PLATFORM VOOR CYBERSECURITY
CPNI.NL

Weerbaarheid van **het Rijk** tegen uitval van elektriciteit en telecommunicatie

Diplomatieke Communicatie, Besluitvorming Openbaar Bestuur Rijk, Informatieverstrekking Overheid en Basisregistraties

Rapportage

In opdracht van de ministeries van
Veiligheid en Justitie/DG Veiligheid en
Economische Zaken, Landbouw en Innovatie/DG Energie en
Telecom en Mededinging

Rubricering: TLP Geel

Capaciteitsadvies Elektriciteit en Telecom

Juli 2011

PLATFORM VOOR CYBERSECURITY
CPNI.NL

Het Traffic Light Protocol (TLP) is ontworpen om sensitieve informatie op basis van vertrouwen te delen met andere personen en organisaties. Uitgangspunt is dat de eigenaar van de informatie bepaalt in welke mate de ingebrachte informatie geopenbaard mag worden door de ontvangende personen c.q. organisaties.

De rubricering **TLP GEEL** geeft een beperkte distributie aan. Op basis van **need-to-know** mag informatie binnen een **beperkte kring** gedeeld worden. De eigenaar van de informatie kan eventueel extra beperkingen aangeven betreffende de verspreiding.

Versie	Datum	Auteur	Opmerkingen
0.1	05-05-2011	CPNI.NL	
0.2	06-05-2011	CPNI.NL	
0.4	25-05-2011	CPNI.NL	
0.5	30-05-2011	CPNI.NL	
0.6	06-06-2011	CPNI.NL	
0.7	05-07-2011	CPNI.NL	
0.8	06-07-2011	CPNI.NL	
0.9	07-07-2011	CPNI.NL	
0.91	30-08-2011	CPNI.NL	
0.93	20-09-2011	CPNI.NL	
1.0	03-10-2011	CPNI.NL	

INHOUDSOPGAVE

MANAGEMENTSAMENVATTING 3

1 TOELICHTING ONDERZOEK 6

1.1 INLEIDING EN ACHTERGROND 6
1.2 DOELSTELLING 6
1.3 VRAAGSTELLING 6
1.4 UITGANGSPUNTEN 7
1.5 ONDERZOEKSMETHODEN 7
1.6 AFBAKENING 8
1.7 VERTROUWELIJKHEID 9
1.8 LEESWIJZER 9

2 TYPERING VITALE DIENSTEN EN PRODUCTEN SECTOR RIJK 11

2.1 DIPLOMATIEKE COMMUNICATIE 11
2.2 BESLUITVORMING OPENBAAR BESTUUR RIJK 12
2.3 INFORMATIEVERSTREKKING OVERHEID 13
2.4 BASISREGISTRATIES 14
2.5 GERELATEERDE ONTWIKKELINGEN 17

3 WEERBAARHEID TEGEN UITVAL TELECOMMUNICATIE EN ELEKTRICITEIT 18

3.1 DIPLOMATIEKE COMMUNICATIE 18
3.2 BESLUITVORMING OPENBAAR BESTUUR RIJK 18
3.3 INFORMATIEVERSTREKKING OVERHEID 19
3.4 BASISREGISTRATIES 20
3.4.1 De Gemeentelijke Basisadministratie Persoonsgegevens (GBA) 20
3.4.2 Nieuw Handelsregister (NHR) 21
3.4.3 Basisregistratie Adressen en Gebouwen (BAG) 22
3.4.4 Basisregistratie Kadaster (BRK) 22

4 MOGELIJK AANVULLENDE MAATREGELEN 24

4.1 DIPLOMATIEKE COMMUNICATIE 24
4.2 BESLUITVORMING OPENBAAR BESTUUR RIJK EN INFORMATIEVERSTREKKING OVERHEID 24
4.3 BASISREGISTRATIES 26

5 CONCLUSIE 28

I. RESPONDENTEN INTERVIEWS 29
II. REFERENTIES CAET PROJECT 29

Managementsamenvatting

Elektriciteit en telecommunicatie vormen het motorblok van de Nederlandse samenleving. Vanuit het programma Nationale Veiligheid van de rijksoverheid is het project Capaciteitsadvies Elektriciteit en Telecom/ICT (CAET) gestart met het doel de weerbaarheid van vitale sectoren tegen uitval van elektriciteit en/ telecommunicatie inzichtelijk te maken en zo nodig te vergroten. Aanvullend dient het project inzicht te geven in kansrijke aanvullende maatregelen. Opdrachtgevers zijn de ministeries van Economische Zaken, Landbouw en Innovatie (EL&I) en Veiligheid en Justitie (VenJ). Opdrachtnemer is Centre for the Protection of National Infrastructure NL (CPNI.NL). Het projectteam van CPNI.NL voert samen met de sectoren het project uit.

Deze rapportage richt zich op de weerbaarheid van de sector Rijk met de afbakening:

- Diplomatieke communicatie
- Besluitvorming Openbaar Bestuur Rijk
- Informatieverstrekking overheid
- Basisregistraties (GBA, NHR, BAG en BRK)[1]

Samengevat worden de kritische processen van deze vitale diensten bij grootschalige uitval van elektriciteit en/of telecommunicatie ernstig bemoeilijkt. Men rekent hier op het kunnen terugvallen op noodcommunicatiemiddelen, noodstroomaggregaten en uitwijklocaties.

Bij uitval van telecommunicatie beschikt het postennetwerk voor diplomatieke communicatie over verschillende alternatieve communicatiemiddelen, zoals satelliettelefoons en satellietschotels. Voor besluitvorming van het openbaar bestuur en informatieverstrekking geldt dat het verzamelen van informatie wordt bemoeilijkt. De departementale crisiscentra en de belangrijkste partners kunnen elkaar echter nog wel bereiken via noodnet. Voor de basisregistraties geldt dat uitwisseling van gegevens bij uitval van telecommunicatie niet op de gebruikelijke manier plaats zal vinden. Een alternatief is het gebruiken van een kopie van het gegevensbestand of een kantoor fysiek aandoen.

Voor de vier vitale diensten geldt dat bij uitval van elektriciteit de beschikbare noodstroomaggregaten en uitwijklocaties de achtervang zijn. De samenleving verwacht op in deze situatie een adequate reactie van de overheid. Op basis van geïnventariseerde mogelijke aanvullende maatregelen zijn aanbevelingen geformuleerd:

Diplomatieke communicatie

- Bestudeer de service level agreements met de aanbieder van de telecommunicatieverbindingen kritisch. In hoeverre blijft deze ook werken bij bijvoorbeeld elektriciteituitval.
- Overweeg om voor alle posten noodstroomaggregaten aan te schaffen.
- Leg vast hoe met elkaar te communiceren bij het wegvallen van een communicatiemiddel.

Besluitvorming openbaar bestuur Rijk en informatieverstrekking

- Ga in gesprek met de telecommunicatie aanbieder en vraag om verduidelijking van de service level agreements. En vraag bij het afsluiten van nieuwe abonnementen naar robuustheid van de verbinding en alternatieven.

---

[1] GBA - Gemeentelijke Basisadministratie van persoonsgegevens
NHR - Nieuw Handelsregister
BAG - Basisregistraties Adressen en Gebouwen (bestaat uit 2 basisregistraties)
BRK - Basisregistratie Kadaster

- Exploreer de mogelijkheden hoe (crisis)besluitvormers en -voorbereiders (buiten kantoortijd) gealarmeerd kunnen worden, wanneer telecommunicatie is uitgevallen. Hoe en door wie wordt het crisisteam bij elkaar geroepen?
- Maak afspraken met alternatieve informatie leverantie mogelijkheden, zoals afspraken met koeriers en leg deze vast.
- Maak afspraken met (informatieleverende) partners hoe met elkaar te communiceren bij uitval van telecommunicatie.
- Oefen samen met (informatieleverende) partners met het scenario telecommunicatie uitval.
- Bedenk hoe medewerkers van (crisis)organisaties ontzorgt en gecompenseerd kunnen worden, zodat zij met een gerust hart hun werk kunnen doen en zich geen zorgen maken of en hoe hun naasten zich redden bij een grootschalige uitval van telecommunicatie en/of elektriciteit.
- Bedenk als Rijk wat een wenselijke noodcommunicatie voorziening is. Voorbeelden uit het buitenland (Engeland, Zweden en Amerika) kunnen hierbij helpen.
- Aanbeveling aan het ministerie van VenJ om met de huidige noodnet abonnees duidelijk te communiceren wat de status van de Nood Communicatie Voorziening (NCV) is.
- De (crisis)organisaties dienen op hun beurt te inventariseren of hun partners ook overstappen naar hetzelfde abonnement, zodat deze partijen met elkaar kunnen communiceren via dezelfde noodcommunicatievoorziening.
- Versterk zelfredzaamheid van burgers en bedrijven door voorlichting te geven over wat te doen bij uitval van telecommunicatie en wat te verwachten van de overheid.
- Werk het scenario drie dagen zonder telecommunicatie voor de samenleving uit. Denk aan:
    - Het maken van afspraken tussen Rijk en Regio hoe met de samenleving te communiceren, bijvoorbeeld m.b.v. communicatiekaarten. Wat zijn de landelijk geldende generieke berichten en wat zijn de specifieke berichten voor die regio?
        - Voorbeeld voorlichting in getrapte vorm: MCCb doet verzoek aan regio's consequent 'het volgende' uit te dragen (bv. schakel uw regionale rampenzender op de radio in). Aanvullend zullen regio's voorlichting geven over regionale zaken (boodschap is plaatsafhankelijk).
    - Welke communicatiemiddelen heb je als overheid bij welk scenario? Dit kan per regio verschillen.
- Voor het NCC is een belangrijke taak weggelegd na de drie dagen. Hoe de samenleving na deze drie dagen voorlichten? Hier kan nu alvast over nagedacht worden. De boodschap na de drie dagen is van groot belang voor de Rijksoverheid. Tijdens deze drie dagen is de boodschap plaatsafhankelijk.
- Houd de continuïteit van het rijk bij elektriciteituitval op orde door:
    - Noodstroomaggregaten (NSA) regelmatig te testen en onderhoud te plegen. Geopperd is hier het Directoraat-Generaal Organisatie en Bedrijfsvoering Rijk (DG OBR) een coördinerende rol in de te laten vervullen;
    - te oefenen met het scenario van drie dagen elektriciteituitval;
    - te weten wat de rol van de rijksoverheid is bij grootschalige elektriciteituitval.
- Versterk zelfredzaamheid van burgers en bedrijven door voorlichting te geven over wat te doen bij uitval van elektriciteit en wat te verwachten van de overheid.
- Weet als vakdepartement wat grootschalige elektriciteituitval doet met de vitale sectoren. Maak met vitale sectoren afspraken over hoe te reageren op grootschalige elektriciteituitval.

