Nationaal Crisisplan ICT

Status: definitief
Datum: 7 september 2012
Versie: 2.0

Inhoudsopgave

Hoofdstuk 1 Inleiding

ICT is niet meer weg te denken in onze hedendaagse samenleving. Dagelijks neemt het gebruik van ICT toe en vrijwel alle vitale processen zijn hiervan direct afhankelijk. Naast alle mogelijkheden en kansen die dat biedt, neemt eveneens onze afhankelijkheid van goed en betrouwbaar werkende ICT toe. Ook lijkt ons vermogen om gebruik te maken van alternatieven die niet op ICT steunen af te nemen. Hierbij kan gedacht worden aan de afname van het contant geld, het verdwijnen van de vaste analoge telefoon en de telefooncel en de afschaffing van de strippenkaart. Daarnaast nemen de digitale toepassing toe zoals de invoering van cell broadcast voor de alarmering van de burger en de opkomst van cloudcomputing waarbij de applicatie niet meer lokaal functioneert, maar centraal, evenals de opslag van data.

Gelukkig wordt er veel gedaan om de weerbaarheid van ICT te verhogen. De aanleg van back-upsystemen, bevordering van de bewustwording bij eindgebruikers ten aanzien van de beveiliging van systemen en een actieve aanpak en verbetering van systemen om de gevoeligheid voor verstoring en uitval te verminderen zijn enkele voorbeelden.

Maar wat als er toch een ontwrichtende verstoring of uitval optreedt? Het doel van het Nationaal Crisisplan ICT (NCP-ICT) is het waarborgen dat tijdens een ICT-crisis zo veel als mogelijk wordt gewerkt volgens de generieke crisisstructuur aangevuld met de noodzakelijke specifieke kennis en expertise om een ICT-crisis te beheersen. Het ICT-crisisplan beoogt steun te bieden aan publieke organisaties die betrokken zijn bij een ICT-crisis in de voorbereiding op en tijdens de situatie waarbij een maatschappelijke ontwrichting dreigt of plaatsvindt als gevolg van een ICT-verstoring of –uitval. Het crisisplan draagt bij aan een effectieve crisisbestrijding.

Het uitgangspunt voor crisisbeheersing op nationaal niveau is het Nationaal Handboek Crisisbesluitvorming. Het NCP-ICT bouwt voort op dit generieke handboek. Er wordt ingegaan op de specifieke aspecten die bij crisisbeheersing van een ICT-crisis een rol spelen.

Scope van het NCP-ICT
De doelgroep van het NCP-ICT zijn publieke organisaties op nationaal niveau die een rol hebben bij een ICT-crisis. Dit zijn onder andere de crisisbeleidsadviseurs van alle ministeries, maar ook ICT-specifieke organisaties bij de Rijksoverheid zoals het Nationaal Cyber Security Centrum (NCSC).

Het functioneren van de departementen, de uitvoeringsdiensten, veiligheidsregio's en gemeenten onder de omstandigheid van een grootschalige ICT-verstoring kan negatief worden beïnvloed. Mogelijk kan bepaalde dienstverlening niet meer plaatsvinden of zullen prioriteiten moeten worden gesteld om bepaalde dienstverlening op gang te houden. De preparatie op een dergelijke uitval moet geborgd zijn in continuïteitsplannen en valt buiten het NCP-ICT.

Naast het beschrijven van de processen bij een ICT-crisis, is het beoefenen van de procedures een belangrijk middel om goed voorbereid te zijn. Apart van het NCP-ICT zal een oefenbeleid en daaraan gekoppelde planning voor nationale en internationale oefeningen worden uitgewerkt voor dit type crisis. Dit specifieke crisisplan zal dan gebruikt worden als hulpmiddel voor een oefening en een aanzet vormen voor departementale plannen en lokale plannen.

Definitie van ICT
ICT is het geheel aan digitale informatie, informatie-infrastructuren, computers, systemen, toepassingen en de interactie tussen informatietechnologie en de fysieke wereld waarover communicatie en informatie-uitwisseling plaatsvindt. Het is dus meer dan alleen het internet, meer dan alleen de infrastructuren.[1] Het gaat ook om toepassingen en diensten en over de informatie die over deze systemen wordt verzonden en opgeslagen.

[1] Uit de Nationale Cyber Security Strategie.

Definitie van een ICT-crisis
Onder een ICT-crisis wordt verstaan een dreiging of crisis waarbij de bron ligt in het ICT-domein, waarbij één of meer vitale belangen in het geding zijn en waarvoor de reguliere structuren niet toereikend zijn.[2]

Een ICT-crisis kan voortkomen uit moedwillig en niet-moedwillig handelen. Bij moedwillig handelen kan het verstoren van de ICT als middel worden gebruikt om vitale belangen te schaden. Beide oorzaken van een ICT-crisis vallen binnen de scope van dit crisisplan.

