orde
	Gevolgen, effecten eventueel groter door mogelijkheid nieuw incident, herhaling of onbekendheid aantal betrokkenen
Betrokken partijen	Digitale dienstverleners van de getroffen partijen
	Aanbieders getroffen (vitale) processen
	Toeleveranciers voor en afnemers van de getroffen (vitale) processen
	Security bedrijven
	Schakelorganisaties en sectorale CERTs
	Politie, Koninklijke Marechaussee
	Openbaar Ministerie
	Forensische en onderzoekende partijen
	Ministeries, verantwoordelijk voor getroffen domeinen of partijen
	NCSC en NCTV

In het geval van een vermoeden van een strafbaar feit leidt het OM het onderzoek en geeft de politie daar uitvoering aan.

Het zal doorgaans niet direct duidelijk zijn dat een digitale crisis met opzet is veroorzaakt. Vanuit opsporingsperspectief wordt altijd rekening gehouden met het feit dat er sprake kan zijn van verwijtbaar handelen tot het moment dat dit expliciet wordt uitgesloten. In het kader van incident respons staat het NCSC (doelgroep) organisaties (Rijk, vitaal) bij in het treffen van maatregelen om de continuïteit van de getroffen dienst te herstellen.

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 digitaal incident evident niet-opzettelijk is, kan er toch sprake zijn van strafbare feiten (bijv. door schuld), 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 en essentiële diensten
Geraakt gebied	Eén veiligheidsregio / Regio-overstijgende effecten / Effecten in het buitenland
Oplossingperspectief	Technisch oplossings-perspectief aanwezig / Technisch oplossings-perspectief onbekend

Bron

Technisch falen buiten Nederland

Er is sprake van een incident in Nederland als gevolg van technisch falen buiten Nederland.

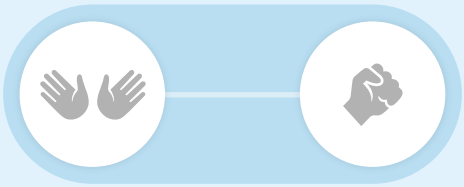
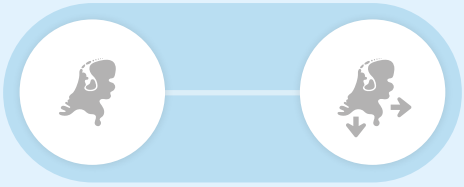
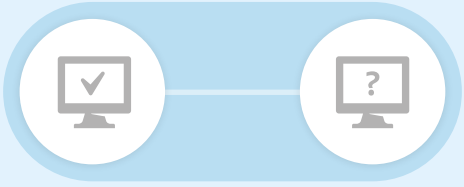
Gevolgen, effecten en betrokken partijen

Gevolgen en effecten	Mogelijke verstoringen van bedrijfsprocessen kunnen in omvang toenemen doordat de bron buiten Nederland ligt.
	Attributie mogelijk lastiger in verband met bron buiten NL.
	Beperkt of weinig invloed vanuit NL op de (technische) oplossing.
Betrokken partijen	Digitale dienstverleners van de getroffen partijen
	Aanbieders getroffen (vitale) processen
	Schakelorganisaties en sectorale CERTs
	Ministerie van Buitenlandse Zaken
	AIVD, MIVD
	NCSC en NCC, o. a. vanwege internationale netwerken
	Andere ministeries, verantwoordelijk voor getroffen domeinen of partijen
	NCTV

De invulling van deze bouwsteen 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 de samenwerking met internationale (cyber) partners en werkt intensief samen met een uitgebreid (inter) nationaal netwerk van computercrisisteams, zoals het Europese CSIRT netwerk, het International Watch and Warning Network (IWWN) en de European Government Cert-Group (EGC). Het NCSC kan, in samenwerking met deze internationale partners, technisch onderzoek verrichten.