Basisregistraties

- Wees duidelijk naar afnemers van de basisregistratie wat uitval van telecommunicatie en/of elektriciteit betekent voor desbetreffende basisregistratie en beoordeel gezamenlijk of genomen maatregelen afdoende zijn.

De ministeries van Veiligheid en Justitie en Binnenlandse Zaken hebben de opdracht met andere ministeries te bespreken hoe opvolging te geven aan de aanbevelingen.

1 Toelichting onderzoek

1.1 Inleiding en achtergrond

Elektriciteit en telecommunicatie vormen het motorblok van de Nederlandse samenleving. Zonder een adequate werking van beide of één van beide diensten werkt er in Nederland niet veel meer. Het is van belang dat beide sectoren zelf en andere, van elektriciteit en telecommunicatie afhankelijke, vitale sectoren zich terdege voorbereiden op een mogelijke grootschalige en/of langdurige uitval van elektriciteit en/of telecommunicatie.

Vanuit het programma Nationale Veiligheid van de rijksoverheid is het project Capaciteitsadvies Elektriciteit en Telecom/ICT (CAET) gestart. Het CAET project heeft het doel de weerbaarheid van alle vitale sectoren tegen verstoringen in elektriciteitsvoorziening respectievelijk de telecommunicatievoorzieningen inzichtelijk te maken en zo nodig te vergroten. Aanvullend dient het project inzicht te geven in kansrijke aanvullende maatregelen. Het project is in 2009 gestart met de sectoren telecommunicatie, energie (elektriciteit en gas) en financiën (fase 1). In 2010 is fase 2 gestart met de sectoren drinkwater, keren en beheren oppervlaktewater, openbare orde en veiligheid, openbaar bestuur en olie.

Opdrachtgevers zijn de ministeries van Economische Zaken, Landbouw en Innovatie (EL&I) en Veiligheid en Justitie (VenJ). Opdrachtnemer is Centre for the Protection of National Infrastructure NL (CPNI.NL). Het projectteam van CPNI.NL voert samen met de sectoren het project uit.

Deze rapportage richt zich op de weerbaarheid van vier onderdelen van de sector openbaar bestuur op rijksniveau, namelijk: diplomatieke communicatie, besluitvorming openbaar bestuur rijk, informatieverstrekking overheid, en basisregistraties. Hierna te noemen als 'sector Rijk'.

1.2 Doelstelling

De ministeries van EL&I en VenJ hebben de doelstelling als volgt geformuleerd: de weerbaarheid van sector Rijk tegen ernstige verstoringen in de elektriciteit- respectievelijk de telecommunicatiesector inzichtelijk maken en zo nodig te vergroten[2]. Na fase 1 is een tweede doelstelling toegevoegd: 'een proces op gang brengen'. Het is belangrijk dat vitale sectoren zich bewust zijn van hun afhankelijkheden van elektriciteit en telecommunicatie, nadenken over de reeds genomen maatregelen en in discussie gaan over mogelijke aanvullende maatregelen.

1.3 Vraagstelling

De centrale vragen van het CAET onderzoek zijn:

1. Wat zijn de kritische processen binnen een vitale dienst in de sector waarvoor het gebruik van elektriciteit en/of telecommunicatie van wezenlijk belang is?
2. Zijn er voor deze processen continuïteitsmaatregelen getroffen bij uitval van elektriciteit en/ of telecommunicatie?
3. Zo ja, hoelang wordt het volgehouden?
4. Welke aanvullende maatregelen kunnen worden getroffen?

[2] In de voortgangsbrief Nationale Veiligheid aan de Tweede Kamer van 5 juni 2009 is de volgende passage opgenomen: "Het kabinet zet zich er voor in dat de vitale sectoren eind 2010 zich volledig bewust zijn van de mate van afhankelijkheid van energie (m.n. elektriciteit) en ICT. Bij die sectoren waar deze afhankelijkheid van wezenlijk belang is voor het kunnen blijven leveren van hun vitale diensten is dan in continuïteitsplannen aandacht gegeven aan de weerbaarheid tegen verstoring van elektriciteit en ICT."

Hierbij wordt uitgegaan van totale uitval van elektriciteit en/of telecommunicatie voor drie dagen.

1.4 Uitgangspunten

Bij de uitvoering van dit project zijn de volgende uitgangspunten gehanteerd:

Maatwerk per sector
Niet elke sector is op dezelfde manier georganiseerd en niet elke sector is op dezelfde manier met businesscontinuïteit bezig. Daarom is binnen dit project gekozen voor maatwerk per sector. Maatwerk betekent in de praktijk vooral het vinden van de juiste aanspreekpunten en sleutelpersonen binnen een sector en het afstemmen van de relevantie van de onderzoeksvragen met deze sleutelpersonen.

Aansluiting bij bestaande structuren
Voor het verkrijgen van draagvlak binnen de sectoren en het beperken van de belasting voor de sectoren is er in dit project voor gekozen om zoveel als mogelijk gebruik te maken van bestaande (overleg)structuren.

Betrokkenheid bronsectoren telecommunicatie en elektriciteit
Belangrijk voor dit traject is de betrokkenheid van de sectoren elektriciteit en telecommunicatie. De detailkennis van deze sectoren helpt bij het verkrijgen van inzicht in de weerbaarheid van vitale sectoren tegen de uitval van elektriciteit en/ of telecommunicatie.

Intersectorale aanpak
Dit project is er nadrukkelijk op gericht om sectoren met elkaar in contact te brengen en informatie-uitwisseling te stimuleren met als doel de weerbaarheid tegen uitval te vergroten. Veel kennis over weerbaarheid is aanwezig binnen een sector, maar ook de bronsectoren (elektriciteit en telecommunicatie) kunnen een rol spelen bij het vergroten van het inzicht in vitale afhankelijkheden en in het vergroten van de weerbaarheid.

1.5 Onderzoeksmethoden

Het plan van aanpak is gezamenlijk met de directie Nationale Veiligheid van het ministerie van VenJ opgesteld. Met behulp van een bureaustudie en interviews is de weerbaarheid van sector Rijk tegen uitval van elektriciteit en/of telecommunicatie in kaart gebracht.

Relevante documenten betreffen beleidsstukken en eerdere onderzoeken naar wederzijdse afhankelijkheden tussen vitale sectoren. Interviews zijn gehouden Departementale CrisisCentra, het Nationaal Crisiscentrum (inclusief cluster risico- en crisiscommunicatie) en vertegenwoordigers van het stelsel van basisregistraties zoals het Bureau Persoonsgegevens en Reisdocumenten, Het Kadaster en de Kamer van Koophandel.

Deze rapportage is ter kennisgeving aan de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) voorgelegd. Voorts zijn de resultaten door de opdrachtgevers (EL&I en VenJ) gedeeld met de Stuurgroep Nationale Veiligheid onder waarborging van de rubricering TLP GEEL.

1.6 Afbakening

De sector Openbaar Bestuur bestaat volgens de tweede inhoudelijke analyse bescherming vitale infrastructuur (2010) uit vier vitale diensten, namelijk:

- Diplomatieke communicatie
- Informatieverstrekking overheid
- Krijgsmacht
- Besluitvorming openbaar bestuur

Na overleg met de opdrachtgevers is besloten de weerbaarheid van de krijgsmacht niet te onderzoeken. De opdrachtgevers gaan ervan uit dat de krijgsmacht onder alle omstandigheden zelfredzaam is gezien haar taakstelling. Aanvullend is, op verzoek van de opdrachtgevers, de weerbaarheid van de basisregistraties in kaart gebracht, omdat de integriteit en vertrouwelijkheid van deze gegevens als zeer belangrijk wordt ervaren. Zie hieronder de nadere specificatie van de doelgroep:

Tabel 1. Afbakening

Vitale producten of diensten	**Vitale deelproducten/diensten**	**Betrokken organisaties**
Diplomatieke communicatie	Het onderhouden van contact met ambassades, buitenlandse regeringen en internationale organisaties (data en spraak-communicatie)	Ministerie van Buitenlandse Zaken
Informatieverstrekking overheid	Media en publieksvoorlichting in crisistijd	Ministerie van VenJ (Nationaal Crisiscentrum (NCC), cluster Risico- en Crisiscommunicatie)
Besluitvorming openbaar bestuur rijk	Functioneren van de nationale crisisbesluitvorming	NCC en departementale crisiscentra (DCC's)
Basisregistraties	Stelsel van basisregistraties[3] GBA, NHR, BAG en BRK	Programmaraad Stelsel van Basisregistraties

In overleg met vertegenwoordigers van het stelsel van basisregistraties is overeengekomen dat niet alle 13 basisregistraties als vitaal kunnen worden aangemerkt. Het onderzoek heeft zich gericht op de basisregistraties: Gemeentelijke Basisadministratie Persoonsgegevens (GBA), Nieuw Handelsregister (NHR), Basisregistratie Adressen en Gebouwen (BAG) en Basisregistratie Kadaster (BRK). Voor de andere basisregistraties geldt dat er of met kopieën gewerkt kan worden, of het drie dagen niet beschikbaar en/of niet bereikbaar zijn, niet als vitaal kan worden aangemerkt.

