STRATEGIE NATIONALE VEILIGHEID
-BEVINDINGENRAPPORTAGE-

Inhoudsopgave Bevindingenrapportage
(VERSIE 180412)

1 Inleiding

1.1 Aanleiding

Risico's en onzekerheden zijn niet uit te sluiten; 100% veiligheid bestaat niet. Ons land kan op talloze manieren worden bedreigd, bijvoorbeeld door natuurgeweld, technisch of menselijk falen, maar ook door mensen of groepen die opzettelijk schade of letsel willen berokkenen of criminele intenties hebben. De nationale veiligheid kan bedreigd worden op Nederlands grondgebied of ten aanzien van Nederlandse belangen in het buitenland.

De nationale veiligheid is in het geding als de vitale belangen van Nederland en de Nederlandse staat in gevaar zijn. Deze vijf vitale belangen zijn: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid en sociale en politieke stabiliteit. De strategie Nationale Veiligheid (strategie NV) is er op gericht aantasting van deze vitale belangen, die mogelijk kunnen leiden tot maatschappelijke ontwrichting, zoveel mogelijk te voorkomen.

1.2 Bouwstenen Strategie Nationale Veiligheid

De werkwijze van deze strategie maakt het mogelijk om een breed en divers palet aan mogelijke risico's in kaart te brengen en onderling te vergelijken, en op basis daarvan keuzes te maken voor te nemen maatregelen.

Het in het kader van de strategie NV ontwikkelde risicodiagram helpt bij het visualiseren van deze risicovergelijking (zie hoofdstuk 2 en bijlage 1.5). Het vergelijken van de risico's kan vervolgens helpen bij het maken van afwegingen en keuzes voor te nemen maatregelen ter verbetering. Waar gaan we nu direct mee aan de slag, wat kan later en wat doen we niet? Dat zijn politieke vragen die in de strategie NV elk jaar weer beantwoord moeten worden.

De kern van de strategie NV bestaat uit drie onderdelen:
1. de Nationale Risicobeoordeling (NRB);
2. de capaciteitenanalyses;
3. de bevindingenrapportage Nationale Veiligheid (het voorliggend document).

Ad 1. NRB
In het eerste onderdeel van de strategie NV, de *NRB,* wordt elk jaar een beperkt aantal risico's geanalyseerd die op Nederland kunnen afkomen en waarvan vermoed wordt dat ze maatschappelijk ontwrichtend kunnen zijn. Dit kunnen risico's zijn die nog niet eerder onderzocht zijn of waarbij zich nieuwe feiten of inzichten voordoen. De risico's worden uitgewerkt tot scenario's[1]. Deze scenario's worden vervolgens door experts op twee punten beoordeeld. Ten eerste scoren de experts op tien impactcriteria, die de vijf vitale belangen kenmerken. Ten tweede schatten de experts in hoe groot de waarschijnlijkheid is dat de scenario's werkelijkheid worden. De gebruikte methodiek van scenarioanalyse en scoring maakt het mogelijk om ook onzekere risico's (risico's waarbij theoretische en/of empirische wetenschappelijke gegevens over waarschijnlijkheid en impact slechts beperkt beschikbaar zijn) te analyseren.

[1] Gedachtenexperiment hoe risico's zich zouden kunnen ontwikkelen tot een daadwerkelijk incident/ramp met als gevolg maatschappelijke ontwrichting. Het zijn nadrukkelijk geen voorspellingen.

In 2011 is de NRB voor het eerst uitgevoerd door experts vanuit het speciaal hiervoor opgerichte analistennetwerk nationale veiligheid (ANV)[2]. Met de oprichting van dit netwerk is een belangrijke stap gezet in het versterken van de strategie NV. Het netwerk moet zorgen voor het efficiënt ontsluiten van benodigde kennis voor het uitvoeren van scenarioanalyses. De kennis en kunde van een aantal gerenommeerde kennisinstituten en inlichtingendiensten vormen de kern van dit netwerk. Het netwerk moet bijdragen aan het verder ontvlechten van enerzijds de scenarioanalyse door inhoudsdeskundigen en anderzijds doorvertaling in beleidsconsequenties door de verantwoordelijke ministeries.

Ad 2. Capaciteitenanalyses
In het tweede onderdeel worden aan de hand van de resultaten uit de NRB capaciteitenanalyses uitgevoerd. Dit zijn analyses waarbij in beeld wordt gebracht in hoeverre de maatschappij is voorbereid op het voorkomen van incidenten enerzijds en het beperken en beheersen van de impact van mogelijke incidenten anderzijds, zoals in de scenario's beschreven.
Op basis van de uitkomsten van deze capaciteitenanalyses wordt een integrale afweging gemaakt welke capaciteiten[3] versterkt zouden moeten worden om de beschreven risico's te reduceren, en dus onzekerheden beter hanteerbaar te maken. Deze capaciteiten zijn of specifiek van aard (gericht op één risico) of breed inzetbaar (toepasbaar bij het beperken van meerdere risico's). Ook de capaciteitenanalyse wordt uitgevoerd op basis van een vooraf vastgestelde systematiek.

Ad 3. Bevindingenrapportage
Als laatste wordt de bevindingenrapportage geschreven. Uit de afzonderlijke capaciteitenanalyses wordt in overleg tussen de verantwoordelijke ministeries een selectie gemaakt uit de door de deskundigen geprioriteerde capaciteiten. Hierbij wordt gelet op onder meer doelmatigheid en toegevoegde waarde in vergelijking met eerder vastgestelde capaciteiten. Deze capaciteiten worden vervolgens door de ambtelijke Stuurgroep Nationale Veiligheid aan het kabinet ter besluitvorming voorgedragen. Het kabinet beslist uiteindelijk op basis van de bevindingenrapportage welke aanbevelingen worden uitgevoerd.

1.3 Leeswijzer

In hoofdstuk 2 worden de belangrijkste uitkomsten van de NRB 2011 kort beschreven. In hoofdstuk 3 wordt het advies gepresenteerd voor de te versterken capaciteiten (specifiek en breed inzetbaar), op basis van de uitkomsten van de capaciteitenanalyses.
In bijlage 1 is een samenvatting van de capaciteitenanalyses opgenomen, zoals gemaakt door de capaciteitenwerkgroepen. In bijlage 2 wordt de gehanteerde werkwijze beschreven.

[2] Het analistennetwerk nationale veiligheid wordt gevormd door een consortium bestaande uit een zestal kennisinstellingen (RIVM, AIVD, WODC, TNO, Clingendael, ISS/EUR). Ten behoeve van de te maken analyses wordt door dit consortium extra kennis en expertise ingeroepen van kennisdragers in de wetenschap, overheid en bedrijfsleven. Kerntaak van het consortium is scenarioanalyses op het terrein van de nationale veiligheid in het algemeen en met name de Nationale Risicobeoordeling in het bijzonder uit te voeren.

[3] Een capaciteit is het vermogen van de (rijks)overheid en private partners om taken uit te voeren die (mede) tot doel hebben de nationale veiligheid te beschermen. Het gaat hierbij om bepaalde combinaties van middelen (bijv. materiaal of informatie-systemen), mensen (civiel, militair, et cetera) en methoden (zoals procedures, plannen, oefenen, PPS-verbanden). Capaciteiten helpen de kans en/of de impact van een of meerdere dreigingen te reduceren. Capaciteiten kunnen het totale spectrum van preventie, preparatie, respons, repressie en nazorg beslaan.

2 Toelichting op de Nationale Risicobeoordeling 2011

2.1 Inleiding

De start van de strategie NV ligt, zoals ook al in de inleiding aangegeven, bij de realisatie van de jaarlijkse nationale risicobeoordeling (NRB), in dit geval de NRB over het jaar 2011 waar in dit hoofdstuk uitgebreider op wordt ingegaan.

2.2 Totstandkoming NRB 2011

In opdracht van de ambtelijke stuurgroep Nationale Veiligheid is de risicobeoordeling dit jaar voor het eerst opgesteld door het analistennetwerk nationale veiligheid (ANV). De ambtelijke stuurgroep Nationale Veiligheid heeft voor de NRB 2011 zes dreigingstypen geselecteerd, die door het ANV zijn uitgewerkt tot in totaal zeven scenario's. Het gaat om de volgende scenario's binnen een aantal bestaande thema's:

- Digitale veiligheid: 'Cyberspionage';
- Klimaat: 'Satellietuitval, veroorzaakt door een zonnestorm';
- Polarisatie en Radicalisering: actualisering van de drie bestaande scenario's 'salafisme' tot één nieuw scenario 'Onrust over salafisme';
- Terrorisme: 'Reactie op exogeen jihadisme';
- Internationale vraagstukken: 'Crisis buiten de Europese Unie';
- Klimaat: Grieppandemie: actualisering van de twee bestaande scenario's 'grieppandemie' tot twee nieuwe scenario's 'Milde grieppandemie' en 'Ernstige grieppandemie'.

In de NRB 2011 zijn voor het eerst reeds bestaande NRB scenario's geactualiseerd. Aanleiding hiervoor zijn recente ontwikkelingen en de gevoerde beleidsinzet in de afgelopen jaren. Voor de twee geactualiseerde grieppandemie scenario's gaat het hierbij om de ervaringen die zijn opgedaan tijdens en naar aanleiding van de grieppandemie (Nieuwe influenza A H1N1) in 2009 en de genomen maatregelen mede naar aanleiding van de uitkomsten van de strategie NV in 2008[4]. Voor de salafisme scenario's geldt dat sinds de vorige analyses in 2007 en 2008 de situatie rond dit onderwerp substantieel is gewijzigd, onder meer door het gevoerde beleid en ontwikkelingen in de samenleving.

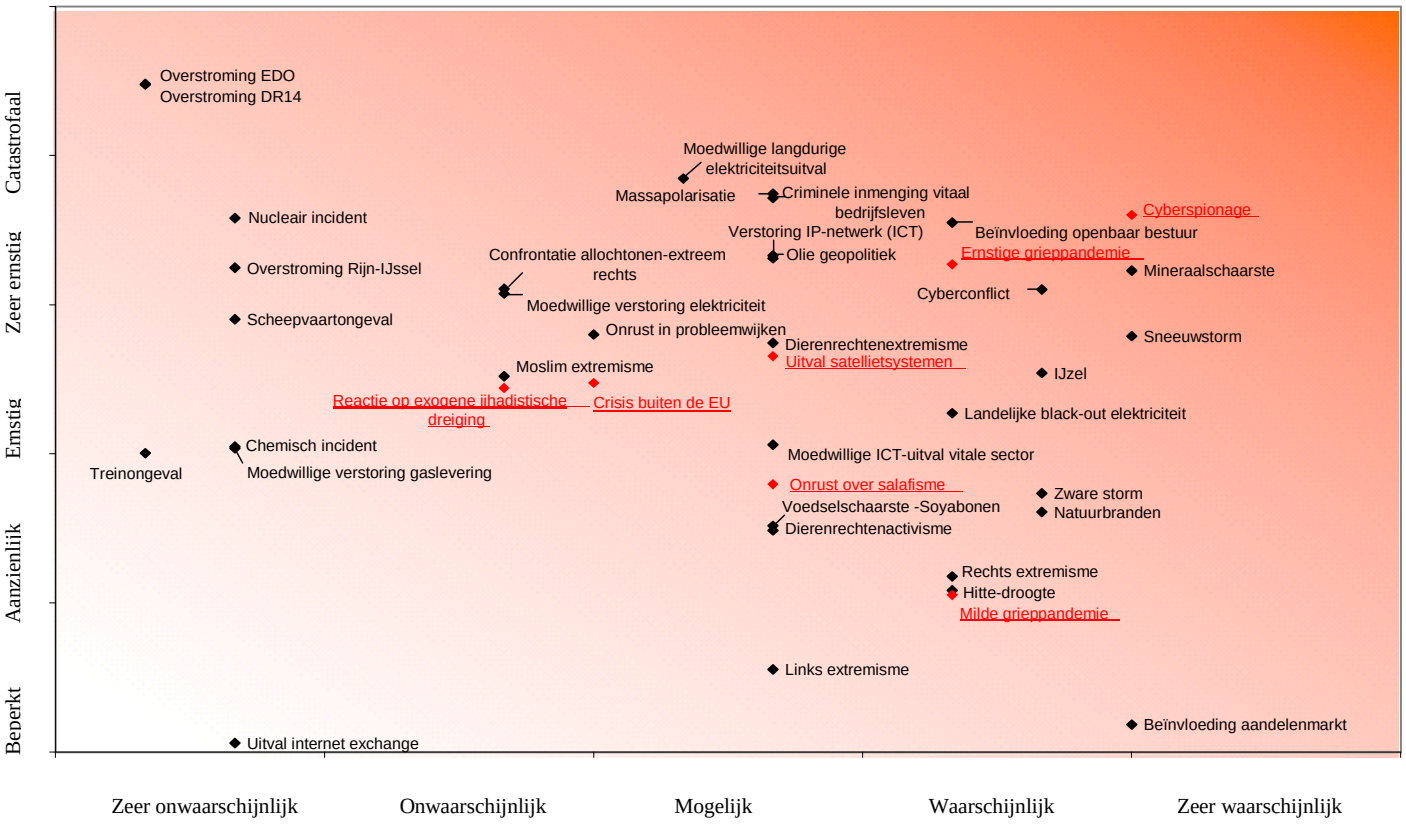
Hierna volgt een korte, *op basis van door het ANV aangeleverde informatie*, beschrijving van de belangrijkste inzichten uit de NRB 2011[5].