De effectbestrijding van een ICT-crisis zal grotendeels overeenkomen bij zowel moedwillig als niet-moedwillig handelen. Moedwillige verstoring kent echter een opsporingscomponent, waardoor in de bronbestrijding andere actoren actief zullen zijn dan bij niet-moedwillige verstoring.

Wat onderscheidt ICT-crisis van veel andere crisistypes?

- De snelheid waarmee een ICT-crisis zich manifesteert. Een ICT-crisis kan van het één op het andere moment gebeuren (aan/uit) of zich eerst als een veenbrand ontwikkelen met een scala aan incidenten waarbij de som der delen zich optellen tot een ICT-crisis. Een extra toevoeging is dat het herstel van de ICT-crisis even plotseling kan optreden als de uitval;
- Uitval van ICT kan gevolgen hebben voor alle vitale sectoren en kan leiden tot maatschappelijke ontwrichting als de uitval meerdere dagen tot een week aanhoudt;
- De crisisorganisaties worden zelf mogelijk ook zwaar geraakt in hun functioneren door uitval of een beperkte beschikbaarheid van de eigen ICT-middelen met een direct effect op interne en externe communicatie (waaronder telefonie);
- Bij de bronbestrijding tijdens een ICT-crisis is de overheid deels afhankelijk van het handelen van private partijen. Vrijwel alle ICT-infrastructuur en diensten zijn in Nederland (en in de rest van de wereld) in handen van private partijen.
- Het is aannemelijk dat de crisis een internationaal karakter heeft, waarbij de oorzaak van de grootschalige verstoring in het buitenland kan liggen, in meerdere landen tegelijkertijd kan optreden, of waarbij de oorzaak mogelijk (mede) in Nederland ligt.
- Er bestaat mogelijk een tekort aan deskundigen die aan bron- en effectbestrijding kunnen doen.

Beheer van het NCP-ICT
Het ICT-domein is bij uitstek een terrein dat zich in hoog tempo ontwikkelt. Het NCP-ICT zal regelmatig geactualiseerd moeten worden. Het Nationaal CrisisCentrum (NCC) zal i.s.m. het ministerie van Economische Zaken, Landbouw & Innovatie (EL&I) en het NCSC jaarlijks bezien in hoeverre het crisisplan actueel is en of aanpassing nodig is. Gezien de ontwikkelingen op het gebied van cyber security is een update in 2013 noodzakelijk.

[2] Gebaseerd op de definitie van een crisis in het Nationaal Handboek Crisisbesluitvorming

Hoofdstuk 2 Wet- en regelgeving en verantwoordelijkheden

Relevante wet- en regelgeving wordt, in dit hoofdstuk beschreven.[3]

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

Hoofdstuk 11a:
In algemene zin hebben aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten de plicht passende technische en organisatorische maatregelen te nemen om de risico's voor de veiligheid en de integriteit van hun netwerken en diensten te beheersen.
Daarnaast moeten zij alle noodzakelijke maatregelen nemen om de beschikbaarheid van de openbare telefoondiensten over de openbare elektronische communicatienetwerken zo volledig mogelijk te waarborgen in geval van een technische storing of uitval van het elektriciteitsnetwerk.
Verder zijn aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten verplicht de minister onverwijld in kennis te stellen van een inbreuk op de veiligheid, of een verlies van integriteit, waardoor de continuïteit van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten in belangrijke mate werd onderbroken.

Hoofdstuk 14:
De Minister van Economische Zaken, Landbouw en Innovatie heeft de volgende taken en bevoegdheden:

- Tijdens een crisis of incident, waarbij geen buitengewone omstandigheden zijn afgekondigd, kan de minister van EL&I in overleg treden met de sector, dat wil zeggen, via het Nationaal Continuïteitsoverleg Telecommunicatie (NCO-T). De als lid daarvan aangewezen bedrijven kunnen verzocht worden mee te werken aan eventuele responsacties.
- Als er wel buitengewone omstandigheden zijn afgekondigd, kan de minister van EL&I handelen conform Telecommunicatiewet, hoofdstuk 14.

Volgens Hoofdstuk 14 van de Telecommunicatiewet kan de Minister van EL&I aanbieders van openbare telecommunicatiediensten en -infrastructuur selecteren die de volgende verplichtingen opgelegd krijgen:
- Ten behoeve van de voorbereiding op buitengewone omstandigheden zijn zij verplicht voorbereidingen te treffen om aanwijzingen tijdens buitengewone omstandigheden te kunnen uitvoeren.