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 tegenhangers 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 en essentiële diensten
Geraakt gebied		Eén veiligheidsregio / Regio-overstijgende effecten / Effecten in het buitenland
Oplossingperspectief		Technisch oplossings-perspectief aanwezig / Technisch oplossings-perspectief onbekend

Actor

Statelijke actor

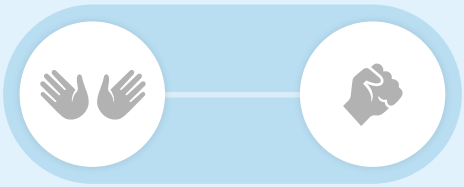
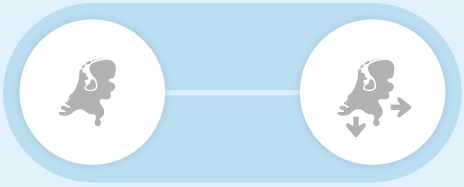
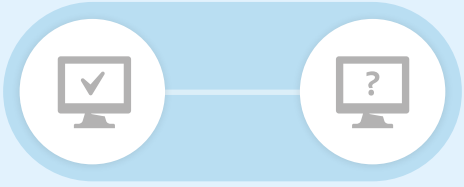
Er is sprake van een incident waarbij een statelijke actor is betrokken. Deze kan diverse doelen hebben: (economische) spionage, (voorbereiding op) sabotage, beïnvloeding als deel van een groter of internationaal conflict, vergelding, enz.

Gevolgen, effecten en betrokken partijen

Gevolgen en effecten	Verstoring (vitale) processen
	Aantasting integriteit (informatie)systemen
	Diplomatieke/internationale onrust
	Maatschappelijke onrust
	Politieke onrust / druk
	Mogelijk meer risico's Nederlandse burgers, bedrijven en instanties in het buitenland
Betrokken partijen	Digitale dienstverleners van de getroffen partijen
	Aanbieders getroffen (vitale) processen
	Schakelorganisaties en sectorale CERTs
	Ministeries van AZ, BZ, BZK, DEF, JenV
	Politie, Koninklijke Marechaussee
	AIVD, MIVD
	NCSC en NCC, o.a. vanwege Internationale netwerken
	Andere ministeries, verantwoordelijk voor getroffen domeinen of partijen
	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.
De meeste uitingen van statelijke actoren zullen echter niet zo snel de grens van een gewapend conflict overschrijden; dan ligt besluitvorming over inzet van de crisisstructuur voor de hand.

Wanneer er een statelijke actor in het spel is hebben de inlichtingen- en veiligheidsdiensten eigenstandige wettelijke taken; de AIVD doet onderzoek naar personen en organisaties die een gevaar vormen voor de gewichtige belangen van de staat, en AIVD en MIVD verrichten onderzoek naar andere landen. Daarnaast veranderen ook de rol en betrokkenheid van Defensie, Buitenlandse Zaken en Algemene Zaken. Operationeel blijft het NCSC ook bij een aanval afkomstig van een statelijke actor haar coördinerende rol met betrekking tot het cyberincident vervullen. Al naar gelang de aard van de aanval, zullen sommige besluiten parallel in verschillende gremia plaatsvinden, zoals afgestemd in de nationale crisisstructuur indien opschaling terzake de casus opportuun is (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 en essentiële diensten
Geraakt gebied		Eén veiligheidsregio / Regio-overstijgende effecten / Effecten in het buitenland
Oplossingperspectief		Technisch oplossings-perspectief aanwezig / Technisch oplossings-perspectief onbekend

Geraakt domein

Maatschappelijk belangrijke voorzieningen (niet-vitaal en geen essentiële dienst)

Er is sprake van een incident waarbij maatschappelijk belangrijke, maar niet-vitale voorzieningen zijn getroffen, zoals openbaar vervoer (inclusief verkeers-signalering), supermarkten, tankstations, scholen, hulpverlening, bedrijven en gemeenten.

Gevolgen, effecten en betrokken partijen

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
Betrokken partijen	Digitale dienstverleners van de getroffen partijen
	Aanbieders getroffen processen
	Toeleveranciers voor en afnemers van de getroffen processen
	Security bedrijven
	Digital Trust Center, schakelorganisaties en sectorale CERTs
	Politie
	Openbaar Ministerie
	Ministeries verantwoordelijk voor getroffen domeinen of partijen
	Veiligheidsregio's, LOCC
	Lokale Driehoek
	Veiligheidsberaad
	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 primair verantwoordelijk voor de continuïteit van hun eigen processen.