2.3 De plaats van de nieuwe scenario's in het risicodiagram

Hoe het risicodiagram te lezen?
De resultaten van de risicobeoordeling door de experts zijn voor elk scenario grafisch weergegeven in het risicodiagram (Figuur 1.1). De scenario's zijn door experts beoordeeld op een tiental impactcriteria en geschat is hoe groot de kans is dat de scenario's werkelijkheid worden.

[4] TK 2007-2008, 30 821, nr. 6
[5] De tekst van de NRB is te downloaden op www.rijksoverheid.nl

In dit diagram heeft elk scenario een positie op grond van de door de experts geschatte waarschijnlijkheid (horizontale as) en impact (verticale as). Bij elkaar vormt dit de relatieve risicopositie van een scenario. De scenario's die in 2011 zijn ontwikkeld zijn met een rode kleur en onderstreept weergegeven. De scenario's uit reeds eerder uitgevoerde NRB's zijn in zwart weergegeven. De eerder gemaakte scenario's op de terreinen grieppandemie en salafisme zijn met de oplevering van de NRB 2011 vervangen door de geactualiseerde scenario's.



Figuur 1 Posities van scenario's in het risicodiagram

Overwegingen bij de NRB en het risicodiagram
Van alle mogelijke scenario's die voor een bepaald risico kunnen worden gemaakt, worden er in de NRB steeds één of slechts enkele uitgewerkt. Voor de meeste scenario's is immers ook een ernstiger variant denkbaar, of juist een minder ernstige. Of varianten met andere eigenschappen, een ander verloop, in andere omstandigheden of een andere context. Gekozen wordt voor die scenario's die een zo goed mogelijk beeld geven van de relevante aspecten van het betreffende risico.

Daarnaast worden de meeste risico's waar de strategie NV zich op richt gekenmerkt door een zekere mate van onzekerheid: het gaat om gebeurtenissen die weinig voorkomen (en waar dus weinig empirische gegevens van zijn) en om scenario's die complex zijn (waar dus veel elementen een rol spelen waarvan de onderlinge samenhang niet altijd bekend is). Daardoor kan het gebeuren dat de individuele risicobeoordelingen van de experts variëren binnen een bepaalde bandbreedte. In het risicodiagram zijn steeds middenwaardes van de expertscores weergegeven.

2.4 Belangrijkste uitkomsten nieuwe scenario's

In deze paragraaf wordt per nieuw scenario kort ingegaan op de uitkomsten. Verder wordt ingegaan op de positie van het scenario in het risicodiagram.

Scenario Cyberspionage
Dit scenario begint met een aantal signalen waaruit bedrijven constateren dat concurrenten over hun kennis beschikken. Van daaruit ontwikkelt het scenario zich verder.

Het scenario valt op door een hoge score op zowel waarschijnlijkheid als impact. De positie van het *cyberspionage* scenario komt ongeveer overeen met dat van *cyberconflict* (ontwikkeld in 2010). Het *cyberspionage* scenario wordt door de experts als zeer voorstelbaar geacht, omdat er concrete aanwijzingen zijn dat gedeelten van het scenario zich kunnen voordoen of, in iets andere vorm, zich zelfs al voor hebben gedaan. Ook blijkt uit diverse incidenten uit de afgelopen periode dat de kwetsbaarheid hoog is. Daar staat tegenover dat er zowel binnen het bedrijfsleven als de overheid steeds meer aandacht wordt besteed aan verhoging van de weerbaarheid. De in het scenario beschreven escalatie op economisch gebied wordt minder waarschijnlijk (hoewel niet onmogelijk) geacht.
De hoge impact wordt volgens de experts vooral veroorzaakt:
- door de ernstige verstoring van het dagelijkse leven en de democratische rechtsstaat;
- door uitval van vitale diensten en de aantasting van het functioneren van de overheid;
- door grote angst en woede in de samenleving;
- door het ontstane wantrouwen in IT als gevolg van de gebeurtenissen.

Ook brengen de spionage activiteiten grote schade toe aan het bedrijfsleven en aan de integriteit van de internationale positie van Nederland.

Scenario's Grieppandemie
Het betreft een scenario over milde grieppandemie en een scenario over ernstige grieppandemie. De scenario's onderscheiden zich door de aannames met betrekking tot de al bestaande en nog aanwezige immuniteit in de populatie en de kansen op ziekenhuisopname en sterfte na infectie. In het milde scenario wordt 8.3% van de bevolking geïnfecteerd; in het ernstige scenario gaat het om 58%.

Evenals het vorige scenario valt het scenario over ernstige grieppandemie op door een hoge score op zowel waarschijnlijkheid als impact. De experts geven aan dat de positie van de *ernstige grieppandemie* redelijk overeen komt met die van het scenario uit 2007, zij het dat zowel de waarschijnlijkheid als de impact iets lager uitvallen. Voor de waarschijnlijkheid heeft een rol gespeeld dat, weliswaar net als in 2007, gebruik is gemaakt van casuïstiek, maar dat er sinds 2009 één pandemie bij is gekomen. Dit leidt tot een geringe bijstelling. De economische schade wordt door de experts minder hoog geschat dan in het 2007 scenario. Een zorgpunt blijft de druk op de gezondheidszorg, in het bijzonder de beperkte Intensive Care capaciteit bij escalatie.

De experts geven aan dat de impact van de *milde grieppandemie* aanzienlijk lager is dan die van het scenario uit 2007. De ervaringen met de Mexicaanse griep hebben duidelijk gemaakt dat de gevolgen van een milde pandemie meevallen.

Het grootste probleem in de respons op een pandemie, of die uiteindelijk mild is of niet, doet zich voor in de beginperiode, omdat dan nog niet bekend is met wat voor nieuw virus men te maken heeft en hoe ernstig de gevolgen (kunnen) zijn. Adequate preparatie en voorlichting

zijn dan van essentieel belang. De experts geven te kennen dat in 2009 is gebleken dat mede door de invloed van de sociale media gemakkelijk verkeerde beelden kunnen ontstaan; de overheid zal hier bij haar communicatie rekening mee moeten houden. Bij een milde pandemie kan maatschappelijke onrust lang na-ijlen, als blijkt dat verregaande maatregelen zijn getroffen die naderhand niet of minder nodig blijken te zijn.

Scenario (Actualisatie) onrust over salafisme
Dit scenario begint met de sluiting van een islamitische middelbare school in een grote stad in Nederland. Dit nadat de onderwijsinspectie al vele jaren had gewaarschuwd dat de kwaliteit van het onderwijs volstrekt onvoldoende was en het leerlingenaantal ver onder de vereiste wettelijke norm lag.

De actualisatie van het onderwerp salafisme heeft eveneens geleid tot een bijstelling van de risicobeoordeling. Vergeleken met de posities van de scenario's *Politiek salafisme*, *Politiek salafisme met geweld* en *Enclavevorming* is de totale impact van het nieuwe scenario *Onrust over salafisme* door de experts in vergelijking met de drie eerdere scenario's lager ingeschat. Ook de waarschijnlijkheid wordt nu lager ingeschat. Dit resultaat hangt samen met een afname van de groei van salafistische groepen in Nederland en hun impact op de moslimgemeenschappen in Nederland (een groter geworden weerstand van deze groep tegen salafisme). Niettemin geven de experts aan dat het van belang blijft alert te blijven op ontwikkelingen op dit vlak.
De totale impact wordt vooral bepaald door de hoge score op de aantasting van de democratische rechtsstaat en, in mindere mate, door de aantasting van de integriteit van de internationale positie van Nederland en de sociaal-psychologische impact. Over de mate van aantasting van de democratische rechtsstaat liepen de meningen van betrokken experts sterk uiteen. Het scenario wordt als beperkt waarschijnlijk beoordeeld.

Scenario Uitval van satellietsystemen
Het scenario Uitval van satellietsystemen als gevolg van een grote zonnestorm heeft tot doel de afhankelijkheden van onze samenleving, in het bijzonder de vitale infrastructuur, van satellietsystemen te onderzoeken en de gevolgen van grootschalige uitval in beeld te brengen.

Dit scenario kent volgens de experts een grote mate van onzekerheid, maar is evenwel geclassificeerd op een ernstige impact en de waarschijnlijkheid is geclassificeerd als mogelijk. Dat heeft te maken met gebrek aan kennis en gegevens, waardoor de kansverdeling 'ernst van de verstoring' versus de 'intensiteit van de zonneactiviteit' niet in kaart is te brengen.

In het scenario is gekozen voor een grote, maar niet maximaal ernstige zonnestorm. De experts geven echter aan dat het wel goed is te realiseren dat de kans op een zeer ernstige zonnestorm weliswaar klein is maar niet nul. De effecten van zo'n gebeurtenis kunnen desastreus zijn. De effecten van het nu uitgewerkte scenario zijn vooral uitval of ernstige aantasting van de vitale producten en diensten met als gevolg een forse verstoring van het dagelijkse leven, het opereren van de hulpdiensten (waardoor een toenemend aantal doden en gewonden), de openbare orde en veiligheid en het functioneren van politiek en bestuur, mogelijk gebrek aan voldoende voedsel gedurende enige periode en grote economische schade.

Scenario Crisis buiten de Europese Unie
Het scenario Crisis buiten de Europese Unie beschrijft een aantal opeenvolgende ontwikkelingen, gebeurtenissen en acties van staten, die uiteindelijk leiden tot een conflict waar (ook) Nederland bij betrokken is en gevolgen van ondervindt.

Dit scenario is qua impact vergelijkbaar gescoord als het scenario *Uitval van satellietsystemen* (namelijk ernstig), maar de waarschijnlijkheid wordt lager ingeschat, zelfs als weinig waarschijnlijk. De impact van dit scenario wordt volgens de experts gedomineerd door de grote aantasting (catastrofaal) van de integriteit van de internationale positie van Nederland. Die aantasting is vooral een gevolg van het escalerende conflict, waarbij Nederland echter niet alleen staat. Het conflict heeft gevolgen voor de handel. De omvang daarvan is moeilijk te bepalen, maar ze kan ernstig zijn.

Scenario Reactie op exogene jihadistische dreiging
Bij het scenario Reactie op exogene jihadistische dreiging spelen twee aspecten een rol: de mogelijkheid van een aanslag en de angst voor een aanslag. In dit scenario gaat het over de angst en ontwrichting die het gevolg zijn van exogene jihadistische dreiging.

Dit laatste scenario is wat impact en waarschijnlijkheid betreft vergelijkbaar gescoord als het scenario *Crisis buiten de Europese Unie*. De waarschijnlijkheid van dit scenario kent een grote onzekerheid, variërend van zeer onwaarschijnlijk tot mogelijk. De combinatie van opeenvolgende gebeurtenissen werd in het kader van de geschetste context (de reactie van samenleving, politiek en overheid) door de meeste experts enigszins voorstelbaar geacht. Echter, enkele experts vonden het scenario als geheel niet voorstelbaar en enkele juist wel. De impact (in haar totaliteit ernstig) wordt voornamelijk bepaald door de aantasting van de democratische rechtsstaat, de toenemende angst en woede in de samenleving en aantasting van de positie van Nederland.

3 Agenderingsadvies Capaciteiten

3.1 Inleiding

In hoofdstuk 2 is aandacht besteed aan de NRB 2011. De resultaten van de NRB zijn vervolgens gebruikt voor het uitvoeren van de capaciteitenanalyse. Tijdens deze analyse is met een groot aantal experts in kaart gebracht welke capaciteiten[6] wij (overheid, bedrijfsleven en burger), uitgaande van de capaciteiten die we nu reeds hebben, zouden moeten versterken om de risico's en dreigingen zoals beschreven in de NRB beter te kunnen hanteren. Zie bijlage 1 voor de samenvatting van de uitkomsten van deze 'capaciteitenanalyses'.

Op basis van door de deskundigen geadviseerde capaciteiten is in overleg tussen de verantwoordelijke ministeries een selectie gemaakt. Hierbij is gelet op onder meer doelmatigheid en toegevoegde waarde in vergelijking met eerder vastgestelde capaciteiten. Verder is vooral gezocht naar capaciteiten die breed inzetbaar zijn zodat een investering maximaal effect heeft en is waar mogelijk rekening gehouden met hetgeen momenteel gebeurt en ontwikkeld wordt. De geselecteerde capaciteiten zijn tenslotte samengevat in een capaciteitsadvies.

Het kabinet beslist op basis van de bevindingenrapportage welke aanbevelingen worden uitgevoerd. In dit hoofdstuk worden de geselecteerde capaciteiten en het capaciteitsadvies beschreven. De niet in het advies opgenomen capaciteiten zijn terug te vinden in bijlage 2 (oriëntatie op capaciteiten).

Opbouw hoofdstuk
In dit hoofdstuk worden in paragraaf 3.2 vier breed inzetbare capaciteiten beschreven, waarvoor versterking wordt geadviseerd. In paragraaf 3.3 worden de geadviseerde specifieke capaciteiten voorgelegd. Paragraaf 3.4 bevat tenslotte de samenvatting van de geselecteerde capaciteiten, het capaciteitsadvies.
.

3.2 Aanbevelingen 2011: breed inzetbare capaciteiten

Gedacht wordt de volgende vier breed inzetbare capaciteiten op te pakken:

1. het vermogen om de vertrouwelijkheid bij aanbesteden te versterken;
2. het vermogen om (potentiële) sociale calamiteiten effectief te beheersen;
3. verdere professionalisering crisiscommunicatie;
4. het vermogen om internationaal de nationale veiligheidsbelangen te beschermen.

Per capaciteit wordt een motivering van de keuze en een omschrijving van de te nemen acties gegeven.

[6] Een capaciteit is het vermogen van de (rijks)overheid, private partners en burgers om taken uit te voeren die (mede) tot doel hebben de nationale veiligheid te beschermen. Het gaat hierbij om bepaalde combinaties van middelen (bijv. materiaal of informatiesystemen), mensen (civiel, militair, et cetera) en methoden (zoals procedures, plannen, oefenen, publiek-private samenweringsverbanden).
Capaciteiten helpen de kans en/of de impact van een of meerdere dreigingen te reduceren.

3.2.1 Het vermogen om de vertrouwelijkheid bij aanbesteden[7] te versterken.

Gaan wij op een zorgvuldige manier om met (informatie)beveiligingsrisico's bij aanbesteden?

Inleiding
Eind 2011 kwam in het eerste nationale Cybersecuritybeeld Nederland[8], digitale spionage als belangrijkste dreiging naar voren, zowel voor de overheid als voor het bedrijfsleven. Dit maakt duidelijk dat het belangrijk is om op een zorgvuldige manier om te gaan met gevoelige kennis en informatie die raakt aan de zogenaamde "kernbelangen"[9].
Het belang van zorgvuldige omgang met informatie en kennis is ook al eerder benoemd in de Kwetsbaarheidsanalyse Spionage (KWAS). Verbeteringen op dit terrein zijn noodzakelijk en intussen ook al ingezet. Een belangrijk aandachtspunt bij het blijvend veilig stellen van deze kennis en informatie is dat ook wanneer een nieuwe opdrachtgever-opdrachtnemer relatie wordt aangegaan zorgvuldig wordt omgegaan met de manier waarop de kennis en informatie in dat kader gedeeld gaat worden.

Recente incidenten zoals de 'Diginotar' kwestie in 2011 en een rij aan recente 'hacks' in binnen- en buitenland, maken duidelijk dat er veel aandacht nodig is voor het beveiligen van digitale kennis en informatie. Nu gebeurt er op dit terrein al veel. Te denken valt daarbij aan de acties die worden ondernomen op basis van de Nationale Cyber Security Strategie (NCSS)[10] en meer specifiek voor cyberspionage, de ingezette acties naar aanleiding van de KWAS[11]. De hier geïdentificeerde capaciteit is een duidelijke, met name niet digitale aanvulling op deze reeds lopende activiteiten. Bij de nadere uitwerking van deze activiteit moet zoveel mogelijk aangesloten worden bij de reeds lopende initiatieven.

Risico's bij aanbesteden
Het proces van aanbesteden c.q. uitbesteden leidt tot het uitwisselen van informatie en kennis met al dan niet 'gekende' partijen. Aandacht voor de mogelijke risico's die hierbij komen kijken en de manieren waarop deze kunnen worden afgedekt is van belang.
De risico's in relatie tot deze capaciteit betreffen met name de eerder genoemde "kernbelangen"**.**

Verlies en misbruik van kennis bij een organisatie die verantwoordelijk is voor kernbelangen kan grote consequenties hebben. Als bijvoorbeeld bouwtekeningen van (nieuw te bouwen) vitale infrastructuur in de verkeerde handen komt ontstaat er een reëel risico. Hierbij kan het ook nog gaan om verlies van technologieën met een lang ontwikkelingstraject. Dit kan dan ook nog grote financiële en economische gevolgen hebben. Aanbesteden houdt dus altijd een risico in. Tegelijk bestaat de mogelijkheid om tijdens een dergelijk traject expliciet rekening te houden met het veiligheidsaspect. Dit middel kan dus ook ingezet worden om het risico van verlies en misbruik van informatie te beperken.

---

[7] Onder aanbesteden wordt hier verstaan, zowel de procedure tot aanbesteden, als de uiteindelijke keuze van het product of dienst.
[8] Zie TK 2011-2012, 26643-220 d.d. 23 december 2011
[9] Definitie afkomstig uit de KWAS (februari 2010). Kernbelangen:
• Datasets en blauwdrukken: hierbij gaat het om in organisaties aanwezige gegevensbestanden, ontwerpen en bouwtekeningen;
• Standpunten en strategie: bijvoorbeeld beleidsstandpunten,langjarige visies en onderhandelingsstrategieën;
• Opkomende kernbelangen en infrastructuur: bijvoorbeeld wetenschappelijke innovaties die in de toekomst in concrete toepassingen belangrijke bijdragen aan de Nederlandse economie kunnen leveren.
[10] TK 2010-2011, 26643, nr. 174
[11] TK 2010-2011, 30821, nr. 13

Als er gesproken wordt over verlies en misbruik bij aanbesteden bij kernbelangen, betreft het twee fases tijdens het proces:
- kennisverlies tijdens aanbesteden (kan informatie veilig beschikbaar worden gesteld tijdens een aanbestedingstraject);
- kennisverlies nadat er een overeenkomst is getekend en wordt geïmplementeerd (onder meer: voldoet het overeengekomen product daadwerkelijk aan bepaalde veiligheidscriteria).

Het is wenselijk om de mogelijke risico's bij aanbesteden bij kernbelangen te beperken.
Bij de uit te voeren acties kan gedacht worden aan:
- het vergroten van de kennis van het geschetste risico van kennis en informatie 'lekken' tijdens aanbesteden en uitvoering van kennisgevoelige projecten en de mogelijkheden om dit te voorkomen;
- het expliciet stellen van voorwaarden om mogelijke kwetsbaarheden af te dekken tijdens aanbestedingstrajecten en het daadwerkelijk toetsen aan deze voorwaarden.

Aangezien de beschreven problematiek niet alleen voor de rijksoverheid opgaat, maar ook zeer relevant is voor onder meer eigenaren en beheerders van vitale infrastructuur en wetenschappers, is het wenselijk te bezien hoe de bovenbeschreven inzet verbreed kan worden naar deze doelgroepen.

3.2.2 Het vermogen om (potentiële) sociale calamiteiten effectief te beheersen

Zijn wij voldoende toegerust op het beheersen of voorkomen van sociale onrust en mogelijke onlusten?

Inleiding
De beoordelingen van de scenario's over polarisatie en radicalisering (scenario: *'Onrust over salafisme'*) en terrorisme (scenario: *'Reactie op exogeen jihadisme'*), maar ook de rellen in Londen in de zomer van 2011 geven aan dat het nodig is om de structurele voorbereiding op calamiteiten met een sociaal (openbare orde) karakter te versterken.

Waarom is deze capaciteit belangrijk?
Bij het niet tijdig of onvoldoende anticiperen op signalen van maatschappelijke onrust kan de situatie op lokaal, regionaal en in bijzondere gevallen nationaal niveau escaleren. De klassieke opschalingstructuur is vaak niet van toepassing op dreigende sociale onrust en veel gemeenten zijn daarmee niet standaard voorbereid op vragen als: met welke acties kan maatschappelijke onrust en escalatie worden voorkomen, en wie is waarvoor verantwoordelijk. Beheersing van dit type vraagstukken vraagt veel van een goede en gestructureerde samenwerking tussen een zeer divers 'palet' aan betrokken partijen.

In gemeenten en regio's zijn rampenplannen voor fysieke crises en rampen voorhanden, maar op calamiteiten met een sociaal karakter moet men ook voorbereid zijn. Een sociaal calamiteitenplan, het proces om dit te realiseren en/of het daadwerkelijk oefenen met een scenario van maatschappelijke onrust vormen een goede voorbereiding op het beheersen van onrust en kan zo escalatie verminderen of voorkomen. Het gaat hierbij om ontwikkelingen, conflicten en incidenten die het risico in zich dragen een bedreiging te vormen voor de sociale en politieke stabiliteit op lokaal, regionaal en/of nationaal niveau. Te denken valt aan

bijvoorbeeld spanningen tussen groepen zoals in Culemborg hebben plaatsgevonden en incidenten rondom gebedshuizen. Een goede voorbereiding op de omgang met sociale onrust en spanningen kan echter ook van meerwaarde zijn bij openbare orde vraagstukken en 'fysieke' rampen en crises, zoals bijvoorbeeld de onrust die speelde onder burgers bij de brand in Moerdijk begin 2011.

Als gekozen wordt voor een sociaal calamiteitenplan zijn belangrijke elementen die hierin uitgewerkt moeten worden:
- hoe vroegtijdig zicht te krijgen op spanningen of ongewenste vormen van bijvoorbeeld radicaal gedrag;
- voorbereid zijn op situaties die vragen om een weerwoord of reactie anderszins op gesignaleerde spanningen door de overheid en haar partners;
- in staat zijn om effectief (de-escalerend) te kunnen handelen in geval van een daadwerkelijke crisis/calamiteit met betrekking tot het escaleren van spanningen door de overheid en haar partners.

Noodzakelijk hierbij is de opbouw van een formeel en informeel netwerk van partijen, die een rol kunnen spelen bij al deze elementen.

Een sociaal calamiteitenplan is dus tweeledig. Het richt zich op preventie met de-escalatie en op repressie als sluitstuk. De ontwikkeling van sociale calamiteitenplannen op lokaal niveau is geen nieuw initiatief. Er zijn door diverse organisaties en gemeenten plannen ontwikkeld. De afgelopen jaren is deze ontwikkeling vanuit de rijksoverheid door middel van verschillende activiteiten gestimuleerd. Deze inzet is echter tot nog toe van beperkte schaal geweest.

Het is wenselijk om de structurele voorbereiding op calamiteiten met een sociaal (openbare orde) karakter te versterken.
Bij uit te voeren acties kan gedacht worden aan:
- dat gemeenten zich in het kader van hun integrale veiligheidsbeleid voorbereiden op eventuele sociale onrust. Lokaal oefenen en een sociaal calamiteitenplan kunnen hier onderdeel van uitmaken;
- dat via het Kernbeleid Veiligheid van de VNG en het Centrum voor Criminaliteitspreventie Veiligheid (CCV) aandacht gevraagd wordt voor en informatie wordt gegeven hoe gemeenten sociale onrust kunnen herkennen en aanpakken;
- in specifieke gevallen van lokale sociale onrust kan er een praktijkteam ter ondersteuning van de betreffende gemeente worden opgericht[12].

[12] Een praktijkteam kan ingezet worden voor overlastgevende situaties. Dit praktijkteam biedt gemeenten ondersteuning als er sprake is van overlastgevend gedrag van jongeren waarbij het risico bestaat dat gedrag leidt tot situaties van maatschappelijke onrust en ontwrichting. Het praktijkteam wordt afhankelijk van de situatie voor kortere of langere tijd ingezet. De samenstelling is afhankelijk van de problematiek en de ambities.

3.2.3. Verdere professionalisering crisiscommunicatie

Hoe kan de overheid de crisiscommunicatie zodanig moderniseren, dat deze beantwoordt aan de beleving van het publiek?

Inleiding
In een tijd, waarin moderne technologieën snelle communicatie mogelijk maken en burgers steeds meer worden gestimuleerd tot zelfredzaamheid is crisiscommunicatie bij iedere (dreigende) crisis of incident een onmisbaar instrument in de crisisbeheersing. De analyses van de scenario's terrorisme, grieppandemie en polarisatie en radicalisering bevestigen dat een optimale inzet van crisiscommunicatie cruciaal is.

De afgelopen jaren heeft crisiscommunicatie zich tot een volwaardige discipline ontwikkeld. Communicatie staat vooraan op de agenda van ieder crisisoverleg; het geeft een beeld van de wijze waarop het publiek de gebeurtenissen ervaart.
De doelstelling van crisiscommunicatie is in iedere situatie drieledig. Het *eerste doel* is de communicatie over de feitelijke situatie (informatievoorziening): wat is er aan de hand, wat ging vooraf, hoe kan de situatie zich ontwikkelen. Het *tweede doel* is communicatie over de schadebeperking (handelingsperspectieven): wat kan de ontvanger doen om schade te voorkomen of te beperken en zijn eigen veiligheid te waarborgen. Het *derde doel* is duiding geven (betekenisgeving) aan de crisis. De burger verwacht informatie over de feitelijke situatie en handelingsperspectieven voor schadebeperking van professionals te krijgen. Duiding zoekt de burger bij de bestuurder; een belangrijke competentie voor een bestuurder is dan ook om in crisistijd in de juiste woorden en op het juiste moment betekenis te kunnen geven aan de situatie.
Ook de organisatie van de crisiscommunicatie is essentieel voor een slagvaardige communicatie in crisistijd; om tijdig de juiste boodschap naar pers en publiek te kunnen communiceren, is het van belang dat de crisiscommunicatie professionals mandaat krijgen om zelfstandig en actief te communiceren over feiten, gebeurtenissen en omstandigheden en over consequenties van genomen beslissingen en gemaakte keuzes, voor zover deze zichtbaar zijn voor pers en publiek. Daarmee krijgt crisiscommunicatie een mandaat, dat vergelijkbaar is met het mandaat dat andere operationele diensten hebben om bij een incident of crisis op te treden.

Bij uit te voeren acties kan gedacht worden aan:
- dat de rijksoverheid bij de veiligheidsregio's gaat aansturen op de inrichting en beschikbaarheid van een kwantitatief en kwalitatief solide en uniform ingericht crisiscommunicatiepool;
- dat de rijksoverheid hiervoor –in nauwe samenwerking met de veiligheidsrgio's- richtlijnen ontwikkelt voor de crisiscommunicatie, onder meer op het gebied van:
  - uitgangspunt (voorzien in maatschappelijke behoefte)
  - doelstellingen (informatievoorziening, schadebeperking, duiding)
  - wijze van organisatie (sleutelfunctionarissen, modelmandaat)
- dat, om bestuurders beter voor te bereiden op hun rol in de crisiscommunicatie (duiding), er trainingen gericht op het overbrengen van de boodschap komen

3.2.4 Het vermogen om internationaal de nationale veiligheidsbelangen te beschermen.

Hoe gaan wij om met internationale incidenten die van invloed zijn op onze nationale veiligheid? Hoe goed zijn wij op dergelijke incidenten voorbereid?

Inleiding
Uit de capaciteitenanalyses van de scenario's *'Crisis buiten de Europese Unie'*, C*yberspionage'*, *'Grieppandemie'* en *'Reactie op exogeen jihadisme'* komt naar voren dat de internationale omgeving van grote invloed kan zijn op de nationale veiligheid. Zowel waar het gaat om de origine en oorzaak van een risico als ook om de mogelijkheden om het hoofd te kunnen bieden aan dit risico. Het Nederlands handelen in deze internationale omgeving kan daarom van grote meerwaarde zijn om onze nationale veiligheid te waarborgen. In de NRB 2010 is voor het eerst het onderwerp 'integratie nationale veiligheidsbelangen in internationaal beleid' opgevoerd. In reactie op de NRB 2010 is ingezet op de versterking van de samenhang tussen het internationale en nationale veiligheidsbeleid. De analyse in het kader van de NRB 2011 is een onderdeel van deze versterking en moest leiden tot mogelijke aangrijpingspunten voor versterking op het thema nationaal-internationaal. Deze aangrijpingspunten zijn gevonden, maar er is tijdens de analyse ook het inzicht ontstaan dat de complexiteit en diversiteit aan internationale vraagstukken vraagt om aanvullende analyses. Hierbij kan gerichter ingezet worden op vraagstukken die internationaal een rol spelen, maar die in het huidige scenario (*'Crisis buiten de Europese Unie'*) niet echt naar voren kwamen. Een eerste stap hierin kan de analyse voor de NRB 2012 zijn.

De nationale veiligheid wordt in toenemende mate bepaald door vraagstukken die een internationale herkomst kennen. Het betreft kwesties die in binnen- en buitenland spelen en die onze vitale belangen in Nederland of daarbuiten raken.

Het bewust en integraal omgaan met onze vitale belangen in relatie tot de internationale context waarin wij staan is dan ook van groot belang en zal de komende jaren alleen maar toenemen in betekenis. Er zijn echter een aantal uitdagingen bij de realisatie van een integrale aanpak:

- de complexiteit van de vraagstukken is groot. Buitenlandse ontwikkelingen zijn divers en de mogelijkheden om deze ontwikkelingen te beïnvloeden zijn voor Nederland meestal beperkt;
- Nederlandse (vitale) belangen in het buitenland zijn lang niet altijd eenduidig of evident;
- op veel plekken – zowel binnen de overheid als bij bedrijven – is informatie en kennis beschikbaar, het is echter een uitdaging om deze informatie in samenhang te analyseren;
- de manier waarop Nederland omgaat met dit soort vraagstukken bepaalt echter in sterke mate of we mogelijke risico's die samenhangen met deze vraagstukken adequaat het hoofd kunnen bieden.

Het is dan ook gewenst om op basis van periodieke risicoanalyse, meer gestructureerd potentiële dreigingen voor de Nederlandse veiligheid op strategisch niveau te benoemen. Hierdoor kunnen zich in het buitenland ontwikkelende crises vroegtijdig geïdentificeerd worden, zodat ook beleidsinterventies tijdig kunnen worden geformuleerd en ingezet.
Een beter en integraler inzicht in (potentiële) bedreigingen en de strategische betekenis hiervan voor Nederland maakt het mogelijk effectief regie te voeren op het Nederlandse handelen in internationale context. Zodat dit handelen ook sneller en coherenter kan zijn wat onder meer de inzet van diplomatie en inlichtingendiensten nog effectiever kan maken.

Essentie is dat we van een *registrerende houding naar een meer regisserende werkwijze toe moeten* waar het gaat om het beschermen van onze vitale belangen in Nederland, maar juist ook daar buiten.

Het is van belang om vroegtijdig te kunnen beschikken over een integraal inzicht in mogelijke dreigingen en in de strategische belangen die bedreigd kunnen worden, de zogenaamde vroege signalering. Voor deze signalering is de inzet van diplomatie en/of inzet van inlichtingendiensten nodig. Om de vroege signalering te versterken wordt geadviseerd:

Stelselmatig de ontwikkelingen in de wereld en de implicaties daarvan op de nationale veiligheid in kaart brengen. Daartoe richten BZ en Defensie samen met VenJ een strategische monitorfunctie in, die tevens zal worden gekoppeld aan de Strategie NV. Op deze wijze kan meer aandacht worden besteed aan de internationale bedreigingen van de nationale veiligheid.

Om een breder zicht te krijgen in de betekenis van internationale risico's voor het nationale veiligheidsterrein wordt ook geadviseerd om in de komende NRB een internationaal scenario op te nemen.
.

3.3 Aanbevelingen 2011: specifiek inzetbare capaciteiten

De volgende specifiek inzetbare capaciteiten worden naar aanleiding van de verschillende capaciteitenanalyses aanbevolen:
1. versterken van de detectie van aanvallen op netwerken en informatiesystemen;
2. versteviging van de implementatie van de (informatie)beveiligingskaders Rijk;
3. vergroten weerbaarheid tegen gevolgen satellietuitval door een zonnestorm;
4. nadere uitwerking van de aanpak van gewelddadige eenlingen.

Per capaciteit wordt een motivering van de keuze, omschrijving van de te nemen acties en het benoemen van een trekker gegeven.

3.3.1 Versterken van de detectie van aanvallen op netwerken en informatiesystemen

De informatietechnologie ontwikkelt snel. Kunnen we snel genoeg ontdekken dat er, met steeds weer nieuwe technologieën, inbreuk plaats vindt op de eigen informatiesystemen?

Inleiding
Technologie neemt een steeds prominentere plaats in onze samenleving in. We maken in toenemende mate gebruik van informatiesystemen voor opslag, verwerking en uitwisseling van informatie. Tijdige detectie van aanvallen op informatiesystemen en mogelijk ontvreemding van gevoelige gegevens is van groot belang om de aard en impact van die aanvallen te kunnen beoordelen en op basis daarvan adequaat en slagvaardig te kunnen handelen. Het monitoren van informatiesystemen is daarvoor een hulpmiddel. Detectie van aanvallen verbetert als van verschillende plekken in de nationale ICT-infrastuctuur signalen kunnen worden verzameld, en als detectie op verschillende manieren plaatsvindt.

De rijksoverheid gaat dit jaar uitwerken op welke manier de detectie van aanvallen op de nationale ICT-infrastructuur, te beginnen bij de rijksoverheid, het beste kan plaatsvinden. Hierbij wordt gekeken hoe op de meest effectieve wijze verschillende digitale aanvallen kunnen worden gedetecteerd. Detectie van zogenaamde *advanced persistent threats* zullen hieronder moeten vallen, maar ook de verspreiding van *botnets* binnen de infrastructuren. Tegelijk worden eisen geformuleerd om te bepalen hoe een rijksinformatiesysteem gemonitord moet worden en zo ja, welke soorten monitoring daarvoor benodigd zijn. Daarbij wordt rekening gehouden met grondrechten zoals de bescherming van de privacy. Tenslotte wordt bezien waar en op welke wijze de resultaten van de monitoring worden geaggregeerd en welke voorzieningen nodig zijn om adequaat te kunnen handelen.
Mogelijke dreigingen of risico's beperken zich echter zeker niet tot de rijksoverheid alleen. De rijksoverheid zal het belang van goede detectie van aanvallen op informatiesystemen actief uitdragen aan private partijen en de wetenschap. De rijksoverheid wil in gesprek gaan met private partijen en de wetenschap om tot afspraken te komen over de uitwisseling van monitoringsinformatie die deze organisaties zelf verzamelen, bijvoorbeeld via Security Operating Centres van dienstverlenende organisaties. Het Nationaal Cyber Security Centrum (NCSC) zal hier in het bijzonder een actieve rol spelen.
Aandacht voor detectie van aanvallen op informatiesystemen is geen eenmalige aangelegenheid. Vanwege de snelle technologische ontwikkelingen blijft dit constante aandacht vragen zodat de implementatie mee ontwikkelt met de technische mogelijkheden en de dreigingen.

Om tijdige detectie en een adequate aanpak mogelijk te maken van een aanval op informatiesystemen die een kernbelang vertegenwoordigen worden de volgende acties voorgesteld:

- de rijksoverheid inventariseert in 2012 welke typen monitoring het meest effectief zijn, ontwikkelt criteria en waarborgen om te bepalen voor welke onderdelen van de nationale ICT-infrastructuur monitoring ten behoeve van detectie van aanvallen nodig is en welke technische en personele voorzieningen nodig zijn voor adequate detectie en respons en aan welke voorwaarden deze moeten worden gebonden;
- de rijksoverheid ontwikkelt in 2012 een businesscase en implementatieplan voor detectie van cyberaanvallen op de informatiesystemen bij het Rijk en start begin 2013 een pilot om de detectie te toetsen;
- daarnaast stelt de rijksoverheid in 2012 in samenwerking met private partijen modelafspraken op om met private vitale organisaties afspraken te kunnen maken over monitoring en start begin 2013 een pilot om de uitwisseling van monitoringsinformatie met private partijen te toetsen.

Het NCSC zal beide trajecten, in samenspraak met de AIVD en andere partners, als uitvoerende organisatie coördineren, onder de beleidsverantwoordelijkheid van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (rijksoverheid) en het ministerie van Veiligheid en Justitie (vitaal).

3.3.2 Implementatie van de (informatie)beveiligingskaders Rijk

De technologische mogelijkheden ontwikkelen vaak sneller dan de beveiliging daarvan. Als er binnen het Rijk een nieuwe technologie in gebruik wordt genomen, gebeurt dit dan conform de informatiebeveiligingskaders?

Inleiding
De ontwikkelingen in het digitale domein gaan in een erg hoog tempo. De wens bestaat bij veel mensen om deze technieken (bijvoorbeeld tablets en smartphones) in de dagelijkse praktijk toe te passen ook wanneer dat is in relatie tot 'gevoelige' informatie. Het is een uitdaging om de maatregelen en technische beveiligingsoplossingen aan te laten sluiten op deze technologische ontwikkelingen en daarmee de inzet van deze nieuwe technische middelen (uitgaande van de hiervoor geldende standaarden en normen) mogelijk te maken. Parallel hieraan dienen echter ook de bestaande informatiebeveiligingsnormen en standaarden actueel gehouden te worden.

Bestaand beveiligingskader Rijk
Buiten de specifiek op spionage gerichte acties zijn er ook maatregelen met een algemeen effect op het veiligheids- en beveiligingsniveau bij de rijksdienst. Een goed voorbeeld hiervan zijn de informatiebeveiligingskaders van het Rijk, een verplicht uitgangspunt voor de bescherming van informatie(systemen). Het gaat hierbij om het Beveiligingsvoorschrift 2005, het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007) en het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie 2004 (VIR-BI 2004)[13].

Implementatie
Begin 2012 wordt gestart met de implementatie van de Baseline Informatiebeveiliging Rijk (BIR) voor de generieke rijksbrede infrastructuur (tot en met het niveau Departementaal Vertrouwelijk) bij de ministeries. Een passend niveau van gegevensbeveiliging, zowel in de regel als in de uitvoering, is een eerste vereiste om het risico van digitale spionage te beperken. Een hogere weerstand wordt bereikt door er zorg voor te dragen dat het VIR en VIR-BI zijn geïmplementeerd op elk departement. Met de implementatie van het BIR, wordt een goede basis gelegd voor de rijksbrede infrastructuur op het niveau Departementaal Vertrouwelijk. Voor waar het de grotere te beschermen belangen betreft (Staatsgeheim Confidentieel, Geheim en Zeer Geheim) is implementatie en naleving van de voorschriften van wezenlijk belang. Dit vergt een forse inspanning, al gaat het hier om een kleiner deel van de informatie die binnen het Rijk omgaat. Juist rubriceren is daarbij de basis.

Waar gaat het om?
Het principe achter de beveiligingskaders is risicomanagement. Met dit proces wordt bepaald of een maatregel voldoende bijdraagt aan de bescherming van het belang, het op een andere manier al is afgedekt of efficiënter afgedekt kan worden en wat er eventueel nog moet worden gedaan om het belang te beschermen. Kosten en effectiviteit zijn hierbij nadrukkelijk punt van aandacht. Feitelijk moet voorafgaand voor alle 'nieuwe' manieren van werken een risicoanalyse gemaakt worden. Met behulp van risicomanagement kan dan bepaald worden of, hoe en waar het geïmplementeerd wordt.

Daarnaast is het van belang de kaders actueel te houden (evaluatie eens in de vijf jaar). Door technologische vooruitgang veranderen immers ook het soort dreigingen waartegen

[13] Het VIR-BI 2004 zal worden vervangen door het VIR-BI 2012

beschermd moet worden. Vastgesteld moet worden of die dreigingen (nog) voldoende gedekt worden met de geldende kaders. Meer praktisch en daarmee veel afhankelijker van (technologische) ontwikkelingen zijn de middelen die nu goedgekeurd zijn omdat ze voldoende bescherming bieden tegen bijvoorbeeld diefstal van informatie. Dat vraagt om een goed en actueel zicht op (mogelijke) dreigingen, onder andere voortkomend uit technologische vooruitgang, en een voortvarende ontwikkeling en toetsing van mogelijke technische beveiligingsmiddelen. Uiteraard geldt eenzelfde constatering voor organisatorische en voor fysieke beveiliging. Het VIR 2007 heeft een onderhoudscyclus van 5 jaar; met de herziening ervan is in 2012 gestart. Het herziene VIR-BI wordt in 2012 van kracht. De BIR heeft een jaarlijkse onderhoudscyclus.

De implementatie van de BIR is gestart bij de ministeries door het uitvoeren van een analyse tussen *ist* en *soll* situatie (*fit-gap* analyse). De implementatie van de BIR wordt afgesloten door een audit.

Met de risicoanalyse, het risicomanagement, de implementatie van de maatregelen (waaronder het aanschaffen van veilige middelen) en het goed beheren zijn kosten gemoeid; het gaat daarbij om het realiseren van het gewenste en noodzakelijke niveau van vertrouwelijkheid van de informatie (in welke vorm dan ook).

De I-strategie van de rijksdienst spreekt van een permanente investering in de weerbaarheid van de rijksoverheid tegen (on)opzettelijke inbreuken, in het vergroten van het herstelvermogen bij onverhoopt geslaagde inbreuken en in processen ten aanzien van het omgaan met privacygevoelige gegevens. Onderdeel van de vergroting van de weerbaarheid is het hebben van solide informatiebeveiligingsconcepten. Een belangrijke lijn daarbij is het investeren in gegevensbeveiliging, in aanvulling op apparaat- en netwerkbeveiliging. Een tweede lijn is die van onbewuste risicomijding naar bewust en verantwoord risicomanagement. Medewerkers moeten veilig met informatie kunnen en willen omgaan. De gewenste inzet van zelfgekozen middelen in combinatie met de enorm toegenomen communicatiemogelijkheden (social media) maken dat een ambtenaar anno 2012 zich meer dan ooit bewust moet zijn van de risico’s van het gebruik van digitale middelen, en daar dus ook verstand van moet hebben. De rijksdienst zal medewerkers hierin ondersteunen door te voorzien in adequate middelen en in heldere regels en adviezen.

Geadviseerd wordt de volgende acties in gang te zetten:
- controleer de implementatie van het VIR 2007 en het VIR-BI 2004. De Algemene Rekenkamer heeft hier onderzoek naar verricht bij de verschillende departementen. Implementeer de bevindingen conform het principe voldoe of leg uit;
- implementeer het BIR in de rijksbrede infrastructuur. Dit vormt een onderdeel van de eind 2011 vastgestelde I-strategie rijksoverheid, in het bijzonder van de thema's 'I-infrastructuur voor de rijksambtenaar' en 'Vertrouwen en beveiliging van informatie';
- houd een actueel overzicht van ontwikkelingen en dreigingen bij.

3.3.3. Vergroten weerbaarheid tegen gevolgen satellietuitval door een zonnestorm

Zijn we voorbereid op de uitval van satellieten en van de diensten die gebruik maken van satellietsignalen, en weten we wat we moeten doen als dit gebeurt?

Inleiding
Satellietuitval door een zonnestorm met als gevolg het uitvallen van satellietsignalen is een nieuw dossier voor de rijksoverheid. Het scenario van satellietuitval maakt duidelijk dat de kans op uitval van satellieten door met name de activiteiten van de zon behoorlijk groot is[14]. De afhankelijkheid van satellietgebruik is tegelijkertijd groot en zal in de toekomst alleen nog maar toenemen. Uit buitenlandse experimenten blijkt dat de impact van uitval van satellietsignalen voor bijvoorbeeld navigatie groot is, zowel qua omvang van verstorende effecten als de gevolgen. In verschillende landen is momenteel sprake van een bewustwordingsproces en worden maatregelen geformuleerd.

Het ministerie van Infrastructuur en Milieu heeft eerder onderzoek laten uitvoeren naar satellietuitval in verband met het belang van gebruikers van satellietdiensten binnen het eigen beleidsdomein, zoals transport en waterbeheer. Dit onderzoek en ook het huidige NRB-scenario laten echter zien dat bijna alle (vitale) sectoren kwetsbaar zijn voor satellietuitval omdat zeer veel systemen en producten afhankelijk zijn van satellietsignalen. Dit betreft bijvoorbeeld ook de communicatiesector, de gezondheidszorg, de energiesector, de financiële sector en de primaire voedselvoorziening. Het ligt daarom voor de hand om de aanbevolen acties in een rijksbreed kader op te pakken, bijvoorbeeld naar analogie van de in 2010 en 2011 uitgevoerde Capaciteitsanalyse Elektriciteit en Telecom (CAET) . Voordeel van de eerdere CAET-aanpak is dat het gebruikersaspect door het vroegtijdig betrekken van het bedrijfsleven en gebruikersorganisaties voldoende geborgd wordt. Uiteraard moet er ook voldoende inzet zijn vanuit de betrokken vakdepartementen.

In Nederland is tot nu toe weinig aandacht voor satellietuitval en er is dan ook geen expliciet beleidskader voorhanden, noch een duidelijke kennisinfrastructuur en alarmeringsfunctionaliteit. Meer aandacht en prioriteit lijken gewenst voor dit dossier.

Verbetering kennispositie
Het kennisniveau dient op twee vlakken te worden vergroot. Ten eerste is meer inzicht nodig in het fenomeen zonneactiviteit en de daaruit voortvloeiende mogelijke gevolgen van grootschalige satellietuitval. Dit betreft zowel satellietsystemen voor navigatie (positiebepaling en tijdssignaal) als voor communicatie en dataverkeer. In het verlengde hiervan dient ook de informatiepositie van overheid en gebruikers in geval van een daadwerkelijke dreiging (alarmering) verbeterd te worden. Internationaal zijn er verschillende instituten die de zonneactiviteit monitoren en daarmee in een vroegtijdig stadium kunnen waarschuwen voor een mogelijk schadelijke zonnestorm. De inschatting is dat hierbij aangesloten kan worden en een Nederlandse alarmeringsfunctionaliteit relatief snel gerealiseerd kan worden. Ook de aanbieders van dergelijke systemen zullen betrokken moeten worden.

Ten tweede is meer inzicht nodig in de mate van kwetsbaarheid van Nederland. Binnen heel veel branches en sectoren is niet of onvoldoende in kaart gebracht welke van de gebruikte

[14] Andere oorzaken van uitval van satelliet(signalen), zoals het moedwillig verstoren of vervalsen van signalen, zijn niet bekeken. Mogelijk dat hier in de toekomst nog nader naar gekeken moet worden.

systemen en producten afhankelijk zijn van satellietsignalen en dus potentieel kwetsbaar zijn. In het verlengde hiervan is vaak ook niet bekend wat de gevolgen van uitval zijn voor de eigen activiteiten. Inventarisatie van systemen en kwetsbaarheden zou tevens tot bewustwording en risicocommunicatie richting gebruikers kunnen leiden.
Op basis van de opgedane kennis op genoemde twee vlakken dient vervolgens bekeken te worden wat dit betekent voor de nationale crisisvoorbereiding waar het gaat om dit type risico. Mogelijk is een speciaal crisisplan voor satellietuitval wenselijk.

Beschikbaarheid alternatieve voorzieningen
Aan de hand van de vergaarde kennis kan vervolgens ook inzichtelijk worden gemaakt welke terugvalopties noodzakelijk en mogelijk zijn. Met name bij vitale sectoren of -functies is de beschikbaarheid van alternatieve voorzieningen die bij satellietuitval de functionaliteit overeind houden, van groot belang. De inschatting is dat alternatieve voorzieningen feitelijk al beschikbaar zijn. Wel zijn beleidsmaatregelen nodig om gebruik op langere termijn te waarborgen. Voorbeelden hiervan zijn het eLORAN[15] systeem voor plaats- en tijdsbepaling via radiozenders op het land en het fijnmazige plaatsbepalingsysteem van het kadaster. Bij deze alternatieven moet de inschatting worden gemaakt of bij het uitrollen hiervan gewacht zou moeten worden tot de kennispositie op orde is of dat gezien de reëel beschouwde risico's ze niet al op kortere termijn ingevoerd moeten worden.

Problemen ontstaan door directe effecten zonnestormen
Niet direct voortkomend uit het gebruikte scenario, maar tijdens de capaciteitenanalyse wel geïdentificeerd, is het probleem van de zogenaamde directe effecten van zonnestormen. Dit betreft onder andere het uitvallen van vaste netwerken op het land (elektriciteit, dataverkeer) door de inwerking van elektromagnetische straling als gevolg van (heftige) zonneactiviteit. Geadviseerd wordt om dit probleem in kaart te brengen, bij voorkeur gelijktijdig met de problematiek van de – indirecte - satellietuitval. Dit laatste is belangrijk omdat er naar verwachting sprake is van stapeling van risico's en keteneffecten tussen beide effecten. Zo kunnen alternatieve systemen om de gevolgen van satellietuitval tegen te gaan (bijvoorbeeld mobiele telefonie gebruiken in plaats van satelliettelefoons) op hun beurt uitvallen als het landzijdige elektriciteitsnet uitvalt. Bij het inzichtelijk maken van de risico's dienen zeer uiteenlopende disciplines te worden betrokken. Ook vanwege dit aspect lijkt een overall aanpak naar analogie van het CAET-traject wenselijk

Geadviseerd wordt de volgende acties in gang te zetten (in chronologische volgorde):
- verbeteren van de kennispositie van overheid en gebruikers, zowel wat betreft een beter inzicht in het fenomeen zonne-uitbarstingen en de gevolgen hiervan;
- inrichten van een alarmeringsfunctie ten behoeve van het tijdig waarschuwen voor het optreden van uitbarstingen (alarmeringsfunctionaliteit);
- verkrijgen van inzicht in de kwetsbaarheden bij gebruikers van producten en systemen die afhankelijk zijn van satellietsignalen;
- afhankelijk van de uitkomsten van voornoemde inventarisatie van kwetsbaarheden besluiten tot de ontwikkeling van terugvalopties;
- ontwikkelen van een crisisplan satellietuitval, indien sprake is van (blijvende) grote kwetsbaarheden.

[15] Een plaats- en tijdsbepaling systeem, dat geen gebruik maakt van satellieten maar een aantal radiozenders in Engeland, Frankrijk, Duitsland, Denemarken en Noorwegen.

3.3.4. Aanpak van gewelddadige eenlingen

Zijn we in voldoende mate in staat om potentiële risico's van potentieel gewelddadige eenlingen te signaleren en te voorkomen?

Inleiding
Uit de capaciteitenanalyse van polarisatie en radicalisering is, in het kader van het tegengaan van extremisme, de aanpak van 'gewelddadige eenlingen' als prioriteit naar voren gebracht. Het gaat hier om een relatief nieuwe dreiging, die zich echter in de afgelopen periode in meerdere ernstige incidenten heeft gemanifesteerd.

Het betreft hier personen die zonder medewerking van anderen een dreiging vormen in woord of gedrag als gevolg van een individueel doorlopen proces richting geweld. Voorbeelden hiervan zijn de gebeurtenissen in:
- Apeldoorn Koninginnedag 2009;
- Oslo en op het eilandje Utøya;
- Alphen aan de Rijn, schietpartij in 2011.

Ook bij verschillende schietpartijen op scholen in het buitenland (Duitsland, Verenigde Staten) ging het om geweldsuitbarstingen van eenlingen.
Deze geweldsuitbarstingen hebben vaak geen terroristisch oogmerk. Het vraagstuk dient dan ook breder bezien te worden dan alleen vanuit terroristische optiek. Hierdoor zijn ook meerdere departementen betrokken.

Aanpak
Van belang is dat er al in een vroeg stadium potentieel gewelddadige eenlingen kunnen worden gesignaleerd om incidenten te kunnen voorkomen. Hiervoor is kennis nodig van hoe men afwijkend gedrag van deze personen kan herkennen. Het gevaar dat uitgaat van eenlingen wordt grotendeels bepaald door de toegang tot informatie (bedreiging) en tot middelen die deze groep heeft om hun intenties om te zetten in concrete daden. Te denken valt aan vuurwapens, munitie, explosieve stoffen en/of CBRN-middelen.

Belangrijk aandachtspunt bij deze capaciteit is het risico dat 'afwijkende' meningen en gedragingen al gauw en soms ten onrechte als verdacht kunnen worden gezien. Bij de versterking van deze capaciteit moet dan ook nadrukkelijk de balans worden gezocht tussen alertheid en onnodige alarmering.

Bij mogelijk uit te voeren acties kan gedacht worden aan:
Awareness/preventie:
- nodig is dat geradicaliseerde eenlingen vroegtijdig kunnen worden gesignaleerd. Deskundigheidsbevordering van eerstelijnswerkers in het onderwijs, welzijnswerk en politie is hierbij van cruciaal belang. Andere partijen zoals de (geestelijke) gezondheidszorg spelen hierbij een belangrijke signalerende en behandelende rol. Er wordt op dit moment reeds een reeks trainingen over dit onderwerp aangeboden aan eerstelijns professionals, conform de toezegging van de minister van Veiligheid en Justitie aan de Tweede Kamer in oktober 2011.
- er moet ook aandacht komen voor (de mogelijkheid tot) informatie delen waar dit kan. Dit moet duidelijk zijn voor professionals, maar ook voor oplettende burgers. Ook dit is een element dat aan bod komt in de trainingen.

Toegang tot middelen:

- de toegang tot middelen moet tot een minimum beperkt worden. Zo kijkt het ministerie van Veiligheid en Justitie naar de mogelijkheid tot verbetering van het legale wapenbezit, naar aanleiding van de aanbevelingen van de Onderzoeksraad voor de Veiligheid betreffende het schietincident in Alphen a/d Rijn in april 2011.

NRB 2012:

- ook zal nog in de NRB 2012 een specifieke analyse uitgevoerd worden op betekenis en mogelijke aanpak van dit type vraagstuk. Hiervoor zal in de NRB 2012 een scenario specifiek over gewelddadige eenlingen worden uitgewerkt en vervolgens in een capaciteitenanalyse worden beoordeeld.

BIJLAGE 1 ORIENTATIE OP CAPACITEITEN

B1.1 Inleiding

In deze bijlage zijn de samenvatting opgenomen van de capaciteitenanalyses, zoals deze zijn aangeleverd door de experts. In de capaciteitenanalyses wordt op basis van de scenario-analyses en de scoring in de Nationale Risicobeoordeling de analyse weergegeven van mogelijk te versterken capaciteiten per thema, zoals die door de experts zijn geïdentificeerd.

Doel van de capaciteitenanalyses is om inzichtelijk te krijgen waar de zwakke plekken in ons vermogen zitten, om risico's te reduceren en wat daar aan te doen is. Op basis van in eerste instantie deze analyses zijn in hoofdstuk 2 de capaciteiten geformuleerd die geadviseerd worden om te versterken. In tweede instantie is gebruik gemaakt van de kennis die is opgedaan in eerdere capaciteitenanalyses en overige relevantie informatie (bijvoorbeeld de Kwetsbaarheidsanalyse spionage)

In bijlage 3 is de uitleg over de methodiek opgenomen (van scenario's tot capaciteiten).

B1.2 Thema digitale veiligheid: 'Cyberspionage'

Inleiding: Digitale Spionage

Spionage op zich is geen nieuw fenomeen, digitale spionage is echter een fenomeen waar in toenemende mate rekening mee gehouden dient te worden. Het recent gepubliceerde[16] Cyber Security Beeld Nederland gaat dan ook nader in op digitale spionage. Ook in de Nationale Risico Beoordeling is dit erkend door cyber spionage als onderwerp te kiezen voor een scenario. Dit scenario is beoordeeld als een waarschijnlijk scenario met zeer ernstige gevolgen.

Algemene en bestaande capaciteiten

Uiteraard zijn er in het digitale domein reeds de nodige stappen gezet en ook op het gebied van digitale spionage zijn reeds de nodige ontwikkelingen in gang gezet om de mogelijkheid van digitale spionage en de bijbehorende effecten te vermijden dan wel te beperken. Tevens kunnen maatregelen die niet specifiek zien op digitale spionage een belangrijk preventief effect hebben doordat zij een adequaat niveau van beveiliging trachten te bewerkstelligen.

Het al eerder genoemde Cyber Security Beeld Nederland geeft een beeld van de dreigingen waarmee Nederland zich geconfronteerd ziet. Dergelijke informatie vergroot het bewustzijn van de dreiging van spionage en kan daarmee een preventief effect hebben. In het Cyber Security Beeld Nederland dat op 23 december naar de Tweede Kamer is verstuurd, wordt aangegeven dat zowel publieke als private organisaties het slachtoffer kunnen zijn van digitale spionage. Overheden zijn regelmatig doelwit gebleken van digitale spionage, ook in Nederland. Deze cyberaanvallen kunnen gericht zijn op het verkrijgen van vertrouwelijke informatie van economische of politieke waarde, of op direct geldelijk gewin.

[16] Zie Kamerstukken 26 643, nr 220

Binnen de bestaande overlegstructuren (ISAC's) wordt reeds de nodige informatie gedeeld tussen private en publieke partijen over cyberdreigingen. Het kennen van cyberdreigingen vergroot de awareness en kan daarmee een preventief effect hebben. Met de oprichting van het Nationaal Cyber Security Centrum(NCSC) wordt de in de Nationale Cyber Security Strategie ingezette lijn van publiek-private samenwerking verder versterkt.

Uiteraard hebben ook de inlichtingen- en veiligheidsdiensten een rol op het terrein van digitale spionage. Dit vloeit voort uit hun wettelijke taken. Tevens is in samenwerking met de inlichtingen- en veiligheidsdiensten een goede stap gezet op het vlak van voorlichting. Middels de Kwetsbaarheidsanalyse Spionage (KWAS) zijn spionagerisico's in Nederland in beeld gebracht, uitgaande van de te beschermen belangen en de belangrijkste kwetsbaarheden. Inmiddels zijn hier meerdere initiatieven uit voortgevloeid.
Ten eerste is er een intentieverklaring getekend tussen de Ministers van Binnenlandse Zaken en Veiligheid en Justitie en de voorzitters van VNO-NCW en MKB-Nederland, waarin de partijen over en weer hebben afgesproken om het bewustzijn over spionagerisico's te verhogen en elkaar daarbij te stimuleren en faciliteren.
Verder is er een Handleiding beschikbaar gesteld om spionagerisico's zelf in kaart te brengen. Ook is er een e-learning module ontwikkeld die security managers zal helpen in het vergroten van het bewustzijn en het agenderen van spionagerisico's binnen de eigen organisatie. Conform de afspraak uit de intentieverklaring zijn deze hulpmiddelen via VNO-NCW en MKB-NL aan het bedrijfsleven ter beschikking gesteld.

In de kabinetsreactie op de KWAS is aangegeven dat Handleiding KWAS door alle departementen wordt toegepast om kwetsbaarheidsanalyses op te stellen en tegenmaatregelen te treffen. Het veiligheidsbewustzijn van de medewerkers zal worden verhoogd bijvoorbeeld door awareness-presentaties te houden. Hierbij wordt ook de kennis over ICT en haar kwetsbaarheden vergroot met aandacht voor het herkennen en voorkomen van deze kwetsbaarheden. Er zullen strikte afspraken worden gemaakt met ICT-dienstverleners over de gewenste beveiligingsvoorzieningen voor datasystemen die vertrouwelijke of geheime informatie bevatten. Periodiek zullen er security audits en systeempenetratietesten worden gehouden waarin nadrukkelijk aandacht wordt besteed aan spionagerisico's. Deze vallen onder de verantwoordelijkheid van de hoogste managementraden en hun beveiligingsambtenaren(BVA's)[17]. Tot slot wil het Kabinet de weerbaarheid in 2012 zichtbaar versterkt hebben. Daarom zijn de gezamenlijke inspecties verzocht om een onderzoek in te stellen naar de voortgang binnen de Rijksoverheid. Dit onderzoek onder leiding van de Inspectie Openbare Orde en Veiligheid is gestart.

Het beperken van de risico's begint bij een passende mate van risicobewustzijn. Het bevorderen van het risicobewustzijn van cyberspionage is dus van groot belang. De KWAS is een goed begin geweest om zowel de overheid als het bedrijfsleven voor te lichten. In de voorlichting zien de experts het van belang om de sectoren verder voor te lichten. Door experts wordt aangegeven dat het risicobewustzijn in de academische wereld, waar specifieke kennis aanwezig is, verhoogd zou dienen te worden. Hierbij dient aangemerkt te worden dat zich in de academische wereld een spanningsveld voordoet waarbij enerzijds de wil bestaat om wetenschappelijke kennis zoveel als mogelijk te delen en dat het anderzijds noodzaak kan zijn om gevoelige informatie te beschermen.

[17] Zie Kamerstukken 30 821, nr. 13

De overheid heeft, zoals hierboven beschreven, de inspecties gevraagd om de voortgang te onderzoeken. De inspectie V&J kan ook in de toekomst verder gebruikt worden om het risicobewustzijn te verhogen.

Specifieke alertering in geval van risico zorgt ervoor dat men ook daadwerkelijk weet welk risico men loopt en hoe men daarop kan acteren. Om specifiek te kunnen alerteren is echter wel gecentraliseerde kennis nodig die vervolgens gebruikt wordt om sectoren te kunnen alerteren. Hiervoor is het van belang dat de betrokken partijen (De inlichtingen- en veiligheidsdiensten, het NCSC en de sectoren) elkaar goed en centraal weten te vinden en de gerichte informatie bij de juiste persoon weten te krijgen. Een helder aanspreekpunt en specialisatie zorgen voor vertrouwen en daardoor worden adviezen ook daadwerkelijk nageleefd, waardoor de risico's beperkt worden.

Er zijn dus al de nodige initiatieven ontplooid en het onderwerp digitale spionage heeft daarmee de aandacht die het gezien haar score in de NRB ook verdient. Dit neemt echter niet weg dat er voortdurend aandacht dient te zijn voor het risicobewustzijn binnen en buiten de overheid.

<u>Inventarisatie van de te intensiveren capaciteiten</u>
In de inventarisatie van de geprioriteerde capaciteiten zijn binnen de capaciteitenanalyse echter de volgende vier thema's naar voren gekomen waarop volgens de experts, ondanks de al gezette stappen, nog een ontwikkelingsstap gemaakt kan worden die bijdraagt aan het beperken van de risico's, en uiteindelijk de effecten, van digitale spionage. Hierbij wordt zowel ingezet op het bewustzijn om de risico's te beperken en het kennisniveau te verhogen, als op technische en juridische middelen om de risico's, en de mogelijke effecten, te beperken.

Het gaat hierbij om de volgende thema's:

- Monitoring
- Standaarden en normen laten matchen met de technische realiteit
- Kwetsbaarheden in basistechnologie
- Aanbestedingskennis

Deze thema's worden hierna stuk voor stuk in aparte secties behandeld.

Monitoring

Tijdige detectie is van groot belang om de impact van een aanval op informatiesystemen te signaleren en op basis daarvan adequaat en slagvaardig te kunnen acteren. Deze capaciteit verdient dus voortdurend aandacht en dient consequent uitgebouwd te worden naar de stand der techniek. Recent is door het Ministerie van Economische Zaken, Landbouw en Innovatie een subsidie van €800.000 beschikbaar gesteld vanuit de regeling Innovatie voor Maatschappelijke Veiligheid om een Cyber Attack Detector systeem te ontwikkelen waarbij het systeem gebruik maakt van het herkennen van patronen om een cyberaanval waarbij sprake is van digitale spionage te detecteren. Dit in ontwikkeling zijnde systeem kan mogelijkerwijs behulpzaam zijn in de verdere uitwerking van de capaciteit monitoring.

Standaarden en normen laten matchen met de technische realiteit

De ontwikkelingen in het digitale domein gaan in een erg hoog tempo. We maken in toenemende mate gebruik van digitale middelen (tablets en smartphones bijvoorbeeld), waarvan we ons enkele jaren geleden de gebruiksmogelijkheden niet hadden kunnen voorstellen. Het is een uitdaging om de standaarden en normen op het gebied van informatiebeveiliging aan te laten sluiten op deze technologische ontwikkelingen.

Buiten de specifiek op spionage gerichte acties zijn er ook maatregelen met een algemeen effect op het veiligheids- en beveiligingsniveau bij de Rijksdienst. Een goed voorbeeld hiervan zijn de beveiligingskaders van het Rijk, een verplicht uitgangspunt voor ieder informatiesysteem. Daartoe behoort reeds het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR2007), het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI)[18] en de departementale basisbeveiligingsafspraken (baselines). Begin 2012 zal een rijksbrede baseline van kracht worden (BIR). De BIR, evenals de meeste departementale baselines, is gebaseerd op de Code voor Informatiebeveiliging. Uiteraard is een passend niveau van gegevensbeveiliging, zowel in de regel als in de uitvoering, een eerste vereiste om het risico van digitale spionage te beperken.

Het inzetten op (inter)-nationale normen en standaarden (zoals bijvoorbeeld het VIR-BI) voor veilige apparaten is niet hetzelfde als veilig gebruik. Goede technische standaarden en normen helpen echter wel om een goede basis neer te zetten voor een beveiligingsbeleid. Met de Baseline Informatiebeveiliging Rijksdienst wordt een goede stap gezet in de richting van het hebben van een handreiking hoe een norm in de praktijk vertaald wordt. Daarmee weten mensen ook daadwerkelijk hoe ze de abstracte norm in de dagelijkse praktijk en met gebruik van bijvoorbeeld nieuwe technologische middelen, juist ook daar waar er bij medewerkers een wens bestaat om deze nieuwe technieken te kunnen gebruiken, kunnen toepassen. Nieuwe ontwikkelingen en het gebruik van nieuwe toepassingen vergen echter wel een constant proces van up-to-date houden van standaarden en normen.

Deze standaarden dienen te matchen met de technische realiteit (bv cloud computing) en veiligheid dient hierin een prominente rol te krijgen. Juist die technische realiteit en de ontwikkelingen van middelen gaan erg snel. Denk hierbij aan de 10 jaar geleden onvoorstelbaar geachte ontwikkelingen op het gebied van smartphones en tablets.

Uiteraard zijn met het aanschaffen van veilige middelen kosten gemoeid, dit geldt echter voor zowel technische middelen als voor fysieke beveiligingsmiddelen zoals nu reeds gebruikt worden. De ontwikkeling van veilige oplossingen bij vertrouwde bedrijven dient aangemoedigd te worden en deze producten dienen getest en getoetst te worden. Op deze wijze kan invulling worden gegeven aan een passend beveiligingsbeleid waarbij uiteraard oog dient te zijn voor de uitvoerbaarheid. Immers als een norm niet of gecompliceerd uitvoerbaar is dan zal er weinig tot geen navolging aan gegeven worden.

[18] Het VIR-BI zal worden vervangen door het VIR-GI

Basistechnologie is kwetsbaar

Basistechnologie is kwetsbaar gebleken. Voorbeelden hiervan, een aantal hiervan zijn ook beschreven in het Cyber Security Beeld Nederland, zijn: DNS, BGP, SQL[19], certificaten en de GPS-afhankelijkheid van tijdklokken voor het internet. In een aantal gevallen kan met relatief beperkte maatregelen de kwetsbaarheid beperkt worden. De overheid[20] maakt bijvoorbeeld al gebruik van penetratietesten om kwetsbaarheden op te sporen.

Bij de SQL-injectie wordt codetaal toegevoegd aan een web-applicatie om deze web-applicatie een eigen bewerking uit te laten voeren en daarmee bijvoorbeeld een databestand te manipuleren. Het invoeren van DNSSEC[21] bij de overheid en het gebruik hiervan bevorderen bij kennisinstituten en bedrijven kan dit risico beperken. DNSSEC is de beveiligde variant van het in het internetverkeer veel gebruikte DNS.

Met DNS worden namen als www.overheid.nl door een server vertaald in ip-adressen om zo de computergebruiker op een simpele wijze op de website van bestemming te laten komen. Met het invoeren van relatief simpele oplossingen als DNSSEC kunnen veelvoorkomende problemen voorkomen en of beperkt worden. Hierdoor kan de bestaande capaciteit meer aandacht hebben voor de meer specifieke en complexe zaken. Met een geringe investering valt hierbij een aanzienlijk resultaat te bereiken.

Aanbestedingskennis

In aanbestedingen bestaat de mogelijkheid om rekening te houden met het veiligheidsaspect. Dit middel kan dus ook ingezet worden om het risico van digitale spionage te beperken. De aanbestedende partij gaat immers een contractuele relatie aan met de opdrachtnemer. Dit vergt echter wel dat de aanbestedende partij ook de kennis heeft om de opdracht zo te formuleren dat het veiligheidsaspect wordt meegewogen. Naar aanleiding van de tijdens het Diginotar-debat ingediende motie Hachi/Elissen (26643, nr 207 over het verbeteren van de ICT-kennis bij de overheid heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangegeven dat er een rijksbrede pool voor ICT-professionals is opgezet om voor het Rijk cruciale expertise op te bouwen en te behouden. Voor opdrachtgevers en het topmanagement wordt uitbreiding van het opleidingsportfolio voorzien. Voorts wordt een opleiding voorzien ten aanzien van (Europees) aanbesteden alsook het stimuleren van *digivaardigheid:* het besef bij medewerkers van het Rijk ten aanzien van beveiligingsissues[22]. Er dient dus expliciet aandacht besteed te worden bij aanbestedingen aan de veiligheid van ICT, waaronder dus ook cyberspionage. Hiervoor is het nodig om de kennis te verhogen van de technische ICT-veiligheid en van de juridische kennis van aanbestedingsmogelijkheden. Ook dient er binnen organisaties op een goede manier samengewerkt te worden tussen de specialisten op deze diverse terreinen(inkoop, aanbestedingen en ICT-veiligheid). Het gebruik van de concurrentiegerichte dialoog, een mogelijkheid binnen de aanbestedingsregels om via een dialoog tussen opdrachtgever en opdrachtnemers een product op maat te ontwikkelen, kan hierbij een probaat middel zijn om security by design te realiseren. Investeren in veiligheid vergt een investering vooraf, maar het achteraf repareren van opgelopen schade, indien al mogelijk, is uiteindelijk vele malen duurder dan vooraf gericht investeren in veiligheid.

[19] DNS, Domain Name System en BGP, Border Gateway Protocol zijn protocollen die het internetverkeer routeren en mogelijk maken, Structured Query Language is een programmeertaal die gebruikt kan worden om gegevens te bevragen en aan te passen in een databank..
[20] Zie Kamerstukken, 2011, 26643 nr. 214
[21] Ook in de Verenigde Staten is men hiertoe overgegaan
[22] Zie Kamerstukken, 2011, 26643 nr 214

B1.3 Thema klimaat: 'Uitval satellietsystemen als gevolg van een zonne-storm'

Inleiding

Naar aanleiding van een rapport van het ministerie van Infrastructuur en Milieu (IenM) over gevolgen van een mogelijke uitval van satellieten voor tijd- en plaatsbepaling heeft de rijksbrede Stuurgroep Nationale Veiligheid aan TNO opdracht gegeven een scenario te schrijven gericht op grootschalige, langdurige uitval van satellieten ten gevolge van hevige zonneactiviteit.
Het ministerie van IenM heeft het rapport laten opstellen naar aanleiding van de uitkomsten van experimenten in het buitenland en van alarmerende signalen van (professionele) gebruikers van satellietsystemen in Nederland. Uit de (buitenlandse) experimenten blijkt dat de impact van uitval van satellietsignalen voor bijvoorbeeld navigatie behoorlijk groot is, zelfs als de verstoring tevoren wordt aangekondigd. In verschillende landen is momenteel sprake van een bewustwordingsproces en worden maatregelen geformuleerd.
Door een groep van experts uit bedrijfsleven, overheid en andere organisaties[23] is op grond van het scenario vervolgens de mogelijke impact ingeschat in het geval het scenario werkelijkheid zou worden. De capaciteitenwerkgroep "Satellietuitval" heeft voor vijf gevolgen die zeer hoog scoorden qua impact, maatregelen geformuleerd in het geval dat een substantieel aantal navigatie-, communicatie- en weersatellieten uitvalt.

Scenario "satellietuitval"

In het beschreven scenario 'satellietuitval', waarvoor geen rubricering geldt, wordt voor mogelijke uitval een aantal oorzaken genoemd zoals naast technisch falen en menselijk ingrijpen ook heftige zonneactiviteit op het niveau van G4 – G5[24]. De directe effecten van deze ernstige vorm van zonneactiviteit op ons aardoppervlak (elektriciteit en communicatie) vallen buiten de scope van dit scenario. Wel wordt door de experts op dit gebied onderschreven dat nadere studie naar de gevolgen van dit natuurverschijnsel dringend gewenst is, immers de gevolgen van een eventuele herhaling van heftige zonneactiviteit, zoals de Carringtongebeurtenis uit 1859, tijdens een volgende zonnecyclus, zijn op dit moment onvoorspelbaar, maar in potentie zeer groot.
Ook opzettelijke verstoring van signalen is buiten het scenario gelaten. De impact van een dergelijke verstoring kan, vanwege het opzettelijke karakter en de keteneffecten, ook groot zijn.

Het soort satellieten dat is beschouwd betreft navigatiesatellieten[25], zoals GPS (Verenigde Staten) en GLONASS (Rusland), communicatiesatellieten en satellieten voor het verzamelen van meteorologische data. De uitval is van lange duur en herstel vergt tijd en geld.
De waarschijnlijkheid van het scenario is groot (het betreft een cyclisch natuurverschijnsel) en een aantal gevolgen scoren (zeer) hoog. In de onderstaande opsomming is de terminologie van de 'Leidraad voor het werken met scenario's, risicobeoordeling en capaciteiten' aangehouden.

Dit betreft:

[23] Het scenario is door een breed samengestelde groep experts uit verschillende disciplines beoordeeld op waarschijnlijkheid en gevolgen; de gevolgen zijn door een twintigtal vertegenwoordigers uit verschillende sectoren geanalyseerd op grond waarvan maatregelen zijn geformuleerd
[24] G4-G5 zijn gradaties van geomagnetische stormen conform de North Oceanic and Atmospheric Administration schaal uit de V.S., voor een overzicht zie bijlage.
[25] Naast de operationele GPS en GLONASS navigatiesatellieten, zijn er momenteel drie constellaties in ontwikkeling: het Europese Galileo, het Chinese COMPASS en het Indiaase IRNSS.

- Lichamelijk lijden o.a. door gebrek aan primaire levensbehoeften; dit gevolg is in potentie catastrofaal omdat 1-4 weken meer dan 1 miljoen mensen worden getroffen;
- kosten (satellietinfrastructuur, lamleggen van economische activiteit etc.); door experts worden deze kosten als catastrofaal geduid omdat de kosten kunnen oplopen tot 50 miljard;
- verstoring dagelijks leven (verstoring vervoer, lege winkels etc.); experts schatten in dat dit een zeer ernstig gevolg van het scenario is omdat 3-7 dagen meer dan 1 miljoen mensen worden getroffen;
- aantasting democratische rechtsstaat (diensten voor (orde)handhaving en hulp zijn afhankelijk van satellietsystemen); overheid faalt in anticiperend gedrag; ook deze gevolgen worden als zeer ernstig gezien omdat deze verstoring langdurig van aard is;
- sociaalpsychologische impact (ontwrichting van de samenleving); afhankelijk van het keteneffect kan dit gevolg als catastrofaal worden geduid vanwege de perceptie die burgers zullen hebben die leidt tot angst vanwege onzekerheid en onwetendheid, het verwachtingspatroon: het betreft voorzieningen die er altijd zijn en waarvoor men de overheid verantwoordelijk zal stellen en het gebrek aan handelingsperspectief op korte termijn.

De expertgroep heeft in eerste instantie vijf capaciteiten geselecteerd die het meest relevant zijn voor de boven beschreven gevolgen. Na een scherpe selectie zijn maatregelen voorgesteld waarmee deze capaciteiten worden versterkt waardoor de risico's en de gevolgen worden verkleind voor de Nederlandse samenleving.

Dit betreft:

Regie en aansturing

Het opstellen van een Nationaal Crisisplan Satellietuitval door de rijksoverheid, met daarin een beschrijving van de wijze waarop de crisisbeheersing op nationaal niveau in dit specifieke scenario is georganiseerd. In dit plan dienen ook verantwoordelijkheden te worden belegd. In dit crisisplan worden tevens maatregelen opgenomen om te komen tot monitoring van interruptie van satellietnavigatiesignalen (positiebepaling en tijd), van communicatiesignalen en van weergegevens. Hiermee kunnen de gebruikers van de aangeboden diensten op tijd worden gewaarschuwd. Nederland kent momenteel geen georganiseerd monitoring- en attendering systeem. Belangrijk onderdeel van het plan is een bewustwordingsproces voor geïnventariseerde gebruikersgroepen. Hiermee kunnen geschetste risico's aanzienlijk worden verkleind.
In de uitvoering kunnen sectorale koepelorganisaties en beheerders van infrastructuur een belangrijke rol spelen.

Verminderen van kwetsbaarheid door bestudering effecten van zonneactiviteit en (verplichte) alternatieve systemen

Volgens de expertgroep is in Nederland weinig bekend over de gevolgen van sterk vergrote zonneactiviteit. Dit betreft zowel de voor het bestudeerde scenario indirecte effecten van deze activiteit als de directe effecten. Opvallend is de relatie tussen deze effecten. Uit de discussie

is gebleken dat voor indirecte effecten soms maatregelen bestaan (mobiele communicatie) die door het directe effect van de zonneactiviteit mogelijk niet effectief zijn.
Uit een nader onderzoek naar de effecten van zonneactiviteit (conform Carringtoneffect in 1859) op de vitale sectoren energie en radiocommunicatie, zal moeten blijken of monitoring van deze zonneactiviteit en/of het opzetten van een waarschuwingsysteem daarvoor, ook in Nederland gewenst is. Ook de gevolgen van keteneffecten dienen hierbij betrokken te worden.

Door experts is geconstateerd dat eLORAN een plaats- en tijdsbepaling systeem is, dat geen gebruik maakt van satellieten maar van een aantal radiozenders in Engeland, Frankrijk, Duitsland, Denemarken en Noorwegen. Indien onafhankelijkheid van satellieten gewenst is in het kader van de gevolgen die bij dit scenario satellietuitval opdoemen, zal de continuïteit van dit systeem moeten worden geborgd.
Het al dan niet verplicht stellen van deze back-up zal beoordeeld moeten worden.
Voor communicatie en meteosatellieten is een back-up minder eenvoudig te realiseren. Voor meteo kan weerradar en radar op zeeschepen en vliegtuigen behulpzaam zijn. De wenselijkheid moet worden beoordeeld van (internationale) afspraken over verdeling van schaarse capaciteit na satellietuitval.

Risicocommunicatie, bewustzijn

Hierbij heeft de overheid de taak om de professionele en particuliere gebruikers bewust te maken van het feit dat positiebepaling, nauwkeurige tijdsbepaling, communicatie en het weer wel eens niet correct kunnen worden weergegeven voor het gebruikerssegment, in casu de ontvangers (geen autonavigatiesystemen, onbetrouwbare tracking and tracing, gebrekkige communicatie etc.). Gebruikers moeten zich na een eigen risicoanalyse afvragen of alternatieven overwogen moeten worden, zoals het eLORAN navigatie- en tijdsysteem of het DCF[26]-tijdsignaal uit Frankfurt.

Ontwikkelen en toepassen van technische maatregelen

Bestaande en nog in ontwikkeling zijnde systemen kunnen een goede bijdrage leveren aan verkleining van de gevolgen van satellietuitval. Naast bovengenoemde systemen zoals eLORAN[27] en radar betreft dit ook vaste telefoonlijnen en radioverbindingen (marifoon). Tevens moeten in ontwikkeling zijnde alternatieven (de EGNOS Data Access Service kan de atoomtijd vanuit het RIMS[28]-netwerk onafhankelijk van radio- of satellietsignalen, via het Internet of een vaste lijn aanbieden) worden aangepast op de behoefte bij specifieke gebruikers van logistieke systemen. Een voorbeeld van een kwetsbaar systeem is het AIS[29] systeem voor tracking en tracing in zee- en binnenvaart. Dit systeem is afhankelijk van GPS. De wenselijkheid van (verplichte) alternatieve systemen moet in internationaal verband worden geagendeerd.
Ook zal het huidige satellietnavigatieprogramma van de EU, Galileo, op termijn bijdragen in het verlagen van risico's bij de uitval van navigatiesatellieten. Immers een groter aantal compatibele satellieten vergroot de kans op een betrouwbare positie en een nauwkeurige tijd, ervan uitgaande dat niet tegelijkertijd alle navigatiesatellieten door zonneactiviteit zullen uitvallen.

[26] DCF – Duits Radiotijdsignaal afkomstig van een atoomklok in Frankfurt
[27] eLORAN – enhanced Long Range Navigation
[28] RIMS – Ranging and Integrity Monitoring Stations
[29] AIS – Automatic Identification System

Ontwikkelen en onderhouden van training- en oefenprogramma's /Early Warning Systems en aanspreekpunt voor monitoring

Naast het opstellen van een Nationaal Crisisplan Satellietuitval zal het Rijk een oefenprogramma opstellen, waarin ook wordt opgenomen dat bij vitale sectoren de uitval van de frequentiestandaard en van de tijd- en plaatsbepaling zal worden nagebootst. Onderdeel van dit programma is in ieder geval een oefening op politiek-bestuurlijk niveau voor de Ministeriële Commissie Crisisbeheersing(MCCb). Voor gebruikers van satellietnavigatie, satellietcommunicatie en weersatellieten is het belangrijk te weten wie aanspreekbaar is bij calamiteiten en dat indien mogelijk op tijd overgegaan kan worden op fall-back systemen. Aanbieders van satellietcommunicatie en overheid zullen voor wat betreft de verantwoordelijkheid voor het beschikbaar zijn van terugvalmogelijkheden via de bekende crisisstructuren binnen de vitale sectoren, zoals het Nationaal Continuïteitsoverleg Telecom (NCO-T), tot overeenstemming moeten komen.

<u>Bestaand beleid</u>
Het brede gebruik en de toenemende afhankelijkheid van diensten die voor satellieten worden geleverd is een relatief nieuw fenomeen. Bij de werkgroep is geen specifiek beleid bekend dat is gericht op het effectief beheersten van de gevolgen van sterk verhoogde zonneactiviteit. In het buitenland (België, Verenigd Koninkrijk) vindt monitoring van zonneactiviteit plaats. In Nederland vindt momenteel geen structurele monitoring plaats, noch is sprake van een inventarisatie van belanghebbenden en van een waarschuwingssysteem.

Het Agentschap Telecom is in Nederland verantwoordelijk voor het monitoren van verstoringen in het frequentiespectrum. Bij deze organisatie is geen specifieke taak belegd voor uitval van satellieten voor navigatie, communicatie en meteo.

Het Kadaster heeft een fijnmazig netwerk van bakens dat als een back-up zou kunnen dienen voor plaatsbepaling.

<u>Conclusies</u>
1. *Mogelijk onder te brengen maatregelen bij bestaande organisaties zoals het KNMI, het Agentschap Telecom en het Kadaster*
   Deze maatregelen betreffen (1) het monitoren en beoordelen van verkregen informatie over zonneactiviteit, (2) het monitoren van verstoringen als gevolg van deze zonneactiviteit of indien gewenst ook als gevolg van moedwillige verstoringen en (3) het vervolgens kunnen waarschuwen van gebruikers binnen de vitale sectoren of binnen Nederland. Waar het gaat om technisch falen ligt de verantwoordelijkheid voor degradatie van de genoemde satellietdiensten in eerste instantie bij de providers. In het geval van extreme zonneactiviteit echter heeft, mede gelet op de grote risico's en gevolgen, ook de overheid hierin een verantwoordelijkheid te nemen.

2. *Nieuw te treffen maatregelen*
   a. Doen van studies naar gevolgen extreme zonne-activiteit.
   b. Inventarisatie GNSS gebruikers en bewustwording aankweken.
   c. Opstellen van een Nationaal Crisisplan Satellietuitval, inclusief aandacht voor de crisiscommunicatie.
   d. Alternatieven bij satellietuitval vaststellen, uitbreiden en doen continueren.

e. Houden van oefeningen in overleg met vitale sectoren en betrokken ministeries waarbij satellietuitval wordt nagebootst.

B1.4 Thema Polarisatie en Radicalisering: 'Onrust over Salafisme'

INLEIDING

De analyse van te versterken capaciteiten is uitgevoerd in het licht van de Nationale risicobeoordeling (NRB) en tegen de achtergrond van een geactualiseerd scenario over het ontstaan van maatschappelijke onrust. Getoetst is of de aanpak zoals die momenteel is ontwikkeld, robuust genoeg is om de situaties uit het gebruikte scenario het hoofd te kunnen bieden. Deze toetsing heeft geleid tot het inzicht dat een aantal capaciteiten versterkt moet worden. De te versterken capaciteiten worden in de volgende tekst beschreven met een advies over de te volgen richting en aanpak ervan.

Voor de capaciteitenanalyse polarisatie en radicalisering is gebruik gemaakt van het scenario *"Onrust onder salafisten met verstrekkende landelijke en internationale gevolgen"*.
Dit scenario beschrijft, kort samengevat, de nationale en internationale onrust die ontstaat na het sluiten van een islamitische school in een grote Nederlandse stad, de daaropvolgende en steeds hoger oplopende spanningen tussen moslims en niet-moslims in Nederland, een uiteindelijke moordaanslag door een persoon die actief is in de anti-islam beweging, met rellen in Nederland en bij Nederlandse ambassades in het buitenland, als gevolg van de onrust.

BESTAAND BELEID

Het bestrijden van extremisme en escalatie van maatschappelijke onrust vindt plaats met aandacht voor preventie, pro-actie (deskundigheidsbevording, vroegsignalering, informatiehuishouding) en repressie (indammen, confronteren). Lokale inbedding van de aanpak van polarisatie en radicalisering is van groot belang. Dáár immers worden de gevolgen ervaren en dáár hebben bestuurders, professionals en maatschappelijke organisaties het beste zicht op (de eerste signalen van) de problematiek. Gemeenten nemen het voortouw; zij werken samen met maatschappelijke organisaties en burgers aan het voorkomen en tegengaan van radicalisering met aandacht voor zowel pro-actie, preventie als repressie.
Voor een effectieve lokale aanpak zijn de volgende elementen van belang:

- het opzetten van een systeem van vroegsignalering en daarmee gepaard gaand, opbouw van een netwerk van maatschappelijke en hulpverleningsorganisaties en sleutelfiguren in de gemeentelijke samenleving (sociaal calamiteitenplan) en het investeren in bewustwording en deskundigheid (trainingen eerstelijnswerkers);
- activiteiten die voorkomen dat spanningen (in wijken) escaleren;
- activiteiten die voorkomen dat er een voedingsbodem ontstaat waarin idealen afglijden naar radicaal gedrag;
- het verhogen van weerbaarheid tegen radicalisering;
- het zo nodig nemen van maatregelen ter beveiliging van personen en objecten tegen extremisme;
- het aanpakken van extremistisch gedrag (voorkomen en repressie).

De rijksoverheid heeft de afgelopen jaren een landelijk coördinerende, stimulerende en ondersteunende rol gespeeld. De afgelopen jaren is een breed stimuleringsprogramma uitgevoerd (Actieplan Polarisatie & Radicalisering 2007-2011) aan de hand waarvan vooral flink geïnvesteerd is in de versteviging van de lokale aanpak.[30] Circa 150 gemeenten hebben

[30] Een PDF-bestand van het Actieplan Polarisatie & Radicalisering is digitaal beschikbaar: http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/jaarplannen/2007/08/27/actieplan-polarisatie-en-radicalisering-2007-2011/minbiz-actieplan-printnl.pdf.

projecten uitgevoerd op het terrein van bewustwording, kennisopbouw, deskundigheidsbevordering, signalerings- en duidingscapaciteit en weerbaarheidsversterking. Daarnaast zijn tientallen landelijke projecten uitgevoerd, vooral gericht op jongeren, op het gebied van democratische ontwikkeling en conflicthantering.
Omdat de aanpak van extremisme en escalatie een uitzonderlijk terrein is, worden op nationaal niveau kennis en ervaringen verzameld en uitgewisseld en worden adviezen verstrekt. Om gemeenten, professionals en burgers te ondersteunen werd op het nationale niveau een kennis- en adviescentrum opgericht (Nuansa). Daarnaast zijn meerdere (intervisie) bijeenkomsten georganiseerd en is een landelijke reeks van interdisciplinaire trainingen verzorgd. Er zijn brochures uitgebracht over diverse vormen van extremisme met informatie voor gemeenten, bedrijven en instellingen. Ook zijn de nodige handreikingen ontwikkeld, zoals het 'Tweeluik
Religie in het Publieke Domein'. Ook de VNG heeft een tool gemaakt voor het opzetten van een lokale aanpak op radicalisering en polarisatie. Ten behoeve van beroepsgroepen zijn specifieke producten ontwikkeld, zoals een instrument voor docenten om het gesprek over radicalisering te voeren in de klas en modules voor de opleiding en training van bijvoorbeeld politie.

De ondersteuning vanuit het Rijk zal zich de komende jaren meer richten op de gebieden die daadwerkelijk met een probleem te kampen hebben of die zich onderscheiden door een hoge kans op radicalisering én die daadwerkelijk ondersