PLATFORM VOOR CYBERSECURITY
CPNI.NL

Weerbaarheid van **Openbare Orde en Veiligheid op regionaal niveau** tegen uitval van elektriciteit en telecommunicatie

Rapportage

In opdracht van de ministeries van
Veiligheid en Justitie/DG Veiligheid en
Economische Zaken, Landbouw en Innovatie/DG Energie,
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
0.9	06-07-2011	CPNI.NL	
0.97	15-07-2011	CPNI.NL	
0.98	13-09-2011	CPNI.NL	
1.0	20-09-2011	CPNI.NL	

INHOUDSOPGAVE

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 als 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 Openbare Orde en Veiligheid (OOV) op regionaal niveau. Voor de hulpverleningsdiensten zijn dit de kritische processen:

- Functioneren meldkamer
- Uitrukken en respons
- Regionale crisisorganisatie en -besluitvorming

Doorsnijdend zijn de volgende functionaliteiten van essentieel belang voor de doorgang van de kritische processen.

- Informatiemanagement
- Communicatie

Samengevat wordt het proces van hulpverlening bij grootschalige uitval van elektriciteit en/of telecommunicatie ernstig bemoeilijkt. Men rekent hier op het kunnen terugvallen op noodcommunicatiemiddelen, noodstroomaggregaten en uitwijklocaties. Voorts geven respondenten aan dat hulpverleningsdiensten over een groot improviserend vermogen beschikken.

Bij uitval van elektriciteit geldt voor de meldkamers dat er een uitwijklocaties (de meldingen worden dan doorgeschakeld) en noodstroomaggregaten (NSA) aanwezig zijn. Het verschilt per meldkamer voor hoeveel dagen dieselolie voor de NSA aanwezig is. Hetzelfde geldt voor de locatie waar regionale crisisbesluitvorming plaatsvindt.
Voorts is onduidelijk in hoeverre het wagenpark bij uitval van elektriciteit van brandstof kan worden voorzien.

Bij uitval van telecommunicatie is het de vraag of burgers en bedrijven de meldkamer kunnen bereiken, omdat ze mogelijk niet over werkende telecommunicatiemiddelen beschikken. Hulpverzoeken moeten via andere wegen de meldkamer bereiken. C2000 (met T2000 en P2000 als onderdeel) en noodnet zijn (achtervang) communicatiemiddelen voor de hulpverleningsdiensten zelf. Een enkele veiligheidsregio beschikt tevens over satelliettelefonie. Het verzamelen van informatie en crisiscommunicatie richting de burger zal ondanks de achtervang communicatiemiddelen worden bemoeilijkt.

Op basis van geïnventariseerde mogelijke aanvullende maatregelen zijn aanbevelingen geformuleerd:

Functioneren meldkamer

- Organiseer dat alle (nieuwe) meldkamers een redundante uitwijklocatie hebben.
- Advies aan politie en veiligheidregio om vantevoren te hebben nagedacht over:
    - de rol van de politie en veiligheidsregio bij grootschalige uitval van elektriciteit en telecommunicatie. Veiligheidsregio Rotterdam-Rijnmond heeft bijvoorbeeld een responsplan stroomuitval;

  - de manier hoe met de burgers gecommuniceerd zal worden en de burgers de gelegenheid krijgen een melding te doen.
- Bespreek als politie- en veiligheidsregio met vitale partners wat grootschalige uitval van telecommunicatie en/of elektriciteit voor de meldkamer kan betekenen; spreek af hoe hierop te reageren, hoe met elkaar te communiceren/ meldingen te maken en spreek uit wat men van elkaar kan verwachten in deze situatie.

Uitrukken/ respons

- Oefen als politie en veiligheidsregio regelmatig met het gebruik van noodcommunicatiemiddelen. Wissel ervaringen uit en zet ideeën voor verbetering om in aanpassingen ten opzichte van het proces en indien mogelijk de apparatuur.
- Houd voor het kunnen uitrukken van politie, brandweer en ambulance rekening met het scenario 3 dagen geen elektriciteit/ en of telecommunicatie. Zorg ervoor dat personeel met het juiste materiaal en de juiste uitrusting naar het plaats incident kan gaan. Denk bijvoorbeeld aan een wagenpark met volle tanks.
- Test als hulpdienst de noodstroom aggregaten (NSA) regelmatig, momenteel is vaak te onduidelijk of dit gebeurd.
- Oefen als hulpdiensten met een scenario met uitval van telecommunicatie zodat de kwaliteit en kwantiteit van de noodcommunicatiemiddelen worden gestest en de veronderstelde zelfredzaamheid van medewerkers juist is.

Regionale crisisorganisatie en -besluitvorming

- Inventariseer per regio welke operationele en bestuurlijke dilemma's op kunnen treden bij grootschalige telecommunicatie en/of elektriciteit uitval en win alvast informatie van experts in hoe hierop te reageren.
- Het regionaal oppakken van dit vraagstuk is sub-optimaal. Wissel interregionaal de kennis en ervaring uit.
- Stem af met het Rijksniveau wat de regio bij dit scenario van hen kan verwachten.
- Leg als politie en veiligheidsregio vast hoe crisisbesluitvormers en ander essentieel personeel te bereiken tijdens en buiten kantooruren wanneer er geen telecommunicatie verbinding (vast, mobiel, internet) mogelijk is. Denk bijvoorbeeld aan het paraat hebben van de adresgegevens van de besluitvormer om deze persoon bij uiterste nood thuis op te kunnen halen.
- Bespreek de mogelijkheid van alternatieven, zoals bijvoorbeeld het ter plaatse hebben van ROT en RBT om ook zonder telecommunicatiemiddelen op basis van adequate mondelinge informatievoorziening crises te kunnen bestrijden.
- Houd als hulpdienst bij grootschalige en langdurige uitval van elektriciteit ook rekening met uitval van telecommunicatie. Nog te vaak wordt geoefend met het scenario elektriciteitsuitval maar wordt veronderstelt dat de telecommunicatie wel gewoon operationeel is ("anders wordt het oefenen zo lastig").

Informatiemanagement

- Inventariseer de toenemende afhankelijkheid van netcentrisch werken en toets de beschikbaarheid en betrouwbaarheid van onderliggende verbindingen.

Communicatie

- Wees ervan bewust dat noodcommunicatiemiddelen mogelijk niet even toereikend zijn als de gebruikelijke communicatiemiddelen. Blijven oefenen met noodcommunicatiemiddelen is essentieel.
- Werk als veiligheidsregio uit wat alternatieve crisiscommunicatie wegen richting de samenleving kunnen zijn. Naast de geluidswagens kunnen bijvoorbeeld lokale bureaus dienen als voorlichtingsruimte.

- Stimuleer als hulpdiensten het vergroten van de zelfredzaamheid van de burger. Laat als overheidsdiensten weten wat de burger kan verwachten en wat bij grootschalige uitval van telecommunicatie alternatieve communicatiemiddelen zijn.
- Stem met partners af hoe met elkaar te communiceren en hoe informatie met elkaar te delen bij uitval van telecommunicatie.

C2000 en 112

- Investeer als UMS in uitbreiding van de nieuwe Nood Communicatie Voorziening (NCV) voor verbindingen tussen KLPD en regionale meldkamers.
- Inventariseer als beleidsverantwoordelijke welke weerbaarheidsmaatregelen meldkamers hebben genomen zodat C2000 en 112 operationeel blijven en stimuleer onderlinge kennisuitwisseling tussen meldkamers en UMS van Vtspn.

Raakvlakken gerelateerde projecten

- Blijf als beleidsverantwoordelijke het proces van bewustwording bevorderen en stimuleer totstandkoming van continuïteitsplannen binnen de OOV sector.
- In de door de minister gevraagde continuiteitsplannen dient extra aandacht te zijn voor de weerbaarheid van de meldkamer tegen uitval van elektriciteit aangezien het vermoeden bestaat dat dit nog niet bij alle meldkamers goed op orde is.
- Organiseer kennisuitwisseling over weerbaarheid meldkamers tussen regio's en UMS van Vtspn.
- Organiseer samen met het project Continuïteit en het project Vitale Partnerschappen een bijeenkomst met hulpverleningsdiensten en de vitale sectoren elektriciteit en telecom; met als doel het bevorderen van de weerbaarheid van de hulpverleningsdiensten tegen uitval van elektriciteit en telecommunicatie.
- Inventariseer hoe weerbaar NCV is tegen uitval van elektriciteit en/ of telecommunicatie.