Wanneer maatschappelijke onrust/impact en effecten in de fysieke buitenwereld ontstaan kan dit echter wel leiden tot opschaling van crisisstructuren. Onder coördinatie van het NCSC wordt binnen een landelijk dekkend stelsel van cybersecuritysamenwerkingsverbanden, waaronder sectorale CERT's en andere schakelorganisaties, informatie over incidenten en dreigingen gedeeld. Er moet rekening worden gehouden met het cumulatieve effect van verstoringen: wanneer meerdere voorzieningen tegelijk worden getroffen kan dit effect hebben op de mogelijke maatschappelijke ontwrichting wat ertoe zal leiden dat nationale en regionale crisisstructuren sneller zullen anticiperen.

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 en essentiële diensten**
Geraakt gebied	Eén veiligheidsregio / Regio-overstijgende effecten / Effecten in het buitenland
Oplossingperspectief	Technisch oplossings-perspectief aanwezig / Technisch oplossings-perspectief onbekend

Geraakt domein

Vitale processen en essentiële diensten

Er zijn een of meer vitale processen in Nederland getroffen.

Gevolgen, effecten en betrokken partijen

Gevolgen en effecten	Verstoring/uitval essentiële digitale diensten voor de continuïteit van vitale processen
	Mogelijk doorwerking naar niet-vitale voorzieningen in verband met cascade-effecten
	Verstoring bedrijfsprocessen getroffen bedrijven, instanties en organisaties
	Aantasting integriteit (informatie)systemen
	Verstoring openbare orde en veiligheid
	Maatschappelijke onrust
	Politieke onrust/maatschappelijke ontwrichting
	Economische schade
	Reputatieschade en vertrouwensverlies
Betrokken partijen	Digitale dienstverleners van de getroffen partijen
	Aanbieders getroffen vitale processen
	Toeleveranciers voor en afnemers van de getroffen (vitale) processen
	Security-bedrijven
	Politie
	AIVD, MIVD
	Openbaar Ministerie
	Ministeries verantwoordelijk voor getroffen vitale processen
	Veiligheidsregio's, LOCC
	Lokale Driehoek
	Veiligheidsberaad
	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. Bij verstoring of uitval kan het NCSC waar nodig ondersteunen, bijvoorbeeld door het geven van advies, en ten behoeve daarvan technisch onderzoek verrichten.

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 en essentiële diensten
Geraakt gebied	Eén veiligheidsregio / **Regio-overstijgende effecten** / Effecten in het buitenland
Oplossingperspectief	Technisch oplossings-perspectief aanwezig / Technisch oplossings-perspectief onbekend

Geraakt gebied

Regio-overstijgende effecten

Het incident leidt tot gevolgen en effecten in meerdere veiligheidsregio's en/of andere regionaal ingedeelde sectoren of gebieden.

Gevolgen, effecten en betrokken partijen

Gevolgen en effecten	Complexiteit groter vanwege schaarste beschikbare middelen en verschillen tussen regio's
	Verstoring bedrijfsprocessen getroffen bedrijven, instanties en organisaties
	Aantasting integriteit (informatie)systemen
	Verstoring openbare orde en veiligheid
	Maatschappelijke onrust (in plaats van kans op maatschappelijke onrust)
	Politieke onrust/maatschappelijke ontwrichting
	Economische schade
	Reputatieschade en vertrouwensverlies
Betrokken partijen	Digitale dienstverleners van de getroffen partijen
	Aanbieders getroffen (vitale) processen
	Toeleveranciers voor en afnemers van de getroffen (vitale) processen
	Sectorale CERT's
	Security-bedrijven
	Politie
	Openbaar Ministerie
	Ministeries, verantwoordelijk voor getroffen domeinen of partijen
	Veiligheidsregio's, LOCC
	Lokale Driehoek
	Veiligheidsberaad
	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 en essentiële diensten
Geraakt gebied	Eén veiligheidsregio / Regio-overstijgende effecten / **Effecten in het buitenland**
Oplossingperspectief	Technisch oplossings-perspectief aanwezig / Technisch oplossings-perspectief onbekend

Geraakt gebied

Effecten in het buitenland

Er is sprake van een incident in Nederland met effecten in het buitenland.

Gevolgen, effecten en betrokken partijen

Gevolgen en effecten	Reputatieschade Nederland
	Internationale druk op Nederland
	Verstoring bedrijfsprocessen getroffen bedrijven, instanties en organisaties
	Aantasting integriteit (informatie)systemen
	Verstoring openbare orde en veiligheid
	Politieke onrust
	Economische schade
Betrokken partijen	Digitale dienstverleners van de getroffen partijen
	Aanbieders getroffen (vitale) processen
	Toeleveranciers voor en afnemers van de getroffen (vitale) processen
	Security-bedrijven
	Internationale netwerken
	Openbaar Ministerie
	AIVD, MIVD
	NCSC en NCC, o.a. als nationaal contactpunt van NL
	Ministeries van AZ, BZ, DEF, JenV en evt. andere ministeries verantwoordelijk voor getroffen domeinen of partijen
	NCTV

In deze bouwsteen 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 de bouwsteen ‘bron buiten Nederland’). Het verschil zit hem in het feit dat in deze bouwsteen 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. Het NCSC verricht voor zover mogelijk technisch onderzoek naar het incident en zal relevante technische informatie zo veel als mogelijk delen binnen haar uitgebreide netwerk van internationale computercrisisteams.

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 en essentiële diensten
Geraakt gebied	Eén veiligheidsregio	Regio-overstijgende effecten	Effecten in het buitenland
Oplossingperspectief	Technisch oplossings-perspectief aanwezig	**Technisch oplossings-perspectief onbekend**	

Oplossingperspectief

Technisch oplossingsperspectief langdurig onbekend

Er is sprake van een incident waar bij een technisch oplossingsperspectief langdurig onbekend is en de respons zich vooral op het mitigeren van effecten richt.

Gevolgen, effecten en betrokken partijen

Gevolgen en effecten	Maatschappelijke onrust gevoed door ontbreken (zicht op) oplossing
	Onzekerheid Verschuiving van respons naar ‘ermee omgaan’
	Verstoring bedrijfsprocessen getroffen bedrijven, instanties en organisaties
	Aantasting integriteit (informatie)systemen
	Verstoring openbare orde en veiligheid
	Politieke onrust
	Economische schade
Betrokken partijen	Digitale dienstverleners van de getroffen partijen
	Aanbieders getroffen (vitale) processen
	Toeleveranciers voor en afnemers van de getroffen processen
	Security bedrijven
	Veiligheidsregio's, LOCC
	Ministeries verantwoordelijk voor getroffen domeinen of partijen
	NCSC en NCTV

Het NCSC zal in samenwerking met zijn nationale en internationale partners aanjagen dat technisch oplossingsperspectief zo snel mogelijk beschikbaar komt. Ook kan het NCSC (doelgroep) organisaties (Rijk, vitaal) adviseren over handelingsperspectief of mitigerende maatregelen.

Op de meldkamer van van politie en brandweer in Nijmegen komen alle noodmeldingen uit de regio binnen.

5. Verantwoordelijkheden (wet- en regelgeving)

In samenspraak met de betrokken departementen zijn de belangrijkste huidige wettelijke taken en bevoegdheden in kaart gebracht die het mogelijk maken informatie te delen met of in het uiterste geval in te grijpen op de digitale weerbaarheid bij de Rijksoverheid, vitale aanbieders en niet-vitale organisaties. Dit overzicht is op 3 februari 2020 aan de Kamer aangeboden.[14] Hieronder wordt kort ingegaan op de Wet beveiliging netwerk- en informatiesystemen en de Telecommunicatiewet.

Wet beveiliging netwerk- en informatiesystemen

De Wet beveiliging netwerk- en informatiesystemen (Wbni) streeft ernaar digitale weerbaarheid van vitale aanbieders, de Rijksoverheid en digitale dienstverleners te vergroten. De Wbni regelt voor verschillende van deze organisaties een meldplicht van incidenten met aanzienlijke gevolgen voor de continuïteit van de dienstverlening 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.

Alle vitale aanbieders en onderdelen van de Rijksoverheid hebben op grond van de Wbni recht op informatie, adviezen en overige bijstand van het Nationaal Cyber Security Centrum (NCSC) waarmee zij de continuïteit van de door hen geleverde diensten kunnen borgen.

Naast het recht op bijstand hebben de meeste vitale aanbieders 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 en het NCSC. 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 die de beveiliging aantasten van de voor de verlening van de dienst gebruikte netwerk- en informatiesystemen te voorkomen én de gevolgen van dergelijke incidenten zo veel mogelijk te beperken. De verschillende sectorale toezichthouders houden toezicht op de naleving van deze verplichtingen door AED's. De zorgplicht is nader uitgewerkt in het Besluit beveiliging netwerk- en informatiesystemen (Bbni).[15]

14. Te downloaden via: https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/tk-bijlage-overzicht-wet-en-regelgeving-cybersecurity
15. 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.