[3] GBA - Gemeentelijke Basisadministratie van persoonsgegevens
NHR - Nieuw Handelsregister
BAG - Basisregistraties Adressen en Gebouwen (bestaat uit 2 basisregistraties)
BRT - Basisregistratie Topografie
BRK - Basisregistratie Kadaster
BRV – Basisregistratie Voertuigen
BLAU – Basisregistratie Lonen, Arbeids- en Uitkeringsverhoudingen
BRI – Basisregistratie Inkomens
WOZ – Basisregistratie Onroerende Zaken
RNI - Registratie Niet-Ingezetenen
BGT - Basisregistratie Grootschalige Topografie
BRO – Basisregistratie Ondergrond

De continuïteit van de regionale crisisbesluitvorming is meegenomen bij het onderzoek naar de weerbaarheid van de politie- en veiligheidsregio's (openbare orde en veiligheid – regionaal niveau).

1.7 Vertrouwelijkheid

Vanwege het onderwerp van dit project 'de weerbaarheid van een vitale sector' verdient het thema vertrouwelijkheid van informatie extra aandacht.

Rapportage met hoog abstractieniveau
In verband met veiligheidseisen heeft de rapportage een hoog abstractieniveau. Gegevens die betrekking hebben op het voorkomen van een verstoring, de voorbereiding op een verstoring dan wel het optreden in geval van een verstoring is informatie die de veiligheid van de Staat kan schaden. Een aanvraag op basis van de Wet Openbaar Bestuur zou dergelijke schade kunnen opleveren. Om die reden bevat deze rapportage geen sensitieve detail-informatie.

Borging vertrouwelijkheid projectteam
CPNI.NL borgt de vertrouwelijkheid van de gedeelde informatie door middel van screening en een geheimhoudingsverklaring van de bij het project betrokken medewerkers.

Borging vertrouwelijkheid workshop
Het Traffic Light Protocol (TLP) wordt gehanteerd tijdens de workshop(s). Het TLP is een geaccepteerd informatie-uitwisselingsprotocol bij publiek-private informatiedeling. De informatievertrekker bepaalt welke kleur de informatie heeft: rood, geel, groen of wit.[4]

Rubricering: TLP Geel
Deze rapportage is gerubriceerd als TLP Geel. Dit houdt in dat dit rapport **op need-to-know basis** mag worden gedeeld binnen een **beperkte kring** van de organisatieonderdelen van de deelnemende bedrijven (hetzij directe medewerkers, adviseurs, opdrachtnemers, hetzij binnen de organisatie werkzaam, gedetacheerd personeel) die deze informatie uit hoofde van hun werkzaamheden nodig hebben om maatregelen te treffen. De toegangverleners verzekeren zich van de juiste wijze van omgaan met en bescherming en opslag van de gedeelde sectorbrede informatie.

1.8 Leeswijzer

Hoofdstuk 2 typeert de sector Rijk. Hierbij wordt ingezoomd op de vier gedefinieerde vitale diensten en hun kritische processen. Van belang zijn de gerelateerde projecten Continuïteit en ICT Response Board die tevens de weerbaarheid van de sector Rijk tegen uitval van elektriciteit en telecommunicatie bevorderen.

Hoofdstuk 3 beschrijft de weerbaarheid van de sector Rijk en de genomen maatregelen tegen respectievelijk telecommunicatie en elektriciteituitval.

[4] **Rode informatie** betreft geheime informatie uitsluitend ter kennisname van de aanwezigen. **Gele informatie** betreft informatie dat door de aanwezigen mag worden gedeeld binnen hun organisatie (hetzij directe medewerkers, adviseurs, opdrachtnemers, hetzij binnen de organisatie werkzaam, gedetacheerd personeel) die deze informatie nodig hebben om maatregelen te treffen. **Groene informatie** is informatie die met andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de vitale infrastructuurgemeenschap in bredere zin, mag worden gedeeld, maar die niet op andere wijze mag worden geopenbaard of op het web geplaatst. **Witte informatie** is bedoeld voor publieke, onbeperkte verspreiding, publicatie, plaatsing op het web of uitzending. Elke aanwezige mag witte informatie openbaar maken, met inachtneming van het auteursrecht.

In hoofdstuk 4 zijn op basis van mogelijk aanvullende maatregelen aanbevelingen geformuleerd en hoofdstuk 5 beschrijft de conclusies.

2 Typering vitale diensten en producten sector Rijk

De vitale diensten diplomatieke communicatie, informatievertrekking overheid, besluitvorming openbaar bestuur rijk en basisregistraties zijn in dit rapport aangeduid als sector 'Rijk'. Bij grootschalige calamiteiten hebben de Regio en het Rijk de zorg voor openbare orde en veiligheid. De effecten van een verstoring in een willekeurige vitale sector raken daarmee per definitie de verantwoordelijkheid van het openbaar bestuur.[5]

In dit hoofdstuk volgt een verdere toelichting op de vitale diensten, de kritische processen en hun afhankelijkheid van telecommunicatie en elektriciteit. Deze diensten sluiten tevens aan op de twee aspecten die eerder voor het openbaar bestuur als vitaal zijn aangemerkt:[6]

- Het beschermen van de continuïteit van besluitvorming tijdens de respons op en herstel na uitval van vitale infrastructuur.
- Het beschermen van de communicatiemiddelen voor de noodzakelijk informatie-uitwisseling tijdens (de dreiging van) ernstige calamiteiten tussen overheden en voor communicatie naar de bevolking.

Vitale infrastructuren zijn 'die producten, diensten en processen die, als zij uitvallen, maatschappelijk of economische ontwrichting van (inter-)nationale omvang kunnen veroorzaken, doordat er veel slachtoffers kunnen vallen en/of omdat het herstel zeer lang gaat duren en er geen reële alternatieven voorhanden zijn, terwijl we deze producten en diensten niet kunnen missen'[7]. De bescherming van de continuïteit van besluitvorming en communicatie is een belangrijk uitgangspunt voor het Rijk. Dit rapport richt zich op de continuïteit van diplomatieke communicatie, informatievertrekking overheid, besluitvorming openbaar bestuur rijk en vier basisregistraties (GBA, NHR, BAG en BRK). Onder telecommunicatie wordt zowel communicatie via vaste en mobiele telefonie als internet verstaan. Het gaat hier om de afhankelijkheid van de vitale diensten ten opzichte van externe telecomaanbieders.

2.1 Diplomatieke communicatie

Met behulp van diplomatie vinden onderhandelingen tussen vertegenwoordigers van groepen en staten plaats. Onderwerpen die behandeld worden, zijn onder andere vrede, oorlog, veiligheid, economie, cultuur, milieu en mensenrechten. Het kunnen hebben van diplomatieke data- en spraakcommunicatie is van essentieel belang. Denk hierbij niet alleen aan communicatie met andere landen en ambassadeurs, maar ook met internationale organisaties zoals de Verenigde Naties, NAVO en Europese Unie.

Diplomatieke communicatie is afhankelijk van het ontvangen en kunnen versturen van informatie. Via het zogenaamde postennetwerk heeft het ministerie van Buitenlandse Zaken contact met Nederlandse ambassades in het buitenland en met vertegenwoordigers bij internationale organisaties. Zonder telecommunicatie en/of elektriciteit wordt dit proces ernstig bemoeilijkt. Het *kritische proces* voor diplomatieke communicatie is:

- Data- en spraakverkeer met diplomatieke partners

[5] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2009). 2de inhoudelijke analyse bescherming vitale infrastructuur.
[6] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2009). 2de inhoudelijke analyse bescherming vitale infrastructuur.
[7] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2009). 2de inhoudelijke analyse bescherming vitale infrastructuur.

2.2 Besluitvorming openbaar bestuur Rijk

Met name in crisissituaties vervult de besluitvorming openbaar bestuur rijk een vitale rol. De afwezigheid van één of enkele bestuurlijke besluitvormers is niet vitaal. De beschikbaarheid van het openbaar bestuur bij een ernstige calamiteit is echter wel vitaal in verband met de vereiste besluitvorming en crisiscommunicatie richting de bevolking.[8] Het ministerie van Veiligheid en Justitie is als coördinerend ministerie verantwoordelijk voor de inrichting, werking, samenhang en integrale aanpak van het crisisbeheersingsbeleid (preparatie, respons, herstel) en bijbehorende stelsel. Ieder ministerie is daarnaast zelf verantwoordelijk voor de te nemen crisisbeheersingsmaatregelen op het eigen beleidsterrein en het stellen van kaders voor de maatregelen die vitale bedrijven moeten nemen voor de beheersing van crises.[9]

Bij grootschalige calamiteiten waar meerdere departementen betrokken zijn vindt de nationale crisisbesluitvorming plaats bij het Nationaal Crisiscentrum (NCC). De nationale crisisbesluitvorming vindt plaats op zowel ambtelijk als politiek niveau in respectievelijk de overleggen van het Adviesteam, de Interdepartementale Commissie Crisisbeheersing (ICCb) en de Ministeriële Commissie Crisisbeheersing (MCCb).[10]

In eerste instantie wordt een (dreigende) sectorale crisis opgepakt door de bewindspersoon wiens beleidsterrein het betreft. Hij is verantwoordelijk voor en belast met een adequate aanpak. Departementale responsactiviteiten binnen de eigen sector worden uitgevoerd en gecoördineerd door en vanuit het desbetreffende Departementaal Coördinatiecentrum (DCC).

In de aanloopfase van een (dreigende) crisis, waarbij mogelijk beleidsterreinen of belangen van andere ministeries zijn betrokken, komt het Adviesteam bijeen op het NCC. Dit overleg kent een flexibele samenstelling en bestaat onder andere uit het Hoofd NCC, crisisbeleidsadviseurs van de betrokken ministeries, stafmedewerker van het cluster voor Risico- en Crisiscommunicatie (cRC) van het NCC, stafmedewerker van het Landelijk Operationeel Coördinatiecentrum (LOCC) en een informatiemanager.

Indien een (dreigende) crisis één sector overstijgt en/of in geval van (mogelijke) opschaling van de crisiscommunicatie naar het nationale niveau wordt er op hoog ambtelijk niveau (DG/IG/SG-niveau) een Interdepartementale Commissie Crisisbeheersing (ICCb) geactiveerd die vergadert bij het NCC.

In een situatie die vraagt om coördinatie van intersectorale crisisbeheersing op politiek-bestuurlijk niveau kan de Ministeriële Commissie Crisisbeheersing (MCCb) bijeen komen. De commissie beraadslaagt onder meer over beeld- en oordeelsvorming van de (dreigende) crisissituatie en het nemen van besluiten over adviezen van de ICCb.[11]

Voor nationale crisisbesluitvorming is het hebben van informatie op basis waarvan besluiten genomen dienen te worden onmisbaar. Enerzijds reageert de nationale crisisstructuur op de (maatschappelijke) effecten van de grootschalige uitval van elektriciteit en/of telecommunicatie. Anderzijds neemt de nationale crisisbesluitvorming maatregelen zodat hun eigen kritische processen ook bij uitval van elektriciteit en telecommunicatie doorgang kunnen hebben. Zie hieronder de *kritische processen* voor respectievelijk het Adviesteam/ICCb en het MCCb.

---

[8] TNO (2007), Onderlinge Afhankelijkheid Vitale Sectoren: afhankelijkheidsonderzoek elektriciteit (SOVI intern gebruik).
[9] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2009). 2de inhoudelijke analyse bescherming vitale infrastructuur.
[10] Zie Nationaal Handboek Crisisbesluitvorming
[11] Zie Nationaal Handboek Crisisbesluitvorming

Adviesteam/Interdepartementale Commissie Crisisbeheersing

- het uitwisselen van informatie en inventariseren van informatie lacunes
- het vormen van beeld en oordeel van de situatie
- het afstemmen van de maatregelen binnen het eigen functionele beleidsdomein
- besluiten over de inrichting en werkwijze van het voorbereiden van de interdepartementale crisisbesluitvorming van ICCb en/of MCCb
- het nemen van adequate maatregelen in het kader van de voorbereiding, respons en nazorg
- het adviseren aan de minister-president en de minister van Veiligheid en Justitie over het bijeenkomen van een MCCb
- het adviseren aan de ministeriële commissie en/of aan andere overheden over te nemen maatregelen in het kader van de voorbereiding, respons en nazorg
- adviseren over (internationaal) politieke consequenties van genomen of te nemen maatregelen
- het bepalen van strategische kaders
- het opstellen van instructies voor de rijksdienst
- het bepalen van beleidskaders voor (publieks)voorlichting en woordvoering
- het bepalen vergaderstructuur en –frequentie

Ministeriële Commissie Crisisbeheersing

- beeld- en oordeelsvorming van de (dreigende) crisissituatie
- nemen van besluiten over adviezen van de ICCb
- (internationaal) politieke consequenties van genomen of te nemen besluiten
- adviezen ten behoeve van de ministerraad of andere overheden;
- bepalen van de strategische kaders
- inlichten van de Staten-Generaal;
- opstellen van instructies voor de rijksdienst
- bepalen van de beleidskaders voor publieks)voorlichting en woordvoering
- bepalen van de vergaderstructuur en –frequentie van de commissie

2.3 Informatieverstrekking overheid

Communicatie en voorlichting ingeval van een (dreigende) crisis is in eerste aanleg een verantwoordelijkheid van de betrokken departementale voorlichtingsdiensten en regionale en lokale diensten. Indien nodig ondersteunt het Nationaal CrisisCentrum (cluster Risico- en Crisiscommunicatie, cRC) hierbij. Zonodig vindt coördinatie van de communicatie en voorlichting over de crisis met pers en publiek op nationaal niveau plaats door middel van opschaling van het operationele cluster cRC naar het Nationaal Voorlichtingscentrum (NVC).[12]

Nationale media- en publieksvoorlichting ondervindt bij uitval van elektriciteit en/of telecommunicatie problemen in het kunnen verzenden van informatie. Enerzijds heeft de zender van voorlichting mogelijk niet de volledige informatie. Anderzijds heeft ontvanger mogelijk geen middelen om het bericht te kunnen ontvangen. Zie hieronder de *kritische processen* voor cRC en NVC.

Cluster Risico en Crisiscommunicatie en het Nationaal VoorlichtingsCentrum

- monitoren en analyseren van media, internet en de crisisomgeving
- adviseren van de ICCB en de MCCB over de te volgen communicatiestrategie en de communicatieve gevolgen van (voor)genomen besluiten

[12] Zie Nationaal Handboek Crisisbesluitvorming

- ontwikkelen, coördineren en uitvoeren van de communicatie van de rijksoverheid
- voorbereiden en geven van voorlichting aan de nationale en internationale media
- informeren van andere overheden over de communicatieactiviteiten van de rijksoverheid en het coördineren van de communicatie van de rijksoverheid en de andere overheden
- vervaardigen van concrete communicatieproducten en het uitgeven van deze producten aan media, publiek, organisaties en andere overheden

2.4 Basisregistraties

Basisregistraties bevatten de meest gevraagde en gebruikte overheidsgegevens. Er zijn 13 basisregistraties, die samen het Stelsel van basisregistraties vormen.[13] Een basisregistratie is een informatiesysteem dat alle overheden verplicht gebruiken. In het stelsel staan gegevens over: personen, bedrijven, adressen, verblijfplaatsen en hun ligging (percelen en topografie), voertuigen, lonen, arbeids- en uitkeringsverhoudingen, inkomens, ondergrond, de waarde van onroerende zaken.

De 13 basisregistraties wisselen onderling gegevens uit. Gegevensverstrekking vindt plaats via het systeem Digilevering. Gegevensuitwisseling vindt plaats via Digikoppeling. Alle overheden moeten voor de uitvoering van hun publieke taken gebruik maken van gegevens uit het Stelsel van basisregistraties. Dat betekent dat alle gemeenten, alle provincies, alle waterschappen, alle zelfstandige bestuursorganen en overige organisaties met een publieke taak gebruik maken van de basisregistraties.[14]

In overleg met leden van de Programmaraad van het stelsel van basisregistraties is overeengekomen dat niet alle basisregistraties als vitaal kunnen worden aangemerkt. Het onderzoek heeft zich gericht op de basisregistraties: GBA, NHR, BAG en BRK. Voor de andere basisregistraties geldt dat er of met kopieën gewerkt kan worden, of het drie dagen niet beschikbaar en/of niet bereikbaar zijn, niet als vitaal kan worden aangemerkt.

De Gemeentelijke Basisadministratie Persoonsgegevens (GBA)

De gemeentelijke basisadministratie persoonsgegevens (GBA) bevat persoonsgegevens van iedereen die in Nederland woont of gewoond heeft. De overheid heeft deze gegevens nodig om bijvoorbeeld een paspoort, identiteitskaart (ID-kaart) of rijbewijs te maken. Ook gebruikt de overheid de gegevens uit de GBA om te weten wie er mogen stemmen bij verkiezingen en bij het verstrekken van uitkeringen.

---

[13] GBA - Gemeentelijke Basisadministratie van persoonsgegevens
NHR - Nieuw Handelsregister
BAG - Basisregistraties Adressen en Gebouwen (bestaat uit 2 basisregistraties)
BRT - Basisregistratie Topografie
BRK - Basisregistratie Kadaster
BRV – Basisregistratie Voertuigen
BLAU – Basisregistratie Lonen, Arbeids- en Uitkeringsverhoudingen
BRI – Basisregistratie Inkomens
WOZ – Basisregistratie Onroerende Zaken
RNI - Registratie Niet-Ingezetenen
BGT - Basisregistratie Grootschalige Topografie
BRO – Basisregistratie Ondergrond

[14] http: //www.e-overheid.nl/onderwerpen/stelsel-van-basisregistraties

De gemeente verzamelt, registreert en onderhoudt de gegevens in de GBA. Van iedere persoon is een persoonslijst aangelegd.[15] Tevens zijn er zijn gegevens die personen zelf moeten doorgeven aan de gemeente, zoals een verhuizing en de geboorte van een kind. Andere gegevens worden automatisch opgenomen of veranderd in de GBA. Als iemand bijvoorbeeld in Nederland trouwt, dan geeft de ambtenaar van de burgerlijke stand dit door aan de GBA.

De persoonsgegevens in de GBA zijn niet openbaar. Alleen overheidsorganisaties die voor de uitvoering van hun taken persoonsgegevens nodig hebben, ontvangen informatie uit de GBA. Dit geldt bijvoorbeeld voor de Belastingdienst en de Sociale Verzekeringsbank (SVB).[16] Zie voor meer details de Wet gemeentelijke basisadministratie persoonsgegevens.

De landelijke infrastructuur van de GBA is de verantwoordelijkheid van het ministerie van Binnenlandse Zaken (BZK). Het beheer is in handen van het agentschap Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) van BZK.

Nieuw Handelsregister (NHR)

Het nieuwe Handelsregister (NHR) is de basisregistratie van gegevens van ondernemingen en rechtspersonen. De Kamer van Koophandel beheert het NHR. Met het NHR zijn de registratie gegevens van ondernemingen en rechtspersonen vastgelegd op één plaats. Voorts hoeven ondernemers de basisgegevens die ze aan de Kamer van Koophandel hebben verstrekt niet nogmaals aan andere overheidsinstanties te geven.
Er is een handelsregister van ondernemingen en rechtspersonen:[17]

- ter bevordering van de rechtszekerheid in het economisch verkeer.
- voor de verstrekking van de gegevens [...] omtrent de samenstelling van ondernemingen en rechtspersonen ter bevordering van de economische belangen van handel, industrie, ambacht en dienstverlening.
- voor het registreren van alle ondernemingen en rechtspersonen als onderdeel van de gegevenshuishouding die bijdraagt aan het efficiënt werken van de overheid.

Basisregistratie Adressen en Gebouwen (BAG)

De Basisregistratie Adressen en Gebouwen (BAG) is een registratie waarin gemeentelijke basisgegevens over alle gebouwen en adressen in Nederland zijn verzameld.

De basisregistratie Gebouwen is een registratie van alle panden, verblijfsobjecten, standplaatsen en ligplaatsen in Nederland. De registratie is objectgericht opgezet: zowel administratieve gegevens als geometrisch gegevens (de kaart) maken integraal onderdeel uit van de registratie. Voor een aanduiding van de in de registratie opgenomen adresseerbare objecten (verblijfsobject, standplaats en ligplaats) wordt een relatie gelegd met de adressen in de basisregistratie Adressen. De in de basisregistratie Gebouwen

---

[15] Op uw persoonslijst staan bijvoorbeeld gegevens over: uw naam, voornamen, geboortedatum, geboorteplaats en geboorteland; uw verblijfplaats (adres); uw burgerservicenummer (BSN); uw ouders; uw nationaliteit en eventueel uw verblijfsrecht; uw huwelijk of geregistreerd partnerschap; uw kinderen; uw reisdocumenten; uw kiesrecht; de organisaties waaraan uw gegevens worden verstrekt.

[16] http: //www.e-overheid.nl/onderwerpen/stelsel-van-basisregistraties
[17] Artikel 2 Handelsregisterswet 2007

opgenomen objecten representeren als zodanig een ruimtelijke locatie. Zie voor meer details de Wet gemeentelijke basisadministratie adressen en gebouwen.

Het Kadaster beheert de Landelijke Voorziening BAG en stelt de gegevens beschikbaar aan overheden, bedrijven, instellingen en burgers. De BAG biedt een adressenbestand dat gebruikt kan worden om na te gaan of de adressen daadwerkelijk bestaan om te verifiëren of de bestaande adressen zijn opgegeven.

Basisregistratie Kadaster (BRK)

De Basisregistratie Kadaster omvat de landelijk kadastrale kaart en de beschrijving van de authentieke gegevens van de objecten: onroerende zaak; zakelijk recht; hypotheek en beslag. Ook wordt de verwijzing naar de verschillende brondocumenten (stukken) omschreven. Het Kadaster beheert de BRK en heeft als doel:

- de bevordering van rechtszekerheid ten aanzien van registergoederen in het rechtsverkeer, economisch verkeer en in het bestuurlijk verkeer tussen burgers en bestuursorganen.
- de bevordering van doelmatige geo-informatie-infrastructuur.
- een doelmatige informatievoorziening van de overheid ten behoeve van de goede vervulling van publiekrechtelijke taken en de nakoming van wettelijke verplichtingen door bestuursorganen.
- ondersteuning en bevordering van economische activiteiten.

Zie voor meer details de Kadasterwet en de Wet basisregistraties kadaster en topografie.

Het beschikbaar hebben van respectievelijk de GBA, NHR, BAG en BRK is van belang in verband met enerzijds de wettelijke verantwoordelijkheid up to date gegevens te hebben en anderzijds de continuïteit van de processen die afhangen van deze vier basisregistraties. De overheid werkt bijvoorbeeld niet zonder actuele GBA. Het verstrekken van onjuiste informatie aan partijen zoals politie en justitie kan desastreuze gevolgen hebben.

De *kritische processen* van de basisregistraties zijn:

- de beschikbaarheid van up to date gegevens
- de bereikbaarheid van de gegevens om mutaties in te kunnen voeren

Voor de GBA geldt dat afnemers verplicht zijn de authentieke gegevens van Nederlandse burgers af te nemen van de GBA. Zij mogen geen eigen kopie van GBA gegevens aanleggen, tenzij deze synchroon loopt aan de GBA. Een kopie bevat mogelijk verouderde gegevens. Gegevens zijn theoretisch gezien na één minuut verouderd.

2.5 Gerelateerde ontwikkelingen

De weerbaarheid van het Rijk tegen uitval van elektriciteit en telecommunicatie speelt ook bij andere actuele projecten: namelijk het project Continuïteit en de ICT Response Board.

Project continuïteit

Met de slogan 'Bent u voorbereid op uitval van elektriciteit of ICT?' zijn overheids- en hulpverleningsdiensten door minister Opstelten gevraagd in 2011 continuïteitsplannen op te stellen ten aanzien van elektriciteit en ICT-uitval. Het kabinet heeft het doel geformuleerd dat eind 2011 80% van de vitale organisaties in de sectoren Openbaar Bestuur en Openbare Orde en Veiligheid beschikt over een continuïteitsplan waarin het scenario van grootschalige verstoring van telecommunicatie en elektriciteit is opgenomen. Communicatiemateriaal is gemaakt en schrijfsessies om de continuïteitsplannen te maken zijn georganiseerd voor het Rijk, de Provincies, Gemeenten, Waterschappen, Politie- en Veiligheidsregio's. Het projectteam van CAET heeft haar stappen met het Project Continuïteit afgestemd, zodat de trajecten optimaal op elkaar aansluiten. De uitkomsten van het CAET traject dienen als input voor het opstellen van deze plannen.

ICT Response Board

Het functioneren van ICT en Telecom is fundamenteel voor de Nederlandse samenleving. Uit de Nationale Risicobeoordeling is gebleken dat een grootschalige sectoroverstijgende ICT crisis een grote impact impact op de maatschappij zal hebben, en dat hiervoor een adequate responscapaciteit voor nodig is. Met de instelling van de ICT Response Board (IRB) wordt een ontbrekende schakel in adequate crisisbeheersing opgevuld.

De ICT Response Board is een publiek-privaat samenwerkingsverband dat tijdens een grootschalige ICT-crisis of dreiging, waarbij de nationale veiligheid in het geding is, een analyse maakt van de crisis. Indien nodig brengt de IRB een advies uit over te nemen maatregelen aan beslissers binnen de Nationale Crisisstructuur en aan de vitale sectoren.

3 Weerbaarheid tegen uitval telecommunicatie en elektriciteit

3.1 Diplomatieke communicatie

Telecommunicatie
Het datacommunicatieverkeer van het diplomatieke postennetwerk loopt over gehuurde lijnen van één telecommunicatie aanbieder, welke een zeer hoge beschikbaarheid garandeert. Nederland heeft een eigen bandbreedte op deze lijnen. Een deel van de verbindingen gaat via satellieten. Met de telecom aanbieder wordt continu gesproken over de mogelijkheden ter verbetering en optimalisering van de verbindingen. Mochten de diensten van deze telecommunicatie aanbieder uitvallen beschikt het postennetwerk over verschillende achtervang communicatiemiddelen voor data en spraak.

Het postennetwerk beschikt over BGAN van Gannexxion. Dit zijn kleine satellietschotels waarmee zowel data- of spraakverkeer opgestart kan worden. Back-up voor spraakverkeer is satelliettelefonie. Aanvullend beschikt het postennetwerk over satelliettelefoons van verschillende satelliettelefonie aanbieders. Noodnet is het achtervang communicatiemiddel voor communicatie tussen bestuurders in Nederland. Een internationaal Noodnet bestaat niet. Tot slot heeft het ministerie van Buitenlandse Zaken met Europese partners afspraken gemaakt over het gebruik van elkaars communicatiemiddelen in nood- of crisissituaties.[18]

De 24/7 meldkamer van het ministerie van Buitenlandse Zaken heeft zowel digitale als hardcopy oproeplijsten tot haar beschikking. Een openstaand punt is echter het oproepen van besluitvormers en essentieel personeel buiten kantoortijden. Het is niet vastgelegd hoe de crisisbeleidsadviseur, DG en minister te bereiken is bij uitval van telecommunicatie buiten kantooruren.

Elektriciteit
Het ministerie van Buitenlandse Zaken beschikt over noodstroomaggregaten (NSA) voor de kritische processen en informatiesystemen. Bij uitval van elektriciteit in Den Haag slaat automatisch het NSA (UPS) aan. De NSA worden jaarlijks getest (ook op automatisch aanslaan). Het ministerie heeft recent elektriciteituitval ervaren, waarbij de NSA hebben gewerkt. Er is voldoende dieselolie aanwezig om de NSA meer dan drie dagen te kunnen laten draaien.

Voor het postennetwerk is het belangrijk dat de telecommunicatie aanbieder elektriciteit heeft. De *service level agreements* garanderen een beschikbaarheid van 99,8%. In landen waar regelmatig (Afrika, Zuid-Amerika, Azië) de stroom uitvalt beschikken de posten over een noodstroomaggregaat. In landen waar stroomuitval niet wordt verwacht (voornamelijk Westerse landen) beschikken posten niet over een NSA.

3.2 Besluitvorming openbaar bestuur Rijk

Telecommunicatie
Nationale crisisbesluitvorming wordt ernstig bemoeilijkt bij het niet beschikken over telecommunicatie. Beeldvorming is naast oordeelsvorming een belangrijk stap voordat besluitvorming kan plaatsvinden. Beelden komen bij het Nationaal Crisiscentrum (NCC) en de Departementale Crisiscentra (DCC's) binnen via

[18] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2005). Rapport Bescherming Vitale Infrastructuur.

telecommunicatie. Het NCC en de DCC's zijn zich hiervan bewust en beschikken in verschillende mate over achtervang communicatiemiddelen.

De achtervang van spraakverkeer is noodnet. Enkele partners van het NCC en DCC beschikken echter niet over noodnet. Achtervang voor datacommunicatie is, bij uitval van internet, de fax. Het NCC en enkele crisisrijke departementen beschikken naast noodnet en de fax tevens over satelliettelefoons. Respondenten noemen koeriersdiensten ook als achtervang bij uitval van elektriciteit en telecommunicatie. Dit is bij het NCC vastgelegd als achtervang maatregel.

Tot slot hebben het NCC en de DCC's een uitwijklocatie, mocht de telecommunicatie-uitval zeer lokaal zijn. Openstaand punt is hier ook het oproepen van besluitvormers en essentieel personeel buiten kantoortijden. Het is niet vastgelegd hoe de crisisbeleidsadviseur, DG en minister te bereiken is bij uitval van telecommunicatie buiten kantooruren. Ook hier noemen respondenten koeriers- en/of chauffeursdiensten als mogelijke achtervang. Bij het NCC zijn koeriersdiensten vastgelegd als achtervang middel. Niet bij alle DCC's en het NCC zijn echter de thuisadressen van de medewerkers bekend. Het NCC heeft wel de thuisadressen van belangrijke spelers, zoals de ministers. Een enkel DCC heeft voor haar crisiscoördinatoren thuis een noodnet aansluiting, zodat de crisiscoördinatoren buiten kantoor bereikt kunnen worden, mits ze thuis zijn.

Een belangrijk punt is dat ambtelijke (Adviesteam/ICCb) en politiek-bestuurlijke (MCCb) crisisbesluitvorming plaatsvindt indien daar aanleiding voor is. Bij een grootschalige uitval van telecommunicatie zullen DCC's en het NCC opschalen, omdat de uitval ook de vitale sectoren zal raken. De recent opgerichte ICT Response Board (IRB) is bij grootschalige telecommunicatie uitval een belangrijke schakel op Rijksniveau. Zowel private als publieke partijen hebben zitting in de IRB en zullen de nationale crisisstructuur van advies voorzien.

Elektriciteit
Alle DCC's en het NCC beschikken over noodstroomaggregaten (NSA) die bij uitval van elektriciteit automatisch aanslaan. Tevens geldt hier dat de DCC's en het NCC over een uitwijklocatie beschikken. De uitwijklocaties hebben eveneens NSA. Het verschilt per departement voor hoeveel dagen dieselvoorraad voor de NSA aanwezig is bij de departementen en uitwijklocaties. De frequentie van het testen van de NSA (ook op automatisch aanslaan) verschilt tevens per departement.

3.3 Informatieverstrekking overheid

Telecommunicatie
Grootschalige telecommunicatie (vast, mobiel en internet) uitval in Nederland zal voor onrust in de samenleving zorgen. Het NCC en de regionale hulpverleningsdiensten zullen waar mogelijk aan informatievertrekking aan de samenleving doen om onrust te voorkomen. De informatievoorziening richting de samenleving wordt echter bemoeilijkt, omdat de samenleving gewend is informatie te ontvangen via telecommunicatieverbindingen. Tevens maakt de overheid in toenemende mate gebruik van (sociale) media berichten via telecommunicatielijnen om de samenleving te informeren.

Aannemelijk is dat de informatievoorziening naar de burger toe via regionale hulpverleningsdiensten verloopt, waarbij het cRC NCC of het NVC optreedt als adviseur van de regio's.

Het NCC beschikt zelf over dubbele telecommunicatie lijnen en heeft noodnet als achtervang. Via noodnet kan het NCC met behulp van spraakverkeer communiceren met bestuurlijke partners op nationaal en regionaal niveau. Bij

uitval van telecommunicatie zal het NCC waarschijnlijk minder informatie binnenkrijgen (omdat informatieleverende partijen ook problemen ondervinden van de uitval), wat het opstellen van het advies aan bijvoorbeeld de regio's bemoeilijkt. Naast crisiscommunicatie adviezen stelt het cRC NCC/ NVC omgevingsanalyses op en drukt uit wat er speelt en leeft in de buitenwereld en hoe daarop te reageren. Zonder telecommunicatie is het lastig om informatie voor een omgevingsanalyse binnen te krijgen.

Het is niet vastgelegd hoe de crisiscommunicatie adviseurs te bereiken buiten kantoortijden in het geval de telecommunicatie is uitgevallen. Voor het nieuwe NVC (90 personen) is besloten het oproepen tot opschalen per P2000 te laten plaatsvinden.

Tot slot is DARES (Dutch Amateur Radio Emergency Service) een officiële back up telecomvoorziening bij rampen en crisisomstandigheden. Deze stichting heeft zichzelf ten doel gesteld dat, wanneer communicatievoorzieningen uitgevallen zijn, bijvoorbeeld als gevolg van langdurige elektriciteitsuitval of van een overstroming, radiozendamateurs een waardevolle bijdrage kunnen leveren. DARES kent een landelijk netwerk van inzetbare radiozendamateurs en heeft de beschikking over meerdere mobiele units met eigen stroomvoorziening en eigen zend- en ontvangstfaciliteiten. Overheidspartijen hebben afspraken met DARES gemaakt over hun mogelijke rol bij genoemde scenario's.

Elektriciteit
Indien de overheid bij grootschalige uitval van elektriciteit in crisiscommunicatie wil voorzien, is het zenden van de boodschap niet het probleem, maar het kunnen ontvangen van de boodschap. Het NCC en DCC's beschikken over voldoende NSA om de bedrijfsvoering doorgang te laten vinden om analyses en adviezen op te kunnen stellen. De samenleving zal echter moeilijkheden ondervinden om de boodschap bij uitval van elektriciteit te ontvangen.

3.4 Basisregistraties

Voor de beschikbaarheid van up to date gegevens en de bereikbaarheid van de gegevens om mutaties te kunnen doen is telecommunicatie verbinding van essentieel belang. Zonder elektriciteit is er geen beschikbaarheid van up to date gegevens en geen bereikbaarheid van de gegevens om mutaties te kunnen doen.

3.4.1 De Gemeentelijke Basisadministratie Persoonsgegevens (GBA)

Telecommunicatie

16.1.C

GBA heeft een eigen besloten *dedicated* netwerk. [redacted]. Op dit netwerk zitten de gemeenten, die onder andere nieuwe GBA gegevens invoeren en mutaties doorvoeren op persoonslijsten, en een centrale GBA Verstrekkingsvoorziening (GBA-V). De GBA-V is een centrale voorziening en beschikt over een kopie van alle gegevens uit de GBA. Het netwerk en de beheervoorziening van GBA-V wordt via Britisch Telecom ontsloten aan [redacted]

Bij uitval van [redacted] kunnen gegevens niet meer worden gemuteerd met als gevolg dat de actualiteit van de gegevens achterloopt. Tevens vindt berichtenverkeer van naar partners niet plaats. De GBA verzorgt circa 130 miljoen berichten per jaar.

Uitval van korter dan 24 uur is geen probleem, uitval langer dan 24 uur wel. Dan is er geen actuele dataset. Afnemers zouden dan oude gegevens krijgen. Bij het wegvallen van het berichtenverkeer worden bijvoorbeeld pasgeboren kinderen niet opgeroepen voor een verplichte hielprik.

10.1.C [redacted] en [redacted] zeggen een hoge beschikbaarheid toe. Dit zegt echter onvoldoende over hun weerbaarheid tegen uitval van elektriciteit en telecommunicatie. BPR is naar aanleiding van dit onderzoek navraag aan het doen naar de weerbaarheid van zowel [redacted] als [redacted]

Elektriciteit
Het GBA netwerk heeft twee datacenters die voor de continuïteit van de GBA bij elektriciteituitval moeten blijven draaien. De datacenters hebben de kwalificatie 'Tier III'[19] . Deze kwalificatie garandeert een 99,982% beschikbaarheid. Alles is dubbel uitgevoerd. Voorts heeft het datacenter voor het berichtenverkeer een uitwijklocatie. Deze heeft dezelfde back-up condities en ligt 15 km verderop. Onduidelijk is echter of 15 km afstand de continuïteit garandeert.

Om bij elektriciteituitval te kunnen blijven draaien zijn er voor de datacenters back-up voorzieningen aanwezig: accu's, 2 noodstroomaggregaten (NSA) (1 daarvan is back-up) en diesel voor 8 dagen. Voorts is er een contract met Shell afgesloten dat er bij aanvraag binnen 4 uur diesel is.
Aanvullend worden de datacenters jaarlijks getest en geaudit.

Het datacenter met de GBA-V heeft een uitwijklocatie. Deze heeft dezelfde condities en ligt op 20 km afstand. Beide locaties zijn voorzien van N+1 faciliteiten, dat wil zeggen dat alle faciliteiten zijn uitgevoerd in de benodigde capaciteit inclusief minimaal één volwaardig reserve. De volgende back-up voorzieningen zijn aanwezig: UPS, NSA (1 daarvan is back up) en diesel voor 48 uur. De dieselleverancier levert bij aanvraag binnen 8 uur.

10.1.C Een tweede back-up voor de GBA-V is het opvragen van gegevens niet bij de GBA-V maar bij de individuele gemeenten rechtstreeks via [redacted]

3.4.2 Nieuw Handelsregister (NHR)

Telecommunicatie
Voor de beschikbaarheid en de bereikbaarheid van het NHR is internet verbinding en de continuïteit van het datacenter randvoorwaardelijk.

Het NHR draait op één productie datacenter. Mocht het productie datacenter uitvallen, beschikt NHR over een uitwijk datacenter. Bij uitval van het productie datacenter wordt 24 uur 'data(mutatie)achterstand' geaccepteerd. In een *service level agreement* met het ministerie EL&I is opgenomen dat er in geval van een calamiteit een maximale *down*tijd van 24 is toegestaan. Daarnaast geldt ook een maximaal dataverlies van 24 uur.

De fysieke bekabeling van het NHR netwerk tussen de datacenters en de KVK kantoren is dubbel uitgevoerd. Bij kantoren komt de aansluiting op NHR van twee kanten binnen (van twee kanten gevoed).

Bij uitval van het systeem kan er geen informatie meer worden verstrekt en kan nieuwe informatie niet worden gemuteerd. Dit moet dan me de hand ipv de centrale vastlegging.

---

[19] Tier 1 tot en met 4 is een gestandaardiseerde methodologie om de beschikbaarheid van een datacenter weer te geven. Een Tier 4 datacenter is gedefineerd als 'most robust and less prone to failures'.
Tier 1: Guaranteeing 99.671% availability.
Tier 2: Guaranteeing 99.741% availability.
Tier 3: Guaranteeing 99.982% availability.
Tier 4: Guaranteeing 99.995% availability.
Zie voor meer informatie: o.a. http://www.cyberciti.biz/faq/data-center-standard-overview/

Mochten beide lijnen uitvallen dan heeft [redacted] de mogelijkheid een straalzender op locatie te plaatsen. Middels een satellietverbinding wordt dan een WAN verbinding aangeboden. Deze heeft een lagere bandbreedte dan de vaste lijnverbinding. Dit gebeurt echter pas nadat op beide locaties de redundante aansluiting niet beschikbaar is. 10.1.C

Bij uitval van internet kunnen ondernemers geen gegevens aan NHR verstrekken en kan de overheid NHR niet raadplegen. Het fysiek aandoen van een KVK kantoor is hiervoor het alternatief.

Elektriciteit
Het productie datacenter en de uitwijk datacenter zijn Tier III uitgevoerd. Het beheer is uitbesteed aan een externe partij waarmee SLA's zijn afgesproken over de beschikbaarheid.