Het ministerie van Veiligheid en Justitie en de hulpverleningsdiensten hebben de opdracht te bespreken of en 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 de sector Openbare Orde en Veiligheid (OOV) (op regionaal niveau) tegen ernstige verstoringen van de elektriciteit- en telecommunicatievoorziening. Hierna te noemen 'sector OOV'.

1.2 Doelstelling

De ministeries van EL&I en VenJ hebben de doelstelling als volgt geformuleerd: de weerbaarheid van de vitale sector OOV tegen ernstige verstoringen in de elektriciteit- respectievelijk de telecommunicatiesector inzichtelijk maken en zo nodig te vergroten[1]. 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] 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."

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?

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. Gezien de ontwikkelingen in de OOV sector (zie §2.5) is ervoor gekozen de intersectorale kennisuitwisseling op een later tijdstip plaats te laten vinden.

Sector-sector benadering
Er is gekozen voor een sector-sector benadering. Dat betekent dat het contact tussen sectoren wordt gestimuleerd. Specifieke klant-leverancier gesprekken vallen hierbuiten. De consequentie van een sector-sector benadering is dat niet altijd de benodigde diepgang kan worden bereikt. Daarom is er daarnaast de ruimte om overleg tussen klanten en leveranciers verder te faciliteren als wordt geconstateerd dat meer diepgang is vereist. Het faciliteren van klant-leverancier overleg valt echter buiten de scope van het CAET-project.

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 OOV 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 met politiekorpsen, veiligheidsregio's, de Ambulancezorg Nederland (AZN) en de voorziening tot samenwerking Politie Nederland (vtsPN).

Deze rapportage is ter kennisgeving aan het Veiligheidsberaad en het Korpsbeheerdersberaad 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 Openbare Orde en Veiligheid bestaat uit twee vitale diensten, namelijk: handhaving openbare orde en handhaving openbare veiligheid.[2] CAET richt zich hierbinnen op de kritische processen: functioneren meldkamer; uitrukken/ respons; informatiemanagement en communicatie.

De volgende vitale dienst is toegevoegd: regionale crisisorganisatie en -besluitvorming. Het organiseren van de crisisorganisatie en -besluitvorming is onderdeel van de taakstelling van de veiligheidsregio's conform de Wet Veiligheidsregio's.

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 informatieverstrekker bepaalt welke kleur de informatie heeft: rood, geel, groen of wit.[3]

---

[2] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2009). 2de inhoudelijke analyse bescherming vitale infrastructuur.
[3] **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,

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 OOV. Hierbij wordt ingezoomd op de veiligheidsregio en de politie organisatie. Van belang zijn de gerelateerde projecten die tevens de weerbaarheid van de sector OOV tegen uitval van elektriciteit en telecommunicatie bevorderen.

Hoofdstuk 3 beschrijft de kritische processen die afhankelijk zijn van telecommunicatie en/of elektriciteit. Zowel bij de politie als veiligheidsregio zijn de kritische processen: het functioneren van de meldkamer; het uitrukken/ respons; regionale crisisorganisatie en –besluitvorming. Informatiemanagement en communicatie worden als doorsnijdende essentiële functionaliteiten beschreven.

De weerbaarheid van de sector OOV en de genomen maatregelen tegen uitval van telecommunicatie en/of elektriciteit zijn in hoofdstuk 4 en 5 uiteengezet. Waarbij hoofdstuk 5 specifiek in gaat op de weerbaarheid van de communicatiemiddelen C2000 en 112.

In hoofdstuk 6 zijn mogelijk aanvullende maatregelen geïdentificeerd en hoofdstuk 7 beschrijft de conclusies.

---

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.

2 Typering van sector Openbare Orde en Veiligheid

2.1 Openbare Orde en Veiligheid op regionaal niveau

Regionaal zijn de bevolkings-, brandweer-, geneeskundige en politiezorg onderscheiden als de OOV processen van respectievelijk de gemeente, brandweer, GHOR en de politie. Deze processen zijn op hun beurt onderverdeeld in subprocessen (zie tabel hieronder).[4]

OOV Processen	OOV Subprocessen
Bevolkingszorg	• Communicatie • Publieke Zorg • Omgevingszorg
Brandweerzorg	• Bron- en Emissiebestrijding • Redding / Technische Hulpverlening • Ontsmetting
Geneeskundige zorg	• (Spoedeisende) Medische Hulpverlening • Psychosociale Hulpverlening • Publieke Gezondheidszorg
Politiezorg	• Ordehandhaving • Opsporing • Hulpverlening

Tabel 1. OOV processen en subprocessen

De politie- en veiligheidsregio vormen op regionaal niveau de belangrijkste organisaties van de sector openbare orde en veiligheid. Hieronder volgt een korte beschrijving.[5]

2.1.1 Veiligheidsregio

Vanwege de noodzakelijke schaal voor een adequate organisatie van de crisisbeheersing bij crises zijn in Nederland de gemeenten georganiseerd in 25 veiligheidsregio's. De brandweer, de Geneeskundige Hulpverlening in de Regio (GHOR), de politie en gemeenten werken in de veiligheidsregio samen voor een effectieve voorbereiding op en de bestrijding van crises en rampen. Op 1 oktober 2011 is de wet Veiligheidsregio's (Wvr) in werking getreden. De organisatie van de brandweerzorg, de geneeskundige hulpverlening bij ongevallen en rampen, rampenbestrijding en crisisbeheersing valt sinds deze datum officieel onder één regionaal bestuur: het bestuur van de veiligheidsregio. Het bestuur van de veiligheidsregio is identiek aan het regionale college van de politie: dezelfde voorzitter en dezelfde personen, te weten de burgemeesters uit de regio, hebben zitting in de het bestuur. De twee overleggen blijven echter als twee juridische entiteiten naast elkaar bestaan.[6]

Iedere veiligheidsregio beschikt over een regionale crisisorganisatie. De kern van de regionale crisisorganisaties wordt gevormd door de volgende drie multidisciplinaire teams: Regionaal Beleidsteam (RBT); Regionaal Operationeel Team (ROT); één of meerdere Commando's Plaats Incident (CoPI's). Ieder team kent een eigen kernbezetting van functionarissen van gemeente(n), brandweer, politie en geneeskundige hulpverlening. Afhankelijk van de aard van de crisis

[4] Referentiekader Regionaal Crisisplan 2009
[5] Zie voor een uitgebreide beschrijving de Wet op de Veiligheidsregio, Referentiekader Regionaal Crisisplan etc.
[6] Zie www.rijksoverheid.nl en Wet Veiligheidsregio's

kunnen ten behoeve van een directe afstemming over de uitvoering ook andere actoren deelnemen aan een van de teams.[7]

Elke veiligheidsregio heeft een regionale brandweerorganisatie welke onder andere zorg draagt voor: het voorkomen, beperken en bestrijden van brand en/of gevaar voor mensen en dieren bij ongevallen; het waarschuwen van de bevolking bij gevaarlijke situaties; het onderzoeken van gevaarlijke stoffen en het ontsmetten van de omgeving; het adviseren over brandpreventie, brandbestrijding en het voorkomen, beperken en bestrijden van het vrijkomen van gevaarlijke stoffen.[8]

De geneeskundige zorg voor slachtoffers bij rampen of crises geschiedt door de Geneeskundige Hulpverlening in de Regio (GHOR), zoals ambulances, ziekenhuizen en Gemeentelijke Gezondheidsdiensten (GGD's). Geneeskundige zorg houdt onder andere geneeskundige hulp, psychosociale nazorg aan slachtoffers en preventie in. [9] Ambulances worden via de meldkamer met behulp van T2000 (spraak onderdeel van C2000) gealarmeerd. Voorts geeft de meldkamer door naar welke ziekenhuizen de slachtoffers gebracht kunnen worden. De brandweer wordt via de meldkamer gealarmeerd met behulp van P2000. De bevelvoerder houdt daarna contact met de meldkamer met behulp van T2000.

De gemeenten binnen de veiligheidsregio zijn verantwoordelijk voor het proces bevolkingszorg (denk aan: voorlichting, alarmering en uitvaartverzorging). De veiligheidsregio is op haar beurt verantwoordelijk voor de voorbereiding op deze responsprocessen. [10]

2.1.2 Politie

De kerntaken van de politie zijn: het toezicht houden in de publieke ruimte; het handhaven van de openbare orde; het opsporen van strafbare feiten; en het verlenen van hulp bij nood.