2. AAVA's zijn vitale aanbieders die niet actief zijn in sectoren, bedoeld in de bijlage bij de Europese Netwerk en Informatie Beveiliging (NIB) richtlijn maar die wel in Nederland vitaal worden geacht en als andere vitale aanbieders zijn aangewezen in het Bbni. Deze partijen hebben de plicht om incidenten met aanzienlijke gevolgen voor de continuïteit van hun dienst te melden bij het NCSC.

Als AED's bijvoorbeeld de zorgplicht onvoldoende naleven kan een toezichthouder ingrijpen door middel van bijvoorbeeld bestuursdwang of boetes.

Telecommunicatiewet

De voor dit plan belangrijkste wettelijke bepalingen ten aanzien van telecommunicatie zijn opgenomen in de hoofdstukken 11a, 14 en 18.

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 wordt 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, namelijk:

- 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 (bijvoorbeeld in- of uitschakelen van zenders of straalverbindingen); en
- het zo goed mogelijk waarborgen van de bereikbaarheid van het alarmnummer 112 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 Nationaal Continuïteitsoverleg Telecommunicatie (NCO-T) is een overleg dat hieronder valt;
- implementeren van continuïteitsplanning en crisismanagement; en
- 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 aanbieders van de betrokken vitale processen 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).

De ECT terminal voor containeroverslag op de Maasvlakte werkt volledig geautomatiseerd.

Bijlagen

1. **Departementale taken en verantwoordelijkheden en overige relevante organisaties**
2. **Relevante bronnen en literatuur**
3. **Afkortingen**

Bijlage 1

Departementale taken en verantwoordelijkheden en overige relevante organisaties

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Departementale CIO's, CISO's, CIO Rijk en CISO Rijk

Onder coördinatie van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties hebben departementale CIO's en CIO Rijk op grond van het besluit CIO Stelsel een belangrijke rol op het gebied van informatiebeveiliging. De departementale CISO kan namens de secretaris-generaal en de departementale CIO en in afstemming met de beveiligingsautoriteit van het ministerie aanwijzingen geven aan iedere ambtenaar, externe medewerkers en bezoekers, voor zover dat noodzakelijk is voor de uitvoering van het departementale informatiebeveiligingsbeleid en de naleving van de informatiebeveiligingsvoorschriften. De CISO Rijk heeft een interdepartementale coördinatierol bij Rijksbrede informatiebeveiligingsincidenten en -calamiteiten.

De CISO Rijk kan, na afstemming met de betreffende departementale CISO, in het geval van een, mogelijke, ernstige, acute, departement-overstijgende inbreuk op de beveiliging van informatiesystemen of een risico daarop, namens de secretaris-generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onder meer aanwijzingen geven en maatregelen (laten) treffen. De CISO Rijk stemt onverwijld af met de CIO Rijk, de beveiligingsautoriteit Rijk en betrokken departementen over een (mogelijke) inbreuk of het risico daarop en de genomen maatregelen en heeft daarbij in afstemming met de departementale CISO's indien nodig direct toegang tot de secretaris-generaal van ministeries.

DG Digitalisering en Overheidsorganisaties (DGDOO) en directie Digitale Samenleving

Het DG Digitalisering en Overheidsorganisaties (DGDOO, waar de directies CIO Rijk en Digitale Samenleving onderdeel van zijn) fungeert bij een (dreigende) crisis als aanspreekpunt voor overheidsorganisaties ten aanzien van onderwerpen die binnen haar beleidsverantwoordelijkheid vallen (o.a. informatisering en ICT Rijk, digitale overheid en digitale samenleving). DGDOO draagt bij aan het situationele beeld van de overheid, in afstemming met crisispartners zoals het NCSC en de IBD. DGDOO verzorgt onder meer de communicatie richting stakeholders en de bewindspersoon BZK als stelselverantwoordelijke voor digitalisering.

In geval van een (dreigende) overheidsbrede crisis staat de directie Digitale Samenleving in nauw contact met de verschillende Computer Emergency Response Teams (CERT's)/informatieknooppunten van de medeoverheden te weten: de gemeenten, provincies en waterschappen.

Algemene Inlichtingen- en Veiligheidsdienst

De AIVD verricht onderzoek naar digitale aanvallen die een potentiële bedreiging vormen voor de nationale veiligheid, bijvoorbeeld wanneer de betrokkenheid van een statelijke actor wordt vermoed. Hierdoor kan de AIVD dergelijke aanvallen detecteren en mitigeren, slachtoffers informeren en bewustwordingspresentaties geven aan mogelijke doelwitten. Dat doet de dienst in direct contact met slachtoffer- en doelwitorganisaties, maar ook in samenwerking en afstemming met het NCSC, de CIIC-deelnemers en andere partijen binnen de Rijksoverheid. Daarnaast is een belangrijke taak voor de AIVD om beleidsmedewerkers en bestuurders te informeren, zodat zij in staat gesteld worden tot het voeren van effectief digitaal veiligheidsbeleid. Daarnaast verstrekt de AIVD informatiebeveiligingsadviezen op maat, gericht op statelijke actoren, aan de Rijksoverheid en andere belanghebbenden, zoals vitale bedrijven. Het doel van deze

adviezen is de weerstand tegen digitale aanvallen van statelijke actoren te verhogen en (digitale) schade te beperken of te voorkomen. Hierbij werkt de AIVD nauw samen met het NCSC. 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 hierop aangesloten organisaties binnen hun eigen verantwoordelijkheden maatregelen kunnen treffen.

Ministerie van Buitenlandse Zaken

De minister van Buitenlandse Zaken is verantwoordelijk voor de diplomatieke en politieke respons op cyberaanvallen en coördineert voor Nederland de diplomatieke en politieke respons in like-minded-, EU-, OVSE- en NAVO-verband. Ook de attributie van cyberaanvallen wordt door Buitenlandse Zaken gecoördineerd, in afstemming met betrokken binnenlandse en buitenlandse partners.

Daarnaast hebben het ministerie van Buitenlandse Zaken en de ambassades in bijzonder een belangrijke monitorings- 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

In de Catalogus Nationale Operaties zijn verschillende Defensiecapaciteiten 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.

In het geval van opschaling van de nationale crisisstructuur neemt in principe de Bestuursstaf deel aan het IAO. De SG neemt in principe deel aan de ICCb ter voorbereiding op de MCCb. De SG, CDS, DGB of DJZ adviseren de minister voor diens inbreng in de MCCb.

Het **Defensie Cyber Security Centrum** (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 Rijksbreed verband mitigeren van cyberdreigingen.

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. Ook is het DCSC lid van het EU PESCO-project Cyber Rapid Response Teams. Met het NCSC zijn via het NRN 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.

Het **Defensie Cybercommando** (DCC) is verantwoordelijk voor de ontwikkeling en inzet van militaire slagkracht in het cyberdomein. De digitale slagkracht bestaat uit een eigen operationele capaciteit en een kennisinstituut (Cyber Warfare en Trainingscentrum). Daarnaast beschikt het DCC over een groot aantal cyberreservisten die kunnen worden opgeroepen als de nood hoog is. Het DCC kan bij cyberincidenten desgevraagd militaire bijstand leveren aan civiele autoriteiten. Met zijn offensieve cybercapaciteit kan het DCC in het uiterste geval een cyberaanval uitvoeren. 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 kennis- en ervaringsuitwisseling.

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.

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 statelijke actoren detecteren en mitigeren en (potentiële) slachtoffers informeren. Hierbij wordt nauw samengewerkt met het NCSC. Tevens worden bewustwordingspresentaties gegeven 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.

NAVO

Omdat civiele en militaire netwerken en systemen in het cyberdomein nauw met elkaar verweven zijn, is er een kans dat de NAVO bij een eventuele cybercrisis betrokken raakt. In dit geval kan op diverse manieren met en via de NAVO worden samengewerkt. Het NATO Cyber Security Center (NCSC) is verantwoordelijk de beveiliging van NAVO-netwerken. Bondgenoten en diverse NAVO-onderdelen delen via de NAVO ook dreigingsinformatie en andere inlichtingen, bijvoorbeeld via het NAVO MISP. Via de NAVO kan desgewenst ook assistentie van bondgenoten gevraagd worden in de vorm van NAVO Rapid Response Teams. Ook biedt de NAVO diverse platformen voor operationele samenwerking tussen publieke en private partijen. Het DCSC en de MIVD zijn hierin vertegenwoordigd.