De twee datacenters beschikken over meerdere noodstroom aggregaten (NSA's) met minimaal 2 dagen aan dieselolie. Verder zijn er voor de dieselleverantie contracten afgesloten. De NSA's worden vier keer per jaar getest.

Voorts fungeert het ene datacenter als uitwijk voor de andere. Werknemers kunnen vanaf alle locaties werken en zijn onafhankelijk van het kantoor. Eventuele uitwijk is thuis of een andere kantoor. KVK kantoren hebben geen NSA.

3.4.3 Basisregistratie Adressen en Gebouwen (BAG)

Telecommunicatie
Naast de BAG voorziening bij de gemeenten is er de Landelijke Voorziening BAG. De Landelijke Voorziening BAG is in het beheer van het Kadaster. Gemeenten hebben voor het borgen van de BAG een toelatingsaudit gedaan en een beheeraudit volgt. Bij de toelatingsaudit is gekeken of de processen voldoende zijn ingeregeld en de gegevens van voldoende kwaliteit zijn. Ook is de ICT voorziening getoetst. Voorts dienen gemeenten mutaties van de BAG binnen vier dagen verwerkt te hebben.

Afnemers kunnen op vier manieren BAG gegevens verkrijgen: via BAG web, BAG extract, BAG compact en BAG bevragingen. Hiervoor is telecommunicatieverbinding randvoorwaardelijk. Het fysiek aandoen van een gemeente is hiervoor het alternatief.

Bij uitval van de landelijke voorziening BAG kunnen gegevens bij de gemeente worden opgevraagd en bij uitval van de gemeente kunnen de gegevens bij de landelijke voorziening BAG worden opgevraagd. Voorts bestaat de mogelijkheid om een kopie te gebruiken. Een gemeente zal de mutaties na de uitval weer oppakken.

Elektriciteit
BAG gegevens zijn bij zowel gemeenten als bij de landelijke voorziening aanwezig. Bij uitval van elektriciteit bij gemeenten zijn BAG gegevens op te vragen bij de landelijke BAG voorziening en andersom. De landelijke voorziening heeft een uitwijk datacenter dat binnen 24 uur in gebruik kan worden genomen. Voorts beschikt het datacenter van de landelijke voorziening over noodstroomaggregaten en afspraken met dieselleveranciers.

3.4.4 Basisregistratie Kadaster (BRK)

Telecommunicatie
Bij uitval van telecommunicatie is het Kadaster niet digitaal bereikbaar en niet beschikbaar voor digitale mutaties. Bijvoorbeeld transacties komen dan niet

binnen bij het Kadaster. Een alternatief is het doorgeven van de wijzigingen per brief. De wijzigingen worden dan ingescand en later in het systeem verwerkt.

Bij het niet hebben van actuele gegevens kan een huis niet worden verkocht, omdat deze mutatie niet bij BRK kan worden opgenomen. Het huis zou in dit geval meerdere keren verkocht kunnen worden zonder dat dit in de registraties zichtbaar is.

10.1.C Het kadaster beschikt over eigen interne huurlijnen van [redacted] en heeft beschikbaarheidsafspraken met [redacted] gemaakt. Notarissen hebben echter internet nodig om wijzigingen door te geven.

Voor BKR beschikt het kadaster over twee data centers. Waarbij het tweede datacenter binnen 24 uur als uitwijk datacenter in gebruik worden genomen.

Naast dat het datacenter dubbel is uitgevoerd zijn de verbindingen daar naartoe ook dubbel uitgevoerd. Dit geldt ook voor de uitwijklocatie. Hiernaast is het netwerk waar gegevens op staan[20] ook dubbel uitgevoerd. Voor de Automatische Kadastrale Registratie (AKR) is eveneens een beschikbaarheidscontract afgesproken.

Elektriciteit
Voor het beschikbaar hebben van de BRK gegevens is de continuïteit van de datacenters van groot belang. Beide datacenters beschikken over noodstroomaggregaten (NSA) en hebben afspraken met dieselleveranciers.

De brenger van de informatie (bijvoorbeeld de notaris) kan de informatie echter niet meer versturen. Aktes kunnen niet worden gemuteerd. Eventueel kan er worden teruggevallen op handmatig proces en wordt er met stempels gewerkt.

Kadaster kantoren (6 in Nederland) hebben geen NSA. Bij uitval van één kantoor, neemt een ander kantoor het over.

[20] Standard Area Network (SAN)

4 Mogelijk aanvullende maatregelen

4.1 Diplomatieke communicatie

Het diplomatieke postennetwerk is zeer redundant uitgevoerd. Op verschillende manieren kan communicatie met diplomatieke posten plaatsvinden. Voorts is het een netwerk over de gehele wereld en zal het nooit in zijn geheel uitvallen. Mogelijk brengt bij uitval van telecommunicatie het contact leggen praktische problemen met zich mee, omdat er met achtervang communicatiemiddelen gewerkt. In het uiterste geval kunnen ook mensen boodschappen overbrengen door naar de desbetreffende post af te reizen. Om de redundantie te behouden en mogelijk te bevorderen is het volgende aan te bevelen:

- *Bestudeer de service level agreements met de aanbieder van de telecommunicatieverbindingen kritisch. In hoeverre blijft deze ook werken bij bijvoorbeeld elektriciteituitval.*
- *Overweeg om voor alle posten noodstroomaggregaten aan te schaffen.*
- *Leg vast hoe met elkaar te communiceren bij het wegvallen van een communicatiemiddel.*

4.2 Besluitvorming openbaar bestuur Rijk en informatieverstrekking overheid

Uitval telecommunicatie
Grootschalige telecommunicatie (vast, mobiel en internet) uitval is aan de ene kant een probleem voor de (crisis)organisaties op Rijksniveau en aan de andere kant een probleem voor de samenleving. Hiernaast is het de taak van de overheid de samenleving te informeren over de grootschalige uitval. De huidige samenleving is zeer afhankelijk van telecommunicatie.

Uit de interviews blijkt dat de overheid alternatieve communicatieprotocollen richting de samenleving (nog) niet hebben vastgelegd. Geopperd is de crisisbesluitvorming te laten ondersteunen door koeriers; en de crisiscommunicatie aan de burger zou bijvoorbeeld via geluidswagens of radioverbinding plaatsvinden. Voorts geldt, zo is de inschatting van respondenten, dat de burger niet voorbereid is op het kunnen ontvangen van de alternatieve wijze van berichtgeving.

De overheid heeft achtervang communicatiemiddelen om met elkaar te communiceren. Het wordt enerzijds echter lastig om informatie in te winnen, omdat informatieleverende partijen ook last zullen ondervinden van de telecommunicatie uitval. Anderzijds is het de vraag of de crisisbesluitvorming en de benodigde crisiscommunicatie met de samenleving gedeeld kan worden.

Respondenten geven aan dat de *service level agreements* met de telecommunicatie aanbieder niet altijd even duidelijk zijn. Een hoge beschikbaarheid wordt gegarandeerd, maar wat doet de telecommunicatie aanbieder om hieraan tegemoet te kunnen komen?

- *Ga in gesprek met de telecommunicatie aanbieder en vraag om verduidelijking van de service level agreements. En vraag bij het afsluiten van nieuwe abonnementen naar robuustheid van de verbinding en alternatieven.*

Houd als Rijk rekening met het scenario uitval van telecommunicatie. Op dit moment stelt het Rijk continuïteitsplannen voor uitval van ICT op en is de ICT Response Board ingericht. Overweeg de volgende punten mee te nemen bij het opstellen van het continuïteitsplan:

- *Exploreer de mogelijkheden hoe (crisis)besluitvormers en –voorbereiders (buiten kantoortijd) gealarmeerd kunnen worden, wanneer telecommunicatie is uitgevallen. Hoe en door wie wordt het crisisteam bij elkaar geroepen?*
- *Maak afspraken met alternatieve informatie leverantie mogelijkheden, zoals afspraken met koeriers en leg deze vast.*
- *Maak afspraken met (informatieleverende) partners hoe met elkaar te communiceren bij uitval van telecommunicatie.*
- *Oefen samen met (informatieleverende) partners met het scenario telecommunicatie uitval.*
- *Bedenk hoe medewerkers van (crisis)organisaties ontzorgt en gecompenseerd kunnen worden, zodat zij met een gerust hart hun werk kunnen doen en zich geen zorgen maken of en hoe hun naasten zich redden bij een grootschalige uitval van telecommunicatie en/ of elektriciteit.*

Noodnet is een belangrijke achtervang communicatiemiddel voor bestuursorganen. Over de nieuwe Nood Communicatie Voorziening (NCV) (de opvolger van noodnet) bestaat echter veel verwarring. Voor de respondenten is het niet duidelijk wat deze omschakeling precies betekent en of de weerbaarheid hiermee gewaarborgd blijft.

- *Bedenk als Rijk wat een wenselijke noodcommunicatie voorziening is. Voorbeelden uit het buitenland (Engeland, Zweden en Amerika) kunnen hierbij helpen.*
- *Aanbeveling aan het ministerie van VenJ om met de huidige noodnet abonnees duidelijk te communiceren wat de status van het NCV is.*
- *De (crisis)organisaties dienen op hun beurt te inventariseren of hun partners ook overstappen naar hetzelfde abonnement, zodat deze partijen met elkaar kunnen communiceren via dezelfde noodcommunicatievoorziening.*

De samenleving verwacht informatieverstrekking van de overheid bij grootschalige uitval van een vitale sector, zoals telecommunicatie. De reactie en het advies van de overheid op zo een moment is nog niet uitgewerkt.

- *Versterk zelfredzaamheid van burgers en bedrijven door voorlichting te geven over wat te doen bij uitval van telecommunicatie en wat te verwachten van de overheid.*
- *Werk het scenario drie dagen zonder telecommunicatie voor de samenleving uit. Denk aan:*
    - *Het maken van afspraken tussen Rijk en Regio hoe met de samenleving te communiceren, bijvoorbeeld m.b.v. communicatiekaarten. Wat zijn de landelijk geldende generieke berichten en wat zijn de specifieke berichten voor die regio?*
        - *Voorbeeld voorlichting in getrapte vorm: MCCb doet verzoek aan regio's consequent 'het volgende' uit te dragen (bv. schakel uw regionale rampenzender op de radio in). Aanvullend zullen regio's voorlichting geven over regionale zaken (boodschap is plaatsafhankelijk).*
    - *Welke communicatiemiddelen heb je als overheid bij welk scenario? Dit kan per regio verschillen.*
- *Voor het NCC is een belangrijke taak weggelegd na de drie dagen. Hoe de samenleving na deze drie dagen voorlichten? Hier kan nu alvast over nagedacht worden. De boodschap na de drie dagen is van groot belang voor de Rijksoverheid. Tijdens deze drie dagen is de boodschap plaatsafhankelijk.*

Uitval elektriciteit
De betrokken overheidsdiensten beschikken over noodstroomaggregaten (NSA) met voldoende dieselolie voor de kritische processen en informatiesystemen. Tevens beschikken de departementale crisiscentra (DCC's) en het Nationaal Crisiscentrum over een uitwijklocatie. De achtervang faciliteiten zorgen ervoor

dat de kritische processen van de vitale diensten doorgang kunnen hebben bij grootschalige elektriciteituitval. Grootschalige uitval van elektriciteit heeft grote gevolgen voor de samenleving. Bovendien verwacht de samenleving coördinatie en informatie vanuit de overheid. Met het project Vitale Partnerschappen hebben veiligheidsregio's convenanten afgesloten met elektriciteitsleveranciers, zodat de partijen weten wat te doen bij elektriciteituitval en hoe ze elkaar kunnen bijstaan. Maar wat is de rol van de rijksoverheid bij grootschalige elektriciteituitval? En wat is de eigen verantwoordelijkheid van de samenleving?

- *Houd de continuïteit van het rijk bij elektriciteituitval op orde door:*
  - *NSA regelmatig te testen en onderhoud te plegen. Geopperd is hier het Directoraat-Generaal Organisatie en Bedrijfsvoering Rijk (DG OBR) hier een coördinerende rol in de te laten vervullen;*
  - *te oefenen met het scenario elektriciteituitval;*
  - *te weten wat de rol van de rijksoverheid is bij grootschalige elektriciteituitval.*
- *Versterk zelfredzaamheid van burgers en bedrijven door voorlichting te geven over wat te doen bij uitval van elektriciteit wat te verwachten van de overheid.*
- *Weet als vakdepartement wat grootschalige elektriciteituitval doet met de vitale sectoren. Maak met vitale sectoren afspraken over hoe te reageren op grootschalige elektriciteituitval.*

4.3 Basisregistraties

Basisregistraties zijn op meerdere plaatsen beschikbaar wat de redundantie verhoogd. Voor het verwerken van mutaties en het opvragen van gegevens is telecommunicatie verbinding echter onmisbaar. Eventuele achtervang is het uitstellen van mutaties of opvragen van gegevens bij gemeenten, kamer van koophandel of het kadaster. Tijdens de interviews kwam naar voren dat drie dagen uitval van elektriciteit en/ of telecommunicatie voor NHR, BAG en BRK mogelijk te overzien is en niet in alle gevallen te koppelen is aan de definitie van vitale infrastructuur[21]. Uitval van langer dan drie dagen lijkt grotere problemen te veroorzaken. Voorts is het voor de continuïteit van basisregistraties van belang dat datacenters van stroom zijn voorzien. Voor de basisregistraties GBA, NHR, BAG, BRK geldt dat de datacenters noodstroomaggregaten hebben en over een uitwijklocatie beschikken. Aanvullend bestaan er meerdere kopieën van de deze basisregistraties. De beheerders van de basisregistraties zijn zich bewust van het belang van de continuïteit van de basisregistraties en hebben verschillende maatregelen genomen om de continuïteit te waarborgen.

Het bespreken van basisregistraties als onderdeel van een vitale sector is nieuw. De gevolgen van uitval van de basisregistraties heeft verschillende onwenselijke gevolgen. Uit interviews blijkt echter dat nog niet is uitgedacht wat de gevolgen precies zijn en tot welke onwenselijkheden het zal leiden. De inschatting van de respondenten is dat een uitval van 3 dagen niet direct tot grootschalige ontwrichting van de samenleving zal leiden. De basisregistraties vormen een onderdeel van verschillende ketens. Nog niet duidelijk is wat er precies met de ketens gebeurd en hoe de ketens op uitval van telecommunicatie en/of elektriciteit zullen reageren.

---

[21] *Vitale infrastructuren zijn 'die producten, diensten en processen die, als zij uitvallen, maatschappelijk of economische ontwrichting van (inter-)nationale omvang kunnen veroorzaken, doordat er veel slachtoffers kunnen vallen en/of omdat het herstel zeer lang gaat duren en er geen reële alternatieven voorhanden zijn, terwijl we deze producten en diensten niet kunnen missen'.* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2009). 2de inhoudelijke analyse bescherming vitale infrastructuur.

- Wees duidelijk naar afnemers van de basisregistratie wat uitval van telecommunicatie en/of elektriciteit betekent voor desbetreffende basisregistratie en beoordeel gezamenlijk of genomen maatregelen afdoende zijn.

5 Conclusie

De continuïteit van de vitale diensten van het openbaar bestuur zijn van groot belang voor de samenleving. Deze rapportage is gericht op weerbare

- diplomatieke communicatie: contact met buitenland
- besluitvorming openbaar bestuur rijk: functioneren van de nationale crisisbesluitvorming
- informatievertrekking overheid: media- en publieksvoorlichting in crisistijd
- basisregistraties: GBA, NHR, BAG en BRK

Verschillende maatregelen zijn genomen om de continuïteit van deze vitale diensten te waarborgen. De samenleving is afnemer van deze diensten en verwacht niet alleen dat het openbaar bestuur de continuïteit van hun eigen organisatie hebben gewaarborgd, maar ook daarmee de openbare orde en veiligheid voor de samenleving garanderen.

Geconcludeerd kan worden dat de kritische processen van deze vitale diensten met behulp van achtervang communicatiemiddelen en uitwijklocaties doorgang hebben, maar wordt de rol van de overheid en de communicatie naar de samenleving op de proef gesteld.

Samengevat:

- De weerbaarheid van diplomatieke communicatie is gewaarborgd met behulp van verschillende alternatieven voor communicatie.
- De nationale crisisbesluitvorming zal bij uitval van elektriciteit en/of telecommunicatie doorgang hebben, alhoewel zij wel hinder zullen ondervinden. Voorts is het de vraag wat de rol van de rijksoverheid is bij grootschalige uitval van elektriciteit en telecommunicatie.
- Nog niet is uitgewerkt hoe media- en publieksvoorlichting bij uitval van elektriciteit en/of telecommunicatie plaats zal vinden.
- Voor de basisregistraties GBA, NHR, BAG en BRK geldt dat uitval van elektriciteit en/of telecommunicatie kan zorgen voor niet up to date gegevens. Dit heeft gevolgen voor onder andere de rechtszekerheid.

In hoofdstuk 5 zijn aanbevelingen geformuleerd. Het kritisch bestuderen of de genomen maatregelen en/of de achtervang middelen afdoende zijn is een onderdeel hiervan. Op dit moment is het Rijk in opdracht van VenJ continuïteitsplannen aan het opstellen, waarbij benadrukt moet worden dat de continuïteitsplannen niet een doel op zich zijn, maar een middel om de weerbaarheid van het rijk te verhogen.

De ministeries van Veiligheid en Justitie en Binnenlandse Zaken hebben de opdracht met andere ministeries te bespreken hoe opvolging te geven aan de aanbevelingen.

Bijlagen

I. Respondenten interviews

Respondenten	Organisatie
[redacted]	Nationaal CrisisCentrum (NCC)
	NCC cluster Risico- en Crisiscommunicatie
	DCC Defensie
	DCC OCW en SZW
	DCC FIN
	DCC BZK
	DCC BuZa
	DCC IenM
	Logius
	BZK DRI
	[redacted]
	BPR BZK (GBA)
	IenM (BAG)
	IenM (BRK)
	[redacted]

10.2.8 10.1.C

II. Referenties CAET project

Dunn Cavelty, M. and Suter, M., Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection – International Journal of Critical Infrastructure Protection. Zurich: Center for Security Studies, 27 augustus 2009.

Ernst & Young, Afhankelijkheden vitale sectoren van de beschikbaarheid en betrouwbaarheid van de vitale (Telecommunicatie en ICT) infrastructuur, Den Haag: Ernst & Young, 6 februari 2008.

[redacted] 10.1.b

Luiijf H.A.M., Nieuwenhuijs, A.H., Kernkamp, A.C., Jong, de K.Y., Burger, H.H., Bik, A.L., Hoogstraaten, J.M., Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten (managementdeel), Den Haag: TNO, rapport FEL-03-C001, 2003.

Luiijf H.A.M., Nieuwenhuijs, A.H., Kernkamp, A.C., Jong, de K.Y., Burger, H.H., Bik, A.L., Hoogstraaten, J.M., Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten, Den Haag: TNO, rapport FEL-03-C002, 2003.

Luiijf H.A.M., Critical infrastructure dependencies hurt, don't they? - Weak spot analysis - Den Haag: TNO, 2008.

Ministerie van Binnenlandse Zaken/ BVI rapportages

[redacted] 10.1.b

NICC, Proces Control Security in het informatieknooppunt Cybercrime, Den Haag: 2009.

Programma Nationale Veiligheid, Nationale Risicobeoordeling Leidraad Methode, Den Haag: ministerie van Binnenlandse Zaken en Koninkrijksrelaties, juni 2008.

Programma Nationale Veiligheid, Nationale Risicobeoordeling Bevindingenrapportage, Den Haag: ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2008.

Programma Nationale Veiligheid, Robuustheid communicatiemiddelen tijdens crises, Den Haag: ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 1 juli 2009.

Sutton, D., Critical information infrastructure protection Interdependency between Energy and Telecommunications, ENISA Quarterly Review Vol. 5, No. 3, September 2009.