Op dit moment is de Nederlandse politie georganiseerd in 25 regionale korpsen en het Korps landelijke politiediensten (KLPD) met verschillende specialistische en ondersteunende diensten. Een regionaal politiekorps is belast met de uitvoering van de politietaak in een bepaald gebied, de politieregio.

Voorts levert de voorziening tot samenwerking Politie Nederland (vtsPN) diensten, producten en adviezen om de efficiency en mogelijkheden van de politiekorpsen en de ketenpartners vergroten. De vtsPN is op 1 juli 2006 opgericht om tot een doelmatiger beheer van de politie te komen op het gebied van:

- ICT-service en informatiemanagement (Divisie Informatievoorziening & Technologie)
- Bestuurlijke beleidsontwikkeling en ondersteuning politieberaden (Divisie Bestuursondersteuning Nederlands Politie Instituut).
- Verdere ontwikkeling van nieuwe shared services, zoals Inkoop (Divisie Inkoop & Supply)

Onderdeel van vtsPN is de Unit Meldkamersystemen (UMS). In tegenstelling tot de rest van vtsPN, dat primair politiegericht is, is de UMS dienstverlening gericht op het gehele OOV werkveld (brandweer, ambulance en politie en anderen) en de gezamenlijke meldkamers.

[7] Zie Wet Veiligheidsregio's en Nationaal Handboek Crisisbesluitvorming
[8] Zie Wet Veiligheidsregio's
[9] Zie Wet Veiligheidsregio's
[10] Zie Wet Veiligheidsregio's

Het kabinet wil de organisatie van de politie veranderen, met als doel één nationale politie per 1 januari 2012.[11] De politiekorpsen verdwijnen. Daarvoor in de plaats komt één landelijk politiekorps, bestaand uit: 10 regionale eenheden; 1 of meer landelijke eenheden zoals een landelijke recherche eenheid; en een landelijke dienst voor de bedrijfsvoeringstaken, het Politiedienstencentrum.

2.2 Urgentie continuïteit openbare orde en veiligheid

De politiewet en de Wet Veiligheidsregio's stellen eisen aan de politie en de veiligheidsregio om de veiligheid van burgers te waarborgen. De hulpverleningsdiensten zijn het vangnet voor burgers in nood. Naast de wettelijke plicht verwachten burgers dat hulpverleningsdiensten te alle tijde te hulp zullen schieten in noodsituaties. De continuïteit van het kunnen waarborgen van openbare orde en veiligheid is van groot belang voor de samenleving. Bij een grootschalige elektriciteit en telecommunicatie uitval wordt verwacht dat de hulpverleningsdiensten zelfredzaam zijn en ondanks de uitval toch burgers te hulp kunnen en zullen schieten. Minister Opstelten: 'Bij grootschalige uitval of verstoring wordt ook veel van ons werk [overheidsorganisaties en hulpverleningsdiensten] nog urgenter. Hulpverleningsdiensten moeten dan blijven functioneren.'[12]

2.3 Gerelateerde ontwikkelingen

De weerbaarheid van hulpverleningsdiensten tegen uitval van elektriciteit en telecommunicatie speelt naast het project CAET ook bij andere projecten: namelijk het project Continuïteit, Vitale Partnerschappen en de ontwikkelingen rondom de meldkamers.

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.

Vitale partnerschappen in Veiligheid
In juni 2009 is het project 'Vitale partnerschappen in Veiligheid' gestart met als doel om de veiligheids- en politieregio's en vitale sectoren te ondersteunen bij het maken van samenwerkingsafspraken. Landelijke convenanten zijn gemaakt voor de sectoren drinkwater, gas, elektriciteit en telecommunicatie. Met behulp van de convenanten maken veiligheidsregio's samenwerkingsafspraken met hun vitale partners en worden gezamenlijke acties geformuleerd. Niet alleen het gezamenlijk optreden in een crisissituatie is hier een onderwerp van gesprek,

[11] Zie www.rijksoverheid.nl
[12] Ministerie van VenJ. 9 december 2010, continuïteit bij uitval of verstoring elektriciteit of ICT. Den Haag.

maar ook de onderlinge afhankelijkheid en het kunnen waarborgen van continuïteit.[13]

Ontwikkelingen rondom meldkamers
In februari 2010 heeft toenmalig minister Ter Horst (BZK) aan het veiligheidsberaad voorgesteld dat er voor heel Nederland uiteindelijk één meldkamer komt voor de politie, de brandweer en de ambulances. De landelijke meldkamer moet de ruim 20 verschillende regionale meldkamers van hulpdiensten vervangen. Om uitval bij onderhoud en storingen te voorkomen, wordt de meldkamer verspreid over drie locaties. Geconstateerd is dat de werkprocessen en de inrichting van de meldkamers verschillen met onvoldoende standaardisatie en onderlinge uitwisselbaarheid als gevolg. De nieuwe meldkamer beschikt over een gestandaardiseerd meldkamerproces en is geschikt voor nieuwe manieren van informatie-uitwisseling, zoals NL Alert, Burgernet, Amber Alert en het opsturen van foto's door getuigen.[14]

[13] www.veiligheidsberaad.nl
[14] Ministerie van BZK. Brief aan het Veiligheidsberaad over meldkamers in Nederland. 16-02-2010

3 Kritische processen

3.1 Inleiding

Dit onderzoek beperkt zicht tot de kritische processen van de vitale diensten handhaving, respons, noodhulp, ambulancezorg en regionale crisisbesluitvorming die afhankelijk zijn van elektriciteit en/of telecommunicatie. Respondenten hebben de volgende processen als kritisch benoemd:

- Functioneren meldkamer
- Uitrukken en respons
- Regionale crisisorganisatie en -besluitvorming

Doorsnijdend zijn de volgende functionaliteiten van essentieel belang voor de doorgang van de kritische processen.

- Informatiemanagement
- Communicatie

Deze processen gelden zowel voor de veiligheidsregio als de politie en vormen de basis voor bevolkings-, brandweer-, geneeskundige- en politiezorg, oftewel openbare orde en veiligheid. Binnen deze processen zijn specifiek C2000 en 112 essentiële communicatiemiddelen. De weerbaarheid van deze middelen wordt separaat beschreven in hoofdstuk 5.

Dit onderzoek maakt inzichtelijk wat de weerbaarheid van de kritische processen van de veiligheidsregio en politie is tegen uitval van elektriciteit en telecommunicatie. Onder telecommunicatie wordt communicatie via vaste en mobiele telefonie alsmede internet verstaan. Het gaat hier om de afhankelijkheid van de kritische processen ten opzichte van externe telecomaanbieders.

Voor alle kritische processen geldt dat ze niet plaats kunnen vinden zonder elektriciteit en telecommunicatie. Back-up voorzieningen dienen bij uitval van leveranciers van elektriciteit en/of telecommunicatie ervoor te zorgen dat de processen doorgang kunnen vinden zodat openbare orde en veiligheid gewaarborgd is.

3.2 Functioneren meldkamer

Het kunnen ontvangen van meldingen van burgers, bedrijven en ketenpartners is voor de politie- en veiligheidsregio van essentieel belang om hulpverleners en ordehandhavers gecoördineerd op pad te kunnen sturen. Het functioneren van de meldkamers bepaalt mede de snelheid van de respons. De meldkamers laten bijvoorbeeld aan ambulances weten welke ziekenhuizen de slachtoffers op kunnen vangen en stuurt de noodhulpeenheden van de politie aan.

3.3 Uitrukken/ respons

Om vervolgens de hulpverleners en ordehandhavers naar het plaats incident te kunnen sturen om responsactiviteiten uit te voeren, zijn verschillende voorbereidingsstappen van belang. Denk hierbij aan het kunnen oproepen van de hulpverleners en het paraat hebben staan van voertuigen met de juiste uitrustingen. Eenmaal ter plaatse is het van belang dat het aantal hulpverleners en ordehandhavers afdoende is en de hulpmiddelen toereikend.