Deze voorbereidingen liggen op het vlak van:
- deelname aan overleggen[4] en/of oefeningen;
- implementeren van continuïteitsplanning en crisismanagement;
- rapportage over de voorbereidingen.

De aanwijzingen die kunnen volgen liggen op het vlak van:
- de instandhouding en exploitatie van openbare telecommunicatienetwerken en -diensten, hieronder vallen bijvoorbeeld prioritering of juist beperking van communicatie; het evt.

[3] Door de Minister van Veiligheid & Justitie zal in 2012 een wettelijke regeling worden opgesteld waarbij randvoorwaardelijke sectoren (elektriciteit, gas, drinkwater, Telecom, keren en beheren oppervlaktewater en transport: de mainports Rotterdam en Schiphol), alsook de financiële sector en de overheid ertoe verplicht zijn om binnen de scope van de meldplicht melding te doen van security breaches aan de sectorale toezichthouder, dan wel het NCSC. In geval van melding aan de sectorale toezichthouder strekt deze regeling tevens tot het doorgeleiden van de melding aan de toezichthouder, naar het NCSC.
[4] Het NCO-T is een overleg dat onder deze verplichte voorbereiding valt.

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

Rijksbrede verantwoordelijkheden
Voor alle andere sectoren die hierboven niet beschreven zijn geldt dat de betreffende ministeries politiek verantwoordelijk zijn en blijven voor de continuïteit van die sectoren. Dit geldt dus ook voor verlies of verstoring van de vitale diensten van die sectoren als gevolg van een cyber gerelateerde oorzaak.

Hoofdstuk 3 Systeembeschrijving

In dit hoofdstuk worden de actoren geduid die de crisisbeheersing voor ICT-crisis (mede) vormgeven. In dit overzicht wordt kort ingegaan op de partijen die betrokken zijn bij ICT-crises. Partijen die reeds zijn opgenomen in de generieke crisisstructuur, worden hier niet meegenomen.

Voor dit hoofdstuk is een onderscheid gemaakt tussen organisaties, gremia en internationale samenwerkingen. De eerste groep zijn direct betrokken bij de crisisstructuur ten tijde van een ICT-crisis. In paragraaf 3.2 zijn gremia opgenomen die een informele, doch belangrijke, rol spelen in de crisisstructuur bij een ICT-crisis. In paragraaf 3.3 zijn de internationale samenwerkingsverbanden benoemd, voor zover die niet eerder zijn genoemd.

3.1 Organisaties

Ministerie van Veiligheid en Justitie (VenJ)
De Minister van Veiligheid en Justitie is coördinerend minister voor crisisbeheersing en cyber security op nationaal niveau. Het ministerie is daarnaast functioneel verantwoordelijk voor opsporing en rechtshandhaving (hieronder valt ook cybercrime). Crisisbesluitvorming op nationaal niveau wordt gefaciliteerd door het Nationaal CrisisCentrum (NCC) op basis van het Nationaal Handboek Crisisbesluitvorming.

Nationaal Cyber Security Centrum (NCSC)
De Nationale Cyber Security Strategie (NCSS), gepresenteerd in februari 2011, heeft voorzien in de oprichting van de Cyber Security Raad (CSR) en het Nationaal Cyber Security Centrum (NCSC). Het NCSC is een onderdeel van het Ministerie van Veiligheid en Justitie en daarbinnen van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), Directie Cyber Security (DCS). Zowel de CSR als het NCSC zijn publiek-privaat van karakter.

Het NCSC heeft de taak om de digitale weerbaarheid van de Nederlandse samenleving te vergroten. Dit doet het NCSC door het ontwikkelen van inzicht in onder andere cybertrends, dreigingen, incidenten, kwetsbaarheden en risico's. Daarnaast het bieden van een handelingsperspectief wanneer zich een dreiging, incident of crisis voordoet. Het NCSC is een samenwerkingsplatform (fysiek en virtueel) waar de voornaamste publieke en private partners (inclusief wetenschaps- en onderzoeksinstellingen) op het terrein van cyber security worden samengebracht en waar het delen van operationele kennis en informatie op een effectieve en betrouwbare wijze wordt gefaciliteerd. Momenteel nemen als liaison (samenwerkingspartner) deel aan het NCSC: AIVD, Defensie, KLPD, OM, NFI en OPTA. In de loop van 2012 en 2013 wordt dit uitgebreid naar meer partners.