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 digitale 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 minister draagt géén operationele verantwoordelijkheid. Onder buitengewone omstandigheden kan de minister 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; en
- maatregelen treft 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. Dit zijn verplichtingen op het gebied van continuïteitsplanning en crisismanagement.

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. Vertrouwensdiensten worden aangeboden door commerciële partijen maar ook gebruikt binnen de overheid zelf. Zij behoren tot de vitale infrastructuur Telecom.

Daarnaast is EZK ook beleidsverantwoordelijk voor de sector Energie. Krachtens de Wbni zijn aanbieders van essentiële diensten (AED's) aangewezen in de sub sectoren elektriciteit, gas en olie. Er geldt voor AED's een meld- en zorgplicht betreffende cybersecurity. Agentschap Telecom houdt namens EZK toezicht op de naleving van de zorgplicht bij deze AED's. Daarnaast zijn er ook sectorale wetgevingen in de maak waarbij kritieke entiteiten binnen de energiesector aanvullende eisen voor cybersecurity en crisismanagement opgelegd krijgen.

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 o.a.:

- het 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, onderdeel van het ministerie van Justitie en Veiligheid, is opdrachtgever van het NCSC dat als uitvoeringsorganisatie ook 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 strafbare feiten te voorkomen of doen stoppen door middel van het strafrecht of door het laten treffen van maatregelen in het kader van bewaken en beveiligen; en
- de rechtsorde strafrechtelijk handhaaft door het leiden van opsporingsonderzoeken en de vervolging van (rechts)personen voor strafbare feiten, en daarbij ook alternatieve interventiemethoden gebruikt zoals het notificeren van slachtoffers, het verstoren van criminele activiteiten of het voorkomen van nieuw

slachtoffer- of daderschap. Het OM werkt daarbij nauw samen met internationale en private partners.

Politie

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. 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 verantwoordelijk voor het technisch beheer van de 112-meldkamers.

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; en
- 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, ook krachtens de Wbni, en bevordert onder meer de goede werking van het betalingsverkeer. DNB is de voorzitter van het TCO.

Ministerie van Infrastructuur en Waterstaat

Het ministerie van Infrastructuur en Waterstaat (IenW) is beleidsverantwoordelijk voor een groot aantal sectoren die belangrijk zijn voor een veilig, bereikbaar en leefbaar Nederland. Binnen deze sectoren zijn er op dit moment negen vitale processen geïdentificeerd. Daarbinnen zijn de volgende aanbieders van een essentiële dienst (AEDs) krachtens de Wbni aangewezen:

- 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.
- Voor spoorvervoer: aangewezen infrastructuurbeheerders en spoorwegondernemingen.
- Voor wegvervoer: aangewezen wegenautoriteiten en exploitanten van intelligente vervoerssystemen.
- Voor drinkwater: de drinkwaterbedrijven.

Binnen de sector nucleair en de sector keren en beheren zijn ook nog andere vitale aanbieders krachtens de Wbni als zodanig (AAVA's) aangewezen.

Voor de Wbni heeft de minister IenW de Inspectie voor de Leefomgeving en Transport (ILT) als toezichthouder aangewezen op de naleving van de verplichtingen in de Wbni door AED's. Het piketnummer van het Departementaal Coördinatiecentrum Crisisbeheersing IenW (DCC-IenW) doet dienst als 24/7 Wbni meldpunt voor de ILT.

Bij de uitvoeringsorganisatie Rijkswaterstaat (RWS) is voor de drie netwerken Hoofdwatersysteem, Hoofdwegennet én Hoofdvaarwegennet een Security Centre operationeel. Het Security Centre heeft een breed takenpakket, waaronder het adviseren van projecten om de juiste beveiligingseisen te implementeren, het ontwikkelen van cybersecurity standaarden voor de gehele sector (voornamelijk op IA gebied) en het actief monitoren van de netwerken van RWS. Dit gebeurt zowel voor de Industriële Automatisering als voor de kantooromgeving. Het Security Centre werkt dagelijks samen met andere overheidsorganisaties, zoals het NCSC, Joint-SOC (J-SOC, samenwerking van SOC RWS, de Belastingdienst, SSC-ICT, DICTU, DUO en JenV), de AIVD en waterschappen. Tevens is Rijkswaterstaat onderdeel van het Nationaal Respons Netwerk (NRN). Vanuit het SOC RWS kan worden opgeschaald naar een hoger niveau wanneer de situatie complexer wordt en crisisbesluitvorming op een hoger niveau noodzakelijk is. Indien de digitale verstoring fysieke effecten heeft op het netwerk van RWS, kan worden opgeschaald naar de landelijke crisisorganisatie van Rijkswaterstaat.

Overige relevante organisaties in het cyberstelsel

De **Cyber Security Raad** (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De CSR adviseert het kabinet over de uitvoering van de cybersecuritystrategie.

Bijlage 2

Relevante bronnen en literatuur

Agenda en slotbrief Risico- en Crisisbeheersing 2018-2021, TK-brief 12 november 2018 en 30 april 2020.

Algemene Rekenkamer, Digitale dijkverzwaring: cybersecurity en vitale waterwerken, 2019 en reactie minister Infrastructuur en Waterstaat, 25 februari 2019.

W. Bantema e.a., Burgemeesters in cyberspace, 2018.

Cybersecuritybeeld Nederland, 2022.

Defensie Cyber Strategie 2018.

M. van Eeten, Blussen met nullen en enen (Van Slingerlandtlezing 31 oktober 2019).

Evaluatie ISIDOOR 2021.

Inspectie JenV, Evaluatie rijkscrisisorganisatie tijdens de DigiNotar-crisis, juli 2012.

Instellingsbesluit Ministeriële Commissie Crisisbeheersing 2022.

IFV, Bestuurlijke Netwerkkaarten Crisisbeheersing en bijbehorende bevoegdhedenschema's.

IFV, Crisiscommunicatietips voor incidenten met een cybercomponent (digitale verstoring), april 2022.

IFV, Crisiscommunicatietips voor uitval van vitale voorzieningen, december 2018.

IFV, Verbinden van werelden? Een analyse van de aanpak van zeven bovenregionale crisistypen, Arnhem 2019.

NIPV, Cyber scenario's voor veiligheidsregio's, 2021.

NIPV Bestuurlijke bevoegdheden cyber. Verkenning van bevoegdheden en overige interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio's bij (dreigende) digitale incidenten, 2022.

Landelijk convenant voor samenwerkingsafspraken tussen Veiligheidsregio's, Politie en Telecom.

H. Modderkolk, Het is oorlog, maar niemand die het ziet, 2019.

Nationaal Handboek Crisisbeheersing 2022.

Nationale Veiligheid Strategie 2019.

Nederlandse Cyber Strategie 2022-2028

OVV, Kwetsbaar door software. Lessen naar aanleiding van beveiligingslekken door software van Citrix, 2021.

Recommendation EU on coordinated response to large-scale cyber security incidents and crises, 13 September 2017 (L239/36).

RIVM, Rijksbrede risicoanalyse Nationale Veiligheid, 2022.

RIVM, Themarapportages cyberdreigingen, 2022.

Veiligheidsberaad, Bestuurlijk routeboek digitale ontwrichting 2019.

WRR, Voorbereiden op digitale ontwrichting, 2019 en kabinetsreactie 2021.

Handreiking Cybergevolgbestrijding (CGB) G4-gemeenten 2020.

Bijlage 3

Afkortingen

AED	Aanbieder van Essentiële Diensten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CERT	Computer Emergency Response Team
CSIRT	Cyber Security and Incident Response Team
DCC	Defensie Cyber Commando / Departementaal Crisiscoördinatiecentrum
DOCB	Directeurenoverleg Crisisbeheersing
DTC	Digital Trust Center
EGC	European Government CERT's group
ENISA	European Network & Information Security Agency
EU CyCLONe	European Union Cyber Crises Liaison Organisation Network
EU CSIRT's Network	European Union Cyber Security Incident Response Teams Network
EZK	Ministerie van Economische Zaken en Klimaat
FIRST	Forum of Incident Response and Security Teams
ICCb	Interdepartementale Commissie Crisisbeheersing
IAO	Interdepartementaal Afstemmingsoverleg
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
NCSC	Nationaal Cyber Security Centrum
NLCS	Nederlandse Cybersecurity Strategie 2022-2028
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NCV	Noodcommunicatievoorziening
NHC	Nationaal Handboek Crisisbeheersing
NKC	Nationaal Kernteam Crisiscommunicatie
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
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

December 2022