3.4 Regionale crisisorganisatie en -besluitvorming

Afhankelijk van de grootte van het incident schalen de politie- en veiligheidsregio op volgens de GRIP structuur.[15] De kern van de regionale crisisorganisatie wordt gevormd door drie multidisciplinaire teams:

- Regionaal Beleidsteam (RBT)
- Regionaal Operationeel Team (ROT)
- Eén of meerdere Commando's Plaats Incident (CoPI's).[16]

3.5 Informatiemanagement en communicatie

Informatiemanagement en communicatie zijn zowel voor het functioneren van de meldkamers, de responsactiviteiten als de regionale crisisorganisatie van cruciaal belang om openbare orde en veiligheid te kunnen waarborgen. Bij uitval van elektriciteit en/of telecommunicatie worden deze processen bemoeilijkt. In hoofdstuk 4 is uiteengezet welke maatregelen reeds zijn genomen en welke maatregelen mogelijk nog aanvullend genomen kunnen worden om de weerbaarheid van informatiemanagement en communicatie tegen uitval van elektriciteit en/of telecommunicatie te vergroten. **De beschikbaarheid van spraakcommunicatie wordt in hoofdstuk 4 niet in een aparte alinea besproken maar komt per kritisch aan de orde.** De beschikbaarheid van informatiemanagement wordt separaat toegelicht. Voor informatiemanagement is de ontwikkeling van netcentrisch werken van belang. Netcentrisch werken ondersteunt bij informatievoorziening om over verschillende lagen een gedeeld totaalbeeld van de situatie te krijgen. Dit gedeelde totaalbeeld dient als basis voor de te nemen besluiten en de in te zetten acties.

C2000 en 112 als essentiële communicatiemiddelen

Het noodnummer 112 en het communicatienetwerk C2000 met onder andere de communicatiemiddelen T2000 (spraak) en P2000 (pieper) zijn zeer belangrijk voor de continuïteit van de politie en de veiligheidsregio. Gezien het belang van de beschikbaarheid van deze middelen voor alle kritische processen wordt de weerbaarheid ervan separaat besproken in Hoofdstuk 5.

[15] Een Gecoördineerde Regionale Incidentbestrijdings Procedure (GRIP) is in Nederland een landelijke afspraak over de opschaling van incident- en rampenbestrijding voor professionele hulpverleners als de brandweer, politie en GHOR (waaronder ambulancediensten). De procedures regelen opschaling op operationeel niveau op de plaats van het incident en daarnaast op bestuurlijk niveau van gemeente tot waar nodig zelfs landelijk.

[16] Zie Wet op de Veiligheidsregio's en Nationaal Handboek Crisisbesluitvorming

4 Weerbaarheid tegen uitval telecommunicatie en elektriciteit

4.1 Functioneren meldkamer

De meldkamer is het centrale knooppunt waar hulpoproepen binnen komen en de respons van professionals gecoördineerd wordt. Hulpoproepen van burgers, bedrijven en ketenpartners komen via verschillende ingangen binnen bij de meldkamers. De oproepen van mobiele telefoons komen binnen bij het KLPD waarna de oproep, indien mogelijk, wordt doorgeschakeld naar de regionale meldkamer; de oproepen van vaste telefoons komen direct binnen bij betreffende regionale meldkamer. De coördinatie van de respons door de meldkamer vindt veelal plaats via C2000.

Bij **uitval van telecommunicatie** is de meldkamer lastig te bereiken voor hulpoproepen. Indien een hulpoproep wordt gedaan dan zal de oproep worden doorgeschakeld naar een andere meldkamer. Elke meldkamer heeft een uitwijklocatie, meestal een meldkamer in een andere regio. Bij uitval van telecommunicatie in de gehele regio dienen de hulpverleningsdiensten er echter rekening mee te houden dat burgers, bedrijven en ketenpartners mogelijk niet over telecommunicatiemiddelen beschikken waarmee ze de meldkamer kunnen bereiken. Enkele hulpdiensten en slechts een enkele ketenpartner, zoals waterschappen, drinkwaterbedrijven en andere overheidsdiensten, beschikken over achtervang communicatiemiddelen zoals C2000 en/of noodnet om de meldkamer te kunnen bereiken en om onderling te kunnen communiceren. De weerbaarheid van C2000 tegen uitval van externe aanbieders van telecommunicatie wordt nader toegelicht in hoofdstuk 5. Alternatief voor burgers en bedrijven zonder achtervang communicatiemiddelen is het fysiek aandoen van een veiligheidsregio en/of politiebureau.

Uitval van elektriciteit wordt in de meldkamer opgevangen door noodstroom aggregaten (NSA). Het is niet bekend of alle meldkamers in Nederland en hun uitwijklocaties over kwalitatief goede NSA beschikken met voldoende dieselolie om drie dagen te kunnen draaien. De capaciteit en kwaliteit van de NSA verschilt per meldkamer. De geïnterviewde politie- en veiligheidsregio's geven zelf aan over voldoende NSA capaciteit te beschikken. Tevens worden de NSA regelmatig getest en wordt er een enkele keer geoefend met het scenario uitval van elektriciteit. Gezien de ervaringen van onder andere de UMS van Vtspn is dit mogelijk niet representatief voor alle meldkamers. Praktijkervaring laat zien dat uitval van elektriciteit enkele keren voor problemen in de meldkamer hebben gezorgd. De weerbaarheid van C2000 en 112 tegen uitval van externe aanbieders van elektriciteit wordt nader toegelicht in hoofdstuk 5.

4.2 Uitrukken/ respons

Om als ordehandhaver en hulpverlener adequaat op te kunnen treden zijn communicatiemiddelen van cruciaal belang. In de respons is men afhankelijk van communicatie tussen de professionals onderling en communicatie tussen meldkamer en professionals. Een respondent geeft aan dat de politie zelfs steeds meer afhankelijk wordt van externe telecommunicatie leveranciers. Zo wordt er steeds meer gebruik gemaakt van de mobiele telefoon in de uitvoering van de primaire processen en veel minder van de portofoon of C2000. Een voorbeeld is de agent op straat die zijn mail ontvangt op zijn Blackberry en mutaties invoert in een digitaal bonnenboekje.

De politiekorpsen hebben met de aanbieder van de mobiele telefonie prioritaire abonnementen afgesloten. Dit betekent dat de politie prioriteit heeft tot aan de mast wat bijvoorbeeld handig is bij grote evenementen. In geval van congestie

op de gehele infrastructuur (bijvoorbeeld met oud en nieuw) werkt dit echter niet. Ook voor het contact tussen ambulance en ziekenhuis wordt gebruik gemaakt van externe telecomaanbieders. Dit contact verloopt via de meldkamer.

Bij **uitval van** externe **telecommunicatie** aanbieders, vallen ordehandhavers en hulpverleners terug op de (achtervang) communicatiemiddelen T2000 en noodnet voor spraakverkeer. Hulpverleners, zoals de brandweer en de ambulance beschikken tevens over piepers (P2000). Het wegvallen van externe telecommunicatie aanbieders zal tot ongemakken leiden. T2000, P2000 en noodnet zijn voldoende voor de benodigde communicatie echter minder handzaam dan de mobiele telefoon. T2000 en P2000 zijn echter niet geheel ongevoelig voor de uitval van telecommunicatie. Dit wordt separaat toegelicht in hoofdstuk 5. Enkele veiligheidsregio's overwegen additioneel satelliettelefoons aan te schaffen of hebben satelliettelefoons aangeschaft.

Bij **uitval van elektriciteit** geldt dat de bureaus van politie en veiligheidsregio terugvallen op noodstroom aggregaten (NSA). De geïnterviewde politie- en veiligheidsregio's geven aan dat de vitale processen draaien op de NSA, zoals onder andere vitale computersystemen, coördinatiecentra en de klimaatbeheersing. Gemiddeld testen zij de NSA één keer per maand. Een randvoorwaarde voor uitrukken en de respons is echter ook dat de benodigde voertuigen en materialen gebruikt kunnen worden, ook bij elektriciteituitval. Respondenten geven aan dat het wagenpark bij elektriciteituitval mogelijk niet van brandstof kan worden voorzien. Aangegeven is dat mogelijk enkele brandweerkorpsen een eigen pomp hebben die is aangesloten op een noodstroomaggregaat. Voor de ambulances is het van belang dat de medische apparatuur is opgeladen. Naar aanleiding van het interview met Ambulancezorg Nederland wordt verkend in hoeverre Regionale Ambulance Voorzieningen de beschikking hebben over NSA's. De verwachting is dat dit niet het geval is.

Vraag die politie- en veiligheidsregio's hebben is in hoeverre C2000 en 112 in de lucht blijven bij uitval van elektriciteit. Dit is namelijk van essentieel belang voor het optreden van de ordehandhavers en hulpverleners. Dit komt terug in hoofdstuk 5.

4.3 Regionale crisisbesluitvorming en -organisatie

Indien tijdens **telecommunicatie uitval** de crisisorganisatie (Gecoördineerde Regionale Incidentbestrijding Procedure (GRIP)) is of wordt opgeschaald zal enerzijds besluitvorming en anderzijds crisiscommunicatie naar de bevolking worden bemoeilijkt. Beeldvorming en oordeelsvorming vinden plaats om vervolgens met de crisisorganisatie tot besluitvorming te komen. Het hebben van informatie is hierbij van elementair belang. Vraag is in hoeverre de noodcommunicatiemiddelen in deze behoefte kunnen voorzien. Indien er tot crisiscommunicatie met burgers en bedrijven wordt besloten, dient men er rekening mee te houden dat de samenleving bij telecommunicatie uitval niet via telefoon, televisie of internet bereikt kan worden. Een ander openstaand punt is dat veelal niet is vastgelegd hoe de crisisteams worden opgeroepen buiten kantooruren, indien telecommunicatie is uitgevallen. Het hangt er ook van af of de crisisteams op dat moment bij elkaar geroepen moeten worden. Niet iedere uitval is meteen een crisis. Enkele besluitvormers beschikken over een pieper, anderen zullen mogelijk thuis worden opgehaald. Naast crisisbesluitvormers is het kunnen oproepen van bijvoorbeeld onderhoudsmonteurs van groot belang. Respondenten geven aan dat er op zo een moment medewerkers langs gestuurd zullen worden om de onderhoudsmonteurs op te halen.

Bij **elektriciteit uitval** kunnen de crisisteams bij elkaar komen en gebruik maken van de crisisruimtes, omdat deze draaien op NSA. Alternatief is het gebruik maken van de uitwijklocatie. Indien de crisisteams informatie kunnen

ontvangen en versturen zal de elektriciteit uitval de activiteiten van de crisisteams niet of nauwelijks verstoren. Men dient er echter rekening mee te houden dat bij uitval van elektriciteit mogelijk ook telecommunicatie uitvalt. Er wordt nog slechts weinig geoefend met het scenario uitval van elektriciteit en/of telecommunicatie.

4.4 Informatiemanagement

Informatiemanagement, oftewel het kunnen beschikken over de juiste informatie, op het juiste moment en op de juiste plaats, is zeer afhankelijk van van dataverbindingen. Politiekorpsen en Veiligheidsregio's beschikken over een eigen netwerk voor datacommunicatie binnen het korps. Dit betekent dat bij **uitval van** de aanbieder van **telecommunicatie** de professionals binnen de organisatie nog wel onderling data kunnen uitwisselen. Het beheer van de politiesystemen is per verzorgingsgebied ondergebracht bij de VtsPN. De dataverbindingen met het verzorgingsgebied verlopen via een eigen infrastructuur. De belangrijkste meldkamersystemen draaien lokaal en zijn niet afhankelijk van externe telecommunicatie aanbieders. Datacommunicatie met politieauto's (mobipol) zal niet meer functioneren. Informatiebronnen die via internet worden ontsloten zijn bij uitval van externe telecommunicatieaanbieders niet meer beschikbaar. Volgens respondenten beïnvloed dit de uitvoering van de kritische processen minimaal.

De datacommunicatieverbindingen en de beschikbaarheid van ICT-systemen zijn afhankelijk van elektriciteit. Volgens de respondenten wordt bij **uitval van elektriciteit** de beschikbaarheid van de ICT-systemen en dataverbindingen die benodigd zijn ter ondersteuning van de kritische processen gegarandeerd door voldoende NSA capaciteit. Respondenten geven aan dat mobiele communicatiemiddelen kunnen worden opgeladen op kantoor (i.v.m. de aanwezige NSA) of in de auto, brandweerwagen of ambulance.

Tevens geldt dat politie- en veiligheidsregio bijstand kunnen aanvragen bij elkaar en aan de rijksoverheid, zoals het Nationaal CrisisCentrum (NCC), het Landelijk Operationeel CrisisCentrum (LOCC) en de Landelijk Faciliteit Rampenbestrijding (LFR). En op basis van het convenant Intensivering Civiel-Militaire Samenwerking (ICMS) kan Defensie gevraagd worden de regio bij te staan. Deze organisaties hebben alle de mogelijkheid een bijdrage te leveren in het informatiemanagement of de levering van de ondersteunende middelen.

5 Weerbaarheid van C2000 en 112 tegen uitval van telecommunicatie en elektriciteit

De weerbaarheid van het netwerk C2000 (waarvan T2000 en P2000 een onderdeel zijn) het noodnummer 112 zijn hier in een apart hoofdstuk uiteengezet, omdat de respondenten hebben aangegeven dat de weerbaarheid van deze twee communicatie middelen van essentieel belang is voor de openbare orde en veiligheid. Waar 112 gericht is op noodoproepen van de samenleving aan hulpverleningsdiensten, is T2000 een communicatiemiddel voor spraakverkeer tussen hulpverleningsdiensten. P2000 is een netwerk speciaal voor piepers. Eerst wordt ingezoomd op de Unit Meldkamersystemen (UMS) van de VtsPN, de beheerder van de C2000 (T2000 en P2000) en 112 netwerken.

5.1 UMS van VtsPN

De Unit Meldkamersystemen (UMS) van de VtsPN, de beheerder van C2000 en 112, is zich bewust dat de continuïteit van deze diensten van groot belang is. Ten tijde van het CAET project is UMS bezig met het opstellen van continuïteitsplannen tegen uitval van elektriciteit en telecommunicatie.

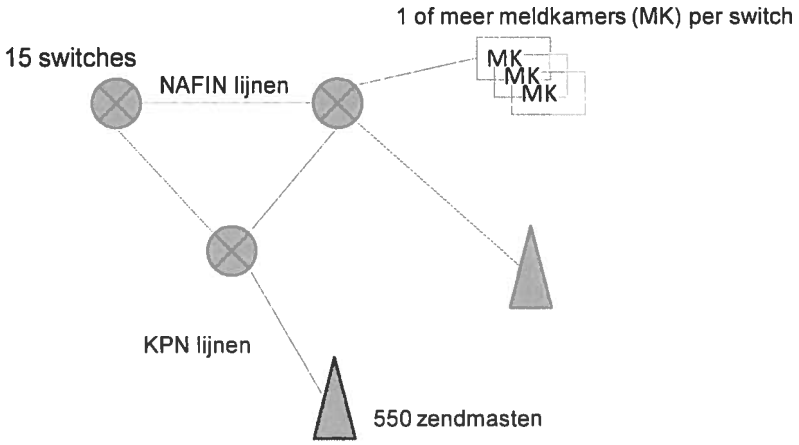
Voorts is een calamiteitenplan geschreven dat beschrijft welke activiteiten moeten worden ondernomen wanneer netspanning is weggevallen op een locatie binnen het netwerk. Ten aanzien van de aanvoer van dieselolie voor NSA is bijvoorbeeld afgesproken dat de Landelijke Faciliteit Rampenbestrijding (LFR) de NSA's op switchlocaties en opstelpunten (masten) van brandstof voorziet. De LFR kan hierbij gebruik maken van de crisisvoorraad die door de rijksoverheid wordt aangehouden. Voor meer detailinformatie wordt verwezen naar de continuïteitsplannen van UMS.

5.2 C2000

De kritische processen van de veiligheidsregio en politie kunnen voor een groot deel doorgang hebben bij uitval van elektriciteit en telecommunicatie in verband met de aanwezigheid van noodstroom aggregaten (NSA) en het achtervang communicatiemiddel C2000. Van essentieel belang is wel dat bij elektriciteit- en telecommunicatie uitval C2000 in de lucht blijft. De weerbaarheid van C2000 tegen uitval van elektriciteit en telecommunicatie wordt in de paragraaf nader toegelicht.

Het T2000 netwerk (het spraak gedeelte van C2000) is een decentraal georganiseerd netwerk en bestaat uit 15 zones. Alle communicatie binnen een zone en met andere zones wordt afgehandeld door een zoneswitch. Dit betreft alle communicatie tussen de op de zoneswitch aangesloten meldkamers onderling, tussen meldkamers en zendmasten, en tussen zendmasten onderling. En bij interzonecommunicatie dus de communicatie met de zoneswitches van de andere zones. Aan elke zoneswitch zijn een of meer meldkamers en een aantal zendmasten gekoppeld. Per zone is de zoneswitch daarmee de spin in het web. Het C2000 netwerk bestaat uit 15 switches in het land. In totaal zijn er circa 25 meldkamers en 550 zendmasten (zie figuur 1).

C2000 netwerk



Figuur 1. C2000 netwerk

De 15 switches zijn onderling en met de meldkamers verbonden via het NAFIN[17] netwerk. De verbindingen tussen de switches en de zendmasten lopen via het KPN netwerk (MCTN[18]). Deze twee netwerken draaien onafhankelijk van elkaar. In geval van elektriciteituitval zijn er het C2000 de volgende back ups:

Netwerk	Locatie	Back-up bij elektriciteituitval
C2000	15 switches	UPS en een vast NSA *of* een aansluiting voor een mobiel NSA. Voorts is er voor de 15 C2000 switches 1 fall back switch die de functie kan overnemen indien een enkele switch uitvalt. Het kost 8 uur om deze operationeel te krijgen.
	Ca. 550 zendmasten	UPS voor 3 tot 8 uur (afhankelijk van aantal baseradio's). Voor masten met meerdere baseradio's op te rekken richting 8 uur door een deel van de baseradio's af te schakelen. Pool van 13 mobiele NSA's landelijk inzetbaar.
	Meldkamerspecials	Verantwoordelijkheid meldkamer; onbekend bij UMS
NAFIN	Hoofdringlocatie	UPS[19] voor 4 uur en vast NSA
	Ringlocatie	UPS voor 4 uur en vast NSA *of* UPS voor 8 uur en aansluitpunt voor een mobiel NSA

[17] Het **Netherlands Armed Forces Integrated Network** (NAFIN) is een eigen, zwaar beveiligd glasvezelnetwerk van het Ministerie van Defensie.NAFIN is een geïntegreerd statisch interlokaal verbindingsstelsel voor spraak- en datacommunicatie voor de gehele defensieorganisatie. Sinds 2004 fungeert NAFIN tevens als backbone voor het C2000 (Tetra) communicatienetwerk voor de OOV-diensten (Openbare Orde en Veiligheid).

[18] MCTN is een huurlijnendienst van KPN.

[19] Het verzorgen van een noodstroomvoeding kan door middel van een Uninterruptible Power Supply (UPS) of een noodstroomaggregaat (NSA). Een UPS is een apparaat dat bij uitval of sterke afwijking van de netspanning, de stroomvoorziening van computers en andere apparatuur voor een bepaalde tijd kan overnemen.

KPN (MCTN)	Tussen switches en masten	UPS voor 2 uur en een vast NSA *of* UPS voor 5 uur een aansluitpunt voor een mobiel NSA

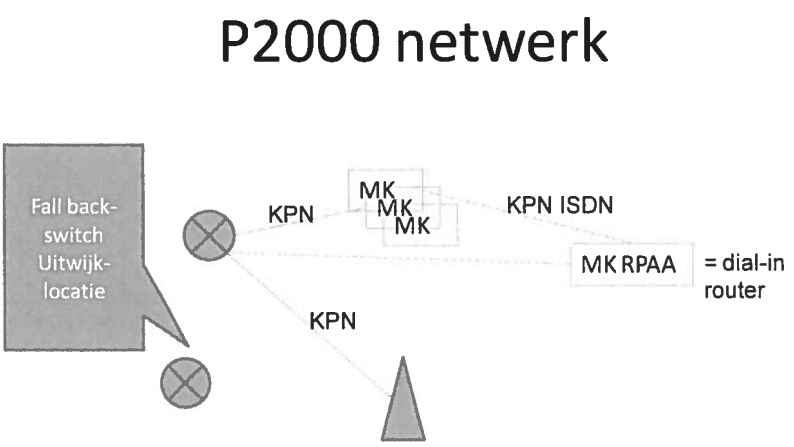
Tabel 2. Back-ups C2000 netwerk

Voor switches en zendmasten geldt dat de systemen een dubbele uitvoering van diverse kritische onderdelen kennen. Hiernaast is het NAFIN netwerk een fysiek gescheiden redundant netwerk. De MCTN verbindingen van KPN zijn niet redundant uitgevoerd. Uitval van deze verbindingen leidt tot de uitval van zendmasten en beperkt de werking van C2000 en P2000.

UMS is de beheerorganisatie van C2000 en stuurt onder andere de onderhoudspartijen aan. Het Engineering Bureau (EB) (onderdeel van UMS), Tetraned en Volker Wessels zijn de belangrijkste partners voor het onderhoud van het netwerk. Hiernaast is de Landelijke Faciliteit Rampenbestrijding (LFR) een belangrijke partner. UMS beschikt over zes mobiele C2000 zendmasten met eigen aggregaat, die bijvoorbeeld bij evenementen ingezet kunnen worden, en 13 mobiele NSA die zowel op de zendmasten aangesloten kunnen worden. EB en LFR hebben beiden een rol in de inzet van de mobiele masten en NSA's. EB, LFR en NMC kunnen elkaar bij uitval van telecommunicatie bereiken via C2000.

5.3 P2000

Naast T2000 werkt met name de brandweer ook met P2000. Dit is een netwerk speciaal voor piepers en kent een andere opbouw dan het T2000 netwerk (zie figuur 2).



Figuur 2. P2000 netwerk

Het P2000 netwerk beschikt over één switch met een UPS, een vast NSA en een aansluitpunt voor een mobiel NSA. Deze switch heeft tevens een back-up op een andere locatie. Voor beide switches is brandstof voor de NSA's geborgd. Tevens zijn de kritische onderdelen telecommunicatieverbindingen dubbel uitgevoerd.

Het P2000 netwerk is volledig afhankelijk van KPN verbindingen. De Amsterdam Dial In verbinding kan eventueel als back-up fungeren indien de vaste verbinding tussen één meldkamer en de switch is uitgevallen.

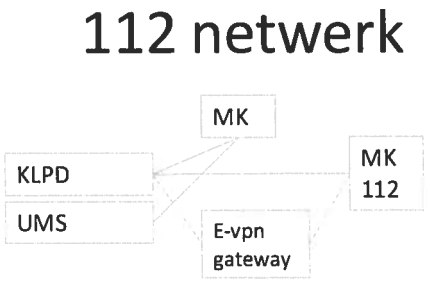
Samengevat zijn er in geval van elektriciteituitval voor het P2000 netwerk de volgende back ups:

Netwerk	Locatie	Back-up bij elektriciteituitval
P2000	Eén switch	UPS, vast NSA, aansluitpunt voor mobiel NSA Uitwijk: back-up switch

Tabel 3. Back-ups P2000 netwerk

5.4 112

Met het noodnummer 112 doen burgers, bedrijven en ketenpartners een beroep op ordehandhavers en hulpverleners. 112 oproepen van de vaste lijn komen binnen bij de regionale meldkamer. 112 oproepen vanaf een mobiel komen binnen bij de KLPD. De KLPD schakelt dan door naar de plaatselijke meldkamer (zie figuur 3). Dit gebeurt grotendeels zonder tussenkomst van de centralist door het gebruik van spraakherkenningssystemen. Alleen de oproepen die niet automatisch gerouteerd kunnen worden, worden door de KLPD centralisten doorgerouteerd.



Figuur 3. 112 netwerk

De KLPD centrale bestaat uit 2 delen die elk afzonderlijk voldoende capaciteit hebben om alle oproepen te kunnen afhandelen. Elk systeemdeel is voor de inkomende oproepen gekoppeld aan twee fysiek gescheiden gerouteerde ISDN-30[20] verbindingen. De twee systeemdelen zijn geografisch gescheiden gehuisvest (bij KLPD en UMS).

[20] Integrated Services Digital Network (ISDN) is een vorm van digitale telefonie. Bij telefonie via ISDN wordt gebruik gemaakt van dezelfde centrales en schakelmiddelen als bij analoog. Het verschil is dat het bij ISDN gaat om digitale signalen die zich veel beter door een netwerk laten transporteren, met minder ruis en storingen. Een standaard ISDN-30-aansluiting biedt 30 communicatiekanalen.

De KLPD centrale staat voor het doorrouteren van oproepen in verbinding met de meldkamers via noodnet en [redacted] Eind 2011 loopt een project waarbij diverse wijzigingen worden doorgevoerd aan het 112 platform. Zo wordt het systeemdeel dat nu bij KLPD staat verhuist naar een beveiligde omgeving in Hilversum (waar ook de T2000 en P2000 fallbackswitches staan). De e-VPN gateways en verbindingen naar de meldkamers vervallen en worden vervangen door NCV verbindingen. De veronderstelling is dat de NCV verbindingen robuuster zijn en daarmee de weerbaarheid van 112 wordt versterkt. 10.1.c

KLPD heeft een uitwijkmeldkamer op de UMS locatie. Beide meldkamers zijn gekoppeld aan beide systeemdelen.

Een systeemredundantie is de 'calamiteitenschakeling naar zogenaamde buddyregio's' voor de regionale meldkamers.

Alle meldkamers (regionaal en KLPD) zijn bij elektriciteit uitval zelf verantwoordelijk voor het hebben van NSA's. UMS, de beheerder van het 112 netwerk, heeft geen inzicht in de weerbaarheid van de meldkamers tegen uitval van elektriciteit.

De NSA van UMS en KLPD worden periodiek getest en voldoende brandstof is geborgd. Bij UMS wordt tevens 3 tot 5 keer per jaar geoefend met elektriciteit uitval.

Voorts heeft de beheerder UMS geen zicht op de weerbaarheid van het nationale noodnet tegen uitval van elektriciteit. Deze borging wordt verondersteld.

In geval van elektriciteituitval heeft het 112 netwerk de volgende back ups:

Tabel 3. Back-ups 112 netwerk

Netwerk	Locatie	Back-up bij elektriciteituitval
112	Regionale Meldkamers	Verschilt. Is verantwoordelijkheid van meldkamer. Oproepen kunnen bij uitval worden gerouteerd naar een buddymeldkamer.
	Meldkamer KLPD	Systeemdeel bij KLPD: UPS, verdere borging onbekend bij UMS; verantwoordelijkheid KLPD/KPN Systeemdeel bij UMS: UPS, vast NSA en aansluiting voor mobiel NSA meldkamer/centralisten: uitwijkmeldkamer bij UMS
[redacted]	Tussen KLPD/UMS en meldkamers	zie de [redacted]pecificaties in 5.2
ISDN-30	Inkomend verkeer	zie de [redacted]specificaties in 5.2

10.1.c

[21] Met [redacted] van [redacted] worden bedrijfsvestigingen aan elkaar gekoppeld op basis van ethernet techniek waardoor één groot Wide Area Network (WAN) is gecreëerd. 10.1.c

6 Mogelijk aanvullende maatregelen

6.1 Functioneren meldkamer

Bij grootschalige uitval van telecommunicatie zullen burgers en bedrijven niet via telecommunicatie om hulp kunnen vragen, met uitzondering van enkele vitale partners die over noodcommunicatiemiddelen beschikken. Burgers en bedrijven vragen bij noodsituaties om hulp aan de overheid, maar wat zullen de burgers van de overheid verwachten bij grootschalige telecommunicatie en/of elektriciteit uitval? De openbare orde is mogelijk in het geding vanwege het niet werken van (vitale) infrastructuren. In het kader van 'Vitale Partnerschappen' sluiten veiligheidsregio's convenanten af met vitale partners, zoals de telecom- en elektriciteitsleveranciers.

- *Organiseer dat alle (nieuwe) meldkamers een redundante uitwijklocatie hebben.*
- *Advies aan politie en veiligheidregio om van tevoren te hebben nagedacht over:*
    - *de rol van de politie en veiligheidsregio bij grootschalige uitval van elektriciteit en telecommunicatie. Veiligheidsregio Rotterdam-Rijnmond heeft bijvoorbeeld een responsplan stroomuitval;*
    - *de manier hoe met de burgers gecommuniceerd zal worden en de burgers de gelegenheid krijgen een melding te doen.*
- *Bespreek als politie- en veiligheidsregio met vitale partners wat grootschalige uitval van telecommunicatie en/of elektriciteit voor de meldkamer kan betekenen; spreek af hoe hierop te reageren, hoe met elkaar te communiceren/ meldingen te maken en spreek uit wat men van elkaar kan verwachten in deze situatie.*

6.2 Uitrukken/ respons

Op basis van coördinatie vanuit de meldkamer rukken ordehandhavers en hulpverleners uit. Bij uitval van telecommunicatie kan deze melding binnenkomen via noodcommunicatiemiddelen. Het is van essentieel belang dat ordehandhavers en hulpverleners, ook in actie, met noodcommunicatiemiddelen om kunnen gaan. Tevens dienen personeel en materiaal te allen tijde gereed te staan om ingezet te kunnen worden. Sommige materialen zijn afhankelijk van telecommunicatie en/of elektriciteit. Het wagenpark van brandstof voorzien, vraagt bijvoorbeeld om elektriciteit. Voorts zijn bewakingssystemen en slagbomen eveneens afhankelijk van elektriciteit.

- *Oefen als politie en veiligheidsregio regelmatig met het gebruik van noodcommunicatiemiddelen. Wissel ervaringen uit en zet ideeën voor verbetering om in aanpassingen ten opzichte van het proces en indien mogelijk de apparatuur.*
- *Houd voor het kunnen uitrukken van politie, brandweer en ambulance rekening met het scenario 3 dagen geen elektriciteit/ en of telecommunicatie. Zorg ervoor dat personeel met het juiste materiaal en de juiste uitrusting naar het plaats incident kan gaan. Denk bijvoorbeeld aan een wagenpark met volle tanks.*
- *Test als hulpdienst de noodstroom aggregaten (NSA) regelmatig, momenteel is vaak te onduidelijk of dit gebeurd.*
- *Oefen als hulpdiensten met een scenario met uitval van telecommunicatie zodat de kwaliteit en kwantiteit van de noodcommunicatiemiddelen worden gestest en de veronderstelde zelfredzaamheid van medewerkers juist is.*

6.3 Regionale crisisbesluitvorming en –organisatie

Grootschalige regionale incidenten vragen om coördinatie door COPI, ROT en/of RBT. Mogelijk wordt er op rijksniveau ook opgeschaald. Uit de inventarisatie blijkt dat voor de besluitvormers nog niet is uitgedacht wat operationele en bestuurlijke dilemma's zijn ten tijde van een grootschalige elektriciteit en/of telecommunicatie uitval. Dit is iets waar van tevoren al over nagedacht kan worden.

- *Inventariseer per regio welke operationele en bestuurlijke dilemma's op kunnen treden bij grootschalige telecommunicatie en/of elektriciteit uitval en win alvast informatie van experts in hoe hierop te reageren.*
- *Het regionaal oppakken van dit vraagstuk is sub-optimaal. Wissel interregionaal de kennis en ervaring uit.*
- *Stem af met het Rijksniveau wat de regio bij dit scenario van hen kan verwachten.*
- *Leg als politie en veiligheidsregio vast hoe crisisbesluitvormers en ander essentieel personeel te bereiken tijdens en buiten kantooruren wanneer er geen telecommunicatie verbinding (vast, mobiel, internet) mogelijk is. Denk bijvoorbeeld aan het paraat hebben van de adresgegevens van de besluitvormer om deze persoon bij uiterste nood thuis op te kunnen halen.*
- *Bespreek de mogelijkheid van alternatieven, zoals bijvoorbeeld het ter plaatse hebben van ROT en RBT om ook zonder telecommunicatiemiddelen op basis van adequate mondelinge informatievoorziening crises te kunnen bestrijden.*
- *Houd als hulpdienst bij grootschalige en langdurige uitval van elektriciteit ook rekening met uitval van telecommunicatie. Nog te vaak wordt geoefend met het scenario elektriciteitsuitval maar wordt verondersteld dat de telecommunicatie wel gewoon operationeel is ("anders wordt het oefenen zo lastig").*

6.4 Informatiemanagement

Informatiemanagement met behulp van netcentrisch werken is steeds belangrijker voor hulpverleningsdiensten. Het niet via netcentrisch werken kunnen uitwisselen van informatie betekent een vertraging van de beeldvorming en daarmee de oordeelsvorming en besluitvorming. Een politiedienst kan onderling data blijven uitwisselen over zijn eigen netwerk. Onduidelijk is echter wat de weerbaarheid is van de dataverbindingen tussen ketenpartners.

- *Inventariseer de toenemende afhankelijkheid van netcentrisch werken en toets de beschikbaarheid en betrouwbaarheid van onderliggende verbindingen.*

6.5 Communicatie

Communiceren zonder telecommunicatiemiddelen brengt de samenleving terug in de tijd. De burger en bedrijven zijn belangrijke partners voor ordehandhavers en hulpverleners, maar om samen effectief op te kunnen trekken is communicatie van essentieel belang. Het anticipatie en improvisatie vermogen van iedereen wordt op de proef gesteld bij grootschalige uitval van telecommunicatie en/of elektriciteit. Desalniettemin kan op voorhand al bedacht worden wat alternatieve communicatiemiddelen richting de samenleving en wat een alternatieve procesgang van informatiemanagement zouden kunnen zijn.