Het NCSC wil de digitale weerbaarheid van de Nederlandse samenleving vergroten door de ontwikkeling van inzicht en het bieden van handelingsperspectieven. Op basis hiervan kan zij:
1. expertise en advies geven,
2. ondersteuning/uitvoering bieden bij respons op dreigingen en incidenten en
3. de crisisbeheersing versterken.

- Expertise en Advies

Informatie en advies ten aanzien van cybercriminaliteit, -spionage, -sabotage en -verstoringen die de Nederlandse samenleving aantasten worden bij het NCSC verzameld en ontwikkeld. Inzichten over kwetsbaarheden, dreigingen en risico's worden continu en proactief vertaald naar impactanalyses en adviezen omtrent handelingsperspectieven.

- Respons op dreigingen en incidenten

Wanneer partijen zelfstandig onvoldoende in staat zijn om te handelen in het geval cyberdreigingen of cyberincidenten plaatsvinden, kan vanuit het NCSC ondersteuning worden geboden. Deze

kerntaak geeft invulling aan de CERT-functie voor de overheid die het NCSC vervult, waarbij het uitgangspunt is dat partners in hun tweede of derdelijnsrespons worden ondersteund. [5]

- Operationele coördinatie van een ICT-crisis

Een crisis vereist collectieve coördinatiekracht: geen partij kan dit alleen oppakken. Binnen het NCSC is een concentratie van kennis, kunde en ervaring. Het NCSC levert een bijdrage aan preparatie door te ondersteunen bij (grootschalige) cyberoefeningen en scenario's. Daarnaast speelt het NCSC een rol in de signalering en eerste duiding van een cyberdreiging die zich mogelijk tot een crisis kan ontwikkelen. Tijdens een crisis vervult het NCSC een rol in de operationele coördinatie, alsmede in de advisering daaromtrent. Het NCSC is het National Point of Contact voor operationele ICT-crisis en incidenten, ook internationaal.

Voor de uitvoering van deze drie kerntaken maakt NCSC gebruik van verschillende samenwerkingsverbanden en instrumenten zowel in preparatie als crisissituaties. Zij treedt in deze samenwerkingsverbanden op als vertegenwoordiger van de Nederlandse overheid:

Information Sharing & Analysis Centers (ISAC's)
ISAC's zijn informatieknooppunten van vitale sectoren op het gebied van cybercrime en cyber security. Een ISAC is een omgeving waarbinnen publieke en private partijen gevoelige en vertrouwelijke informatie over dreigingen en best practices kunnen uitwisselen, binnen en buiten crisissituaties. De leden zijn afkomstig uit de organisaties van die binnen de betreffende ISAC vallen, en uit AIVD, KLPD en NCSC. De ISAC's hebben een signaleringsfunctie wat betreft dreigingen en incidenten.

Operationeel Incident Respons Team Overleg (O-IRT-O)
Het O-IRT-O is een samenwerkingsverband tussen Nederlandse CERTs waarbinnen operationele zaken besproken en afgehandeld worden. Zowel publieke als private CERTs nemen deel. Het O-IRT-O kan snel schakelen op operationele ontwikkelingen en voorzien in een passende respons.

International Watch and Warning Network (IWWN)
Het International Watch and Warning Network (IWWN) is een wereldwijd netwerk van overheidsvertegenwoordigers uit vijftien westerse landen op het gebied van cyber security beleid, operatie en wetshandhaving. In dit hoog vertrouwde netwerk wordt vertrouwelijke informatie uitgewisseld voor en tijdens een cyber crisis en/ of dreiging. Het IWWN onderhoudt de banden tussen de functionele 'point-of-contact' met een nationale verantwoordelijkheid, treedt op als coördinator tijdens dreigingen en crises, organiseert oefeningen, promoot samenwerking en stimuleert informatiedeling.

Forum of Incident Response and Security Teams (FIRST)
Wereldwijd forum van CERT's (ruim 200 leden, zowel publiek als privaat) via welke best practice documenten worden uitgewisseld en technisch colloquia en –cursussen worden georganiseerd.

European Network Information Security Agency (ENISA)
Organisatie die zich richt op de Europese Commissie en de lidstaten rond het onderwerp netwerk- en informatiebeveiliging, en deze partijen daarin ondersteunt. Doelstelling van ENISA is het vergroten van de veiligheid en weerbaarheid van communicatie- en - informatiesystemen.

European Government CERTs (EGC) group
Het "European Government CERT group" (EGC) is een hoog vertrouwd, informeel verband van overheid 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 incidentenrespons en informatiedeling.

[5] CERT staat voor Computer Emergency Response Team. Het NCSC is voor Nederland de aangewezen CERT. Tegenwoordig wordt vaak de term CSIRT gebruikt: Cyber Security and Incident Response Team.

ICT Respons Board (IRB)
De ICT Respons Board is een publiek-privaat samenwerkingsverband dat tijdens een grootschalige ICT-crisis of dreiging een analyse maakt van de situatie, op basis van een adequate informatie-uitwisseling. Indien nodig brengt de IRB een advies uit over te nemen maatregelen aan het Adviesteam en aan de vitale sectoren.

Deelnemers van de IRB zijn ICT-experts uit een aantal vitale sectoren (o.a. Telecom/ICT, Energie, Financieel en Drinkwater) en uit betrokken overheidsdiensten. Indien een IRB geactiveerd wordt bij een cybergerelateerde crisis is de samenstelling van de IRB flexibel om in te kunnen spelen op de situatie, waarbij naast de betrokken overheidsdiensten alleen de ICT-experts van de getroffen vitale sector worden betrokken.

De ICT Respons Board (IRB) wordt gefaciliteerd door het NCSC. Het ministerie van EL&I en het NCSC leveren respectievelijk de voorzitter en de informatiecoördinator aan de IRB. Het NCSC zorgt er daarnaast voor dat in algemene zin de relaties met en binnen de IRB worden onderhouden, zodat ten tijde van een crisis snel kan worden geschakeld.

Ministerie van Economische Zaken, Landbouw & Innovatie (EL&I)
Het ministerie van EL&I is verantwoordelijk voor de sector Telecom/ICT en heeft bij een ICT-crisis waar in hoofdzaak partijen bij zijn betrokken die onder de reikwijdte van de Telecommunicatiewet vallen specifieke bevoegdheden. Het ministerie is daarnaast ook verantwoordelijk voor de sectoren Energie (elektriciteit/olie/gas), Nucleair en Voedsel.

Agentschap Telecom
Agentschap Telecom is een agentschap dat ressorteert onder het ministerie van EL&I. Het agentschap houdt zich bezig met het verruimen, verdelen en optimaliseren van het elektronische communicatiedomein. Het accent ligt daarbij op het frequentiespectrum, maar daarnaast ziet het Agentschap, naast de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA), 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 sinds de inwerkingtreding van de geactualiseerde Telecommunicatie wet, per 5 juni 2012, de organisatie waar de melding in het kader van hoofdstuk 11a van de Telecomwet dient plaats te vinden.

De taken en verantwoordelijkheden van het Agentschap Telecom in crisistijd omvatten onder meer:
- proactief toezicht houden en adviseren op locatie. Dit is ten behoeve van de continuïteit van de netwerken en diensten en ter ondersteuning van de rampenbestrijding;
- het beoordelen van de directe en lange termijn effecten van de ramp;
- het beoordelen van andere processen in relatie tot het Elektronisch Communicatie Domein, zoals bijv:
    - 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.

Tevens verzamelt de operationeel coördinator van het Agentschap Telecom informatie vanuit het werkveld voor bespreking, afweging en zo nodig besluitvorming binnen het Departementaal Coördinatiecentrum van EL&I (DCC EL&I) en het Adviesteam.

3.2 Gremia zonder formele rol in de crisisstructuur

De volgende gremia zijn structureel van aard en vervullen hun rol primair buiten crisissituaties. Bij een opschaling naar de crisisstructuur hebben zij geen formele rol. Indien nodig kunnen deze gremia bij een ICT-crisis informeel geconsulteerd worden.

Cyber Security Raad (CSR)
De CSR is een publiek-private adviesraad op strategisch niveau op het gebied van Cyber Security. De Raad heeft de taak om de regering en private partijen gevraagd en ongevraagd adviezen te geven over relevante ontwikkelingen op het gebied van digitale veiligheid. De Raad kent een co-voorzitterschap van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV, tevens voorzitter ICCB) en de Chief Executive Officer (CEO) van KPN.

NCO-T (Nationaal Continuïteitsoverleg - Telecommunicatie)
Het Nationaal Continuïteitsoverleg - Telecommunicatie (NCO-T) is een regulier overleg tussen het Ministerie van EL&I en de telecommunicatieaanbieders die zijn aangewezen volgens artikel 14.6 van de Telecommunicatiewet. 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. Deelname aan het NCO-T is verplicht voor de aangewezen partijen. Tijdens crises vallen de aangewezen aanbieders in het geval van buitengewone omstandigheden onder de aanwijzingsbevoegdheid van de minister van EL&I.
Aangewezen zijn:

- KPN Telecom
- Ziggo
- UPC
- T-Mobile
- Vodafone
- Tele2

Bij een ICT crisis speelt het NCO-T als gremium geen formele rol. Wel zal het gremium kunnen worden geconsulteerd en heeft het een signalerende functie. De individuele leden kunnen gevraagd worden input aan te leveren voor het DCC-ELI. Uit het NCO-T zijn deelnemers afgevaardigd in de ICT Respons Board (IRB)

Interdepartementale Commissie Chief Information Officers (ICCIO)
Het ICCIO is een gremium van de CIO's van de Rijksoverheid en wordt voorgezeten door de CIO-Rijk van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). De CIO's zijn verantwoordelijk voor de informatiebeveiliging van het Rijk. Aan dit overleg kunnen CIO's worden toegevoegd van medeoverheden (VNG, IPO) en bedrijfsleven (CIO-platform, VNO-NCW, en MKB-Nederland). Dit gremium kan betrokken worden indien de ICT-crisis gevolgen heeft voor de bedrijfsvoering van de overheid.

3.3 Internationale contacten

ICT is zo verknoopt met het buitenland, evenals veel in dit veld werkzame organisaties, dat een ICT-crisis snel een internationaal karakter krijgt. Of de bron van de verstoring komt (gedeeltelijk) uit het buitenland, of de dienstverlenende organisaties ondervinden storingen vanuit het buitenland. Op verschillende niveaus vindt internationale afstemming plaats. De wijze waarop dit plaatsvindt is momenteel sterk in ontwikkeling. Ten behoeve van dit plan wordt een aantal organisaties en gremia genoemd die een specifieke functie vervullen rol bij het aanpakken van een internationale ICT crisis. Buiten beschouwing worden de generieke organisaties, zoals het ambassadenetwerk van het ministerie van Buitenlandse Zaken of private partijen die onderdeel zijn van een internationaal concern.
In de paragraaf van het NCSC worden het IWWN en het EGC kort belicht. Hier kan worden volstaan met het noemen de volgende contacten:

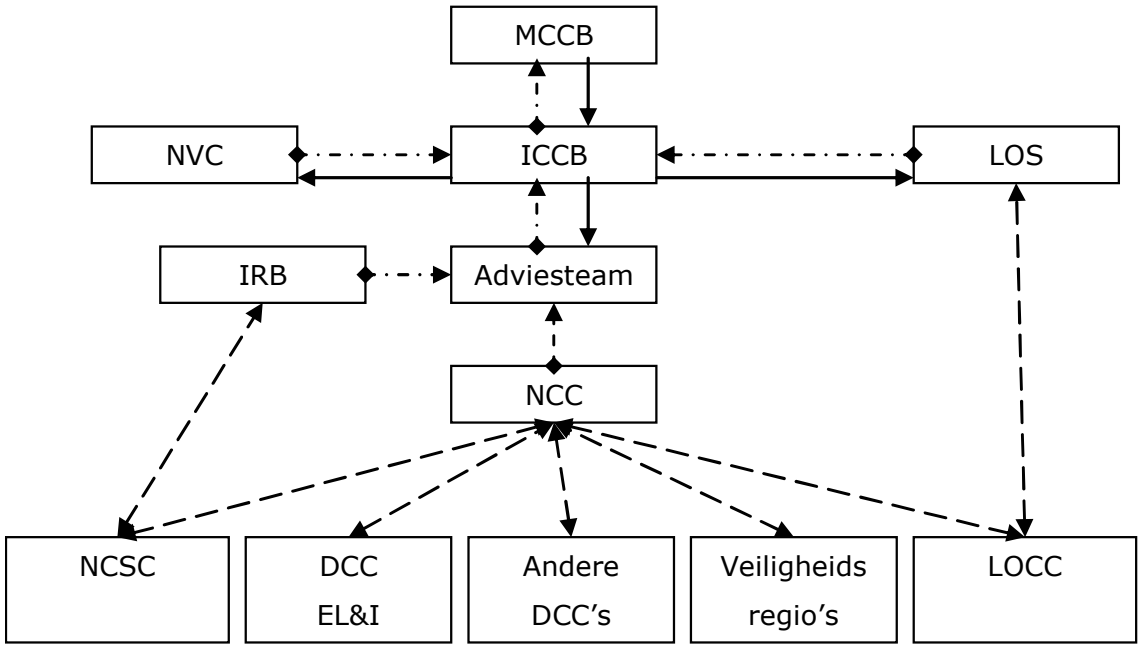
1. Europese Unie: In het kader van het actieprogramma Critical Information Infrastructure Protection (CIIP) zijn enkele activiteiten opgezet ter voorbereiding op ICT crisis binnen de EU. Dit zijn:

   a. De opzet van een zogeheten Standard Operating Procedures (SOP). Dit is een hulpmiddel voor de CERT's in Europa om op een veilige en effectieve wijze informatie uit te wisselen bij een internationale ICT-crisis.
   b. Houden van Internationale oefeningen, de Cyber Europe cyclus, waar ondermeer de SOP wordt getest.
   c. Het ontwikkelen van een European Cyber crisis cooperation framework. Een handreiking voor het effectiever uitwisselen van informatie ten behoeve van besluitvorming in de landen
2. NAVO
   a. Centre of Excellence in Talinn Estland, waar ondermeer oefeningen worden voorbereid zoals de Cyber Coalition oefening
3. EU-VS samenwerking. Afspraak tussen EU en VS op het gebeid van cyber security met ondermeer de afspraak om op operationele crisisbeheersing bij ICT crisis samen te werken. Daarvoor wordt oefeningen als instrument gebruikt, onder de naam Cyber Atlantic.

Hoofdstuk 4 Processen

Dit hoofdstuk bevat een weergave van het crisisbesluitvormingsproces bij een ICT-crisis. Met behulp van figuur 1 is een versimpelde weergave gegeven van de crisisstructuur op nationaal niveau zoals vastgelegd in het Nationaal Handboek Crisisbesluitvorming.[6] Hierin zijn de partijen die een specifieke rol spelen in ICT-crisis opgenomen. Onder figuur 1 volgt een toelichting.

Figuur 1: Crisisbesluitvormingsproces bij ICT-crisis



Legenda:

– – – – – ▶ = informatie-uitwisseling

◆·-·-·-·-·-▶ = advisering

——————▶ = besluitvorming

Toelichting van het crisisbesluitvormingsproces

De generieke interdepartementale coördinatiestructuur bestaat uit de volgende interdepartementale (organisatie)onderdelen:

- Het Adviesteam
- De Interdepartementale Commissie Crisisbeheersing (ICCB)
- De Ministeriële Commissie Crisisbeheersing (MCCB)[7]
- Het Nationaal CrisisCentrum (NCC)
- Het Nationaal Voorlichtingscentrum (NVC)
- De Landelijk Operationele Staf (LOS).

In het Nationaal Handboek Crisisbesluitvorming is deze crisisstructuur uitgebreid beschreven, waarbij wordt ingegaan wanneer de betrokken (organisatie)onderdelen worden geactiveerd, wat de samenstelling is en welke taken en rollen kunnen worden onderscheiden.

[6] Het Nationaal Handboek Crisisbesluitvorming wordt herzien. In de volgende versie van het NCP-ICT zal figuur 1 in lijn worden gebracht met de dan geldende versie van het NHC.

[7] Artikel 25, eerst lid van het Reglement van orde voor de ministerraad en Besluit d.d. 3 juli 2009, nr. 3080014 (Staatscourant, 24 juli 2009).

Tijdens een ICT-crisis hebben daarnaast de volgende partijen een specifieke rol:
- NCSC
- IRB
- DCC EL&I

Hieronder volgt een korte omschrijving van figuur 1 waarbij de beschrijving van de rol van de andere Departementale CoördinatieCentra (DCC's) en de veiligheidsregio's buiten beschouwing worden gelaten, omdat hun rol gelijk is aan de generieke crisisstructuur op nationaal niveau.

Generieke interdepartementale coördinatiestructuur
Het **Nationaal CrisisCentrum (NCC)**, ondergebracht bij het Ministerie van Veiligheid en Justitie, vervult de functie van interdepartementaal communicatiecentrum 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.[8]

Het **Adviesteam** wordt geactiveerd wanneer er een (mogelijke) dreiging op een nationale crisis bestaat. Het Adviesteam vormt een beeld en oordeel van de situatie, stemt af welke maatregelen getroffen moeten worden en levert een advies op voor de ICCB/MCCB. Indien dit nodig is, dan worden de daar te bespreken punten voorbereid.

De **Interdepartementale Commissie Crisisbeheersing (ICCB)** kan worden geactiveerd wanneer sprake is van een (dreigende) nationale crisis, dus wanneer een (dreigende) crisis één sector overstijgt. De ICCB is een gremium op hoogambtelijk niveau. De door de ICCB genomen besluiten worden zo nodig ter goedkeuring voorgelegd aan de MCCB.

De **Ministeriële Commissie Crisisbeheersing[9] (MCCB)** kan geactiveerd worden als bij een nationale crisis interdepartementale coördinatie op politiek-bestuurlijk niveau noodzakelijk is. Er wordt hierbij gekeken naar (internationale) politieke en bestuurlijke consequenties van de te nemen besluiten.

Het Adviesteam en de ICCB kunnen ook bij elkaar komen om informatie uit te wisselen over een (dreigende) nationale crisis, zonder dat dit leidt tot besluitvorming door de MCCB.

In het geval dat landelijke coördinatie van de communicatie en voorlichting naar pers en publiek noodzakelijk is, kan overgegaan worden tot opschaling van het **Nationaal Voorlichtingscentrum (NVC)**. Voor landelijke operationele coördinatie voor de openbare orde en veiligheid kan het Landelijk Operationeel Coördinatie Centrum (LOCC) opgeschaald worden naar de **Landelijke Operationele Staf (LOS)**.

Specifieke rol bij een ICT-crisis
Het **Nationaal Cyber Security Centrum (NCSC)** heeft ten tijde van een ICT-crisis de operationele coördinatie binnen de crisisorganisatie. Daarnaast faciliteert het NCSC de IRB en levert hiervoor een informatiecoördinator. Op deze manier krijgt de IRB informatie direct uit het operationele proces. Het NCSC kan ten tijde van een crisis operationele en tactische informatie doorgeven aan het NCC.

Wanneer er sprake is van een grootschalige sectoroverstijgende crisis, zal er een opschaling van de **ICT Respons Board (IRB)** plaatsvinden. De getroffen vitale sectoren en betrokken publieke partijen zullen een advies opstellen. Het IRB advies wordt primair gestuurd naar het Adviesteam en

[8] Nationaal Handboek Crisisbesluitvorming
[9] De artikelen 11, 21 en 22 van het Reglement van orde voor de ministerraad zijn van toepassing op de werkwijze van de commissie. Met betrekking tot artikel 11 geldt dat de doorslaggevende stem van de voorzitter telt, ook in die gevallen waarin de minister-president geen voorzitter is. De MCCB kan waar nodig afwijken van de bepalingen in deze paragraaf, tenzij dit in strijd is met het voornoemde Reglement en/of het instellingsbesluit van de MCCB.

de "parate organisaties". [10] Het Adviesteam zal een integraal advies opstellen, waar het IRB advies als input wordt meegenomen. Na verzending wordt het IRB advies niet gewijzigd, indien noodzakelijk wordt het advies direct verstuurd naar ICCB. Indien nodig licht de IRB voorzitter het advies toe bij het Adviesteam of ICCB.

Het Ministerie van EL&I (**DCC EL&I**) heeft specifieke bevoegdheden wanneer een ICT-crisis gevolgen heeft die onder de reikwijdte van de Telecommunicatiewet vallen.

[10] Parate organisaties zijn organisaties uit de vitale sectoren die deelnemen in de IRB en getroffen worden door de crisis.

Bijlage 5 Afkortingenlijst

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CSIRT	Cyber Security and Incident Response Team
CSR	Cyber Security Raad
DCC	DepartementaaL CoördinatieCentrum
DCS	Directie Cyber Security
EGC	European Government CERTs group
EL&I	Het Ministerie van Economische Zaken, Landbouw & Innovatie
ENISA	European Network Information Security Agency
FIRST	Forum of Incident Response and Security Teams
NCSC	Nationaal Cyber Security Centrum
NHC	Nationaal Handboek Crisisbesluitvorming
NRB	Nationale Risicobeoordeling
ICCB	Interdepartementale Commissie Crisisbeheersing
ICCIO	Interdepartementale Commissie Chief Information Officers
ICT	Informatie- en communicatietechnologie
IPO	Interprovinciaal Overleg
IRB	ICT Respons Board
ISAC	Information Sharing & Analysis Center
IWWN	International Watch and Warning Network
KLPD	Korps Landelijke Politiediensten
LOCC	Landelijke Operationeel CoördinatieCentrum
LOS	Landelijk Operationele Staf
MCCB	Ministeriële Commissie Crisisbeheersing
MKB	Midden- en kleinbedrijf - Nederland
NAVO	Noord-Atlantische Verdragsorganisatie

NCC	Nationaal CrisisCentrum
NCO-T	Nationaal Continuïteitsoverleg Telecommunicatie
NCP-ICT	Nationaal Crisisplan ICT
NCSC	Nationaal Cybersecurity Centrum
NCSS	Nationale Cyber Security Strategie
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NVC	Nationaal Voorlichtingscentrum
NFI	Nederlands Forensisch Instituut
NRB	Nationale Risicobeoordeling
OM	Openbaar Ministerie
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
O-IRT-O	Operationeel Incident Respons Team Overleg
SOP	Standard Operating Procedures
VenJ	Het ministerie van Veiligheid en Justitie
VNG	Vereniging Nederlanse Gemeenten