- *Wees ervan bewust dat noodcommunicatiemiddelen mogelijk niet even toereikend zijn als de gebruikelijke communicatiemiddelen. Blijven oefenen met noodcommunicatiemiddelen is essentieel.*

- *Werk als veiligheidsregio uit wat alternatieve crisiscommunicatie wegen richting de samenleving kunnen zijn. Naast de geluidswagens kunnen bijvoorbeeld lokale bureaus dienen als voorlichtingsruimte.*
- *Stimuleer als hulpdiensten het vergroten van de zelfredzaamheid van de burger. Laat als overheidsdiensten weten wat de burger kan verwachten en wat bij grootschalige uitval van telecommunicatie alternatieve communicatiemiddelen zijn.*
- *Stem met partners af hoe met elkaar te communiceren en hoe informatie met elkaar te delen bij uitval van telecommunicatie.*

C2000 en 112

De kwetsbaarheid van C2000 en 112 zit in de afhankelijkheid van KPN en de meldkamers zelf. Delen van de systemen kunnen blijven draaien bij uitval van elektriciteit en/of telecommunicatie, maar bij uitval van KPN zullen delen niet meer functioneren. De terugvaloptie is de verbinding via het noodnet. Noodnet bleek deze vraag echter niet aan te kunnen. Onduidelijk is of de nieuwe noodcommunicatievoorziening hier wel in kan voorzien.

- *Investeer in uitbreiding van nieuwe de Nood Communicatie Voorziening (NCV) voor verbindingen tussen KLPD en regionale meldkamers.*

De meldkamers beschikken als back-up over uitwijklocaties. Vraag is echter of de uitwijklocaties mogelijk niet dezelfde problemen hebben. Hiernaast is het opmerkelijk dat de beheerorganisatie UMS niet op de hoogte is van de genomen weerbaarheidsmaatregelen van de meldkamers. Van belang is dat er onderscheid wordt gemaakt tussen de weerbaarheid van systemen enerzijds en de weerbaarheid van meldkamers anderzijds. Waarbij de weerbaarheid van de meldkamers de verantwoordelijkheid is van de meldkamers zelf. Wanneer de C2000 meldkamerspecials uitvallen kan een meldkamer niet terugvallen op een andere regio. Deze meldkamerspecials niet redundant uitgevoerd op de meldkamers. UMS kan zorgen voor redundantie van systemen wanneer de meldkamers aangeven dat zij een uitwijklocatie hebben, en daar backupvoorzieningen moeten worden aangebracht. Dit is echter de verantwoordelijkheid van de meldkamers.

- *Inventariseer welke weerbaarheidsmaatregelen meldkamers hebben genomen zodat C2000 en 112 operationeel blijven en stimuleer onderlinge kennisuitwisseling tussen meldkamers en UMS van Vtspn.*

6.6 Raakvlakken gerelateerde projecten

Binnen het project Continuïteit stellen hulpverleningsdiensten continuïteitsplannen ten aanzien van uitval van elektriciteit en ICT op. En binnen het project Vitale Partnerschappen maken hulpverleningsdiensten samenwerkingsafspraken met onder andere de vitale sectoren elektriciteit en telecommunicatie. De uitkomsten van CAET bevorderden samen met deze ontwikkelingen het verhogen van de weerbaarheid van hulpverleningsdiensten.

- *Blijf het proces van bewustwording bevorderen en stimuleer totstandkoming van continuïteitsplannen binnen de OOV sector.*
- *In de door de minister gevraagde continuiteitsplannen dient extra aandacht te zijn voor de weerbaarheid van de meldkamer tegen uitval van elektriciteit aangezien het vermoeden bestaat dat dit nog niet bij alle meldkamers goed op orde is.*
- *Organiseer kennisuitwisseling over weerbaarheid meldkamers tussen regio's en UMS van Vtspn.*
- *Organiseer samen met het project Continuïteit en het project Vitale Partnerschappen een bijeenkomst met hulpverleningsdiensten en de vitale sectoren elektriciteit en telecom; met als doel het bevorderen van de weerbaarheid van de hulpverleningsdiensten tegen uitval van elektriciteit en telecommunicatie.*

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.

- *Inventariseer hoe weerbaar NCV is tegen uitval van elektriciteit en/ of telecommunicatie.*

7 Conclusie

Hulpverleningsdiensten hebben een cruciale rol in de samenleving. De continuïteit van deze diensten is van groot belang. Naast het wettelijk kader verwacht de samenleving dat deze diensten te allen tijde bereikbaar en beschikbaar zijn. Om openbare orde en openbare veiligheid te kunnen handhaven zijn de volgende kritische processen randvoorwaardelijk:

- De meldkamer functioneert
- Er is capaciteit (personeel en middelen) om te reageren
- Operationele en bestuurlijke besluitvorming vindt plaats
- Informatie wordt verzameld en geanalyseerd
- Hulpverleningsdiensten kunnen onderling communiceren

Bij uitval van elektriciteit en/of telecommunicatie worden deze randvoorwaardelijke processen op de proef gesteld.

Van een meldkamer wordt verwacht dat het bereikbaar is en de noodstroomaggregaten gedurende een lange tijd werken en/of in het uiterste geval de uitwijklocatie de functionaliteiten over kan nemen. Het is van essentieel belang dat deze achtervang is getest, zodat deze het doet op het moment het nodig is.

Hetzelfde geldt voor het kunnen uitrukken. Personeel moet opgeroepen kunnen worden en de middelen die het personeel nodig heeft om op te treden, moeten gebruikt kunnen worden. Noodcommunicatiemiddelen zijn de achtervang van communicatie onderling. Enerzijds is het de vraag of personeel getraind is om ook in deze omstandigheden op te treden. Anderzijds is het de vraag of de middelen toereikend zijn. Beschikt het wagenpark bijvoorbeeld over voldoende brandstof? Respondenten geven aan dat het met name op improviseren aankomt.

De aansturing van de hulpverlening en de crisiscommunicatie naar de burger zullen op een andere manier verlopen met name bij uitval van telecommunicatie. De geëigende paden van beeldvorming, oordeelsvorming en besluitvorming worden bemoeilijkt onder andere door het ontbreken van informatie. Van belang is dat besluitvormers van tevoren hebben nagedacht hoe hiermee om te gaan.

De inventarisatie, die voor dit onderzoek heeft plaatsgevonden, geeft aan dat de hulpverleningsdiensten zich bewust zijn van hun cruciale rol in de samenleving en dat zij inzien dat de continuïteit van hun diensten van groot belang is. De diensten hebben echter niet allemaal rekening gehouden met uitval van elektriciteit en/of telecommunicatie. Ze gaan ervan uit dat het er is. En als het er niet is, gaan ze ervan uit dat de achtervang middelen toereikend zijn.

In hoofdstuk 6 zijn aanbevelingen geformuleerd. Het kritisch bestuderen of de genomen maatregelen en/of de achtervang middelen afdoende zijn is een onderdeel hiervan. Op dit moment zijn de hulpverleningsdiensten 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 hulpverleningsdiensten te verhogen.

Het ministerie van Veiligheid en Justitie en de orde- en hulpverleningsdiensten hebben de opdracht te bespreken of en hoe opvolging te geven aan de aanbevelingen.

Bijlagen

I. Respondenten interviews

Respondenten	Organisatie
[redacted]	Veiligheidsregio Utrecht
	Veiligheidsregio Rotterdam-Rijnmond
	VtsPN
	VtsPN
	Politiekorps Amsterdam-Amstelland
	Politiekorps Amsterdam-Amstelland
	Politiekorps Zuid-Holland Zuid
	Ambulancezorg Nederland

10.2.e

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 VenJ. 9 december 2010, continuïteit bij uitval of verstoring elektriciteit of ICT. Den Haag.

Ministerie van BZK. Brief aan het Veiligheidsberaad over meldkamers in Nederland. 16-02-2010

[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.

Projectteam Regionaal Crisisplan, Referentiekader Regionaal Crisisplan 2009.

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

Websites
www.rijksoverheid.nl
www.veiligheidsberaad.nl
www.vtspn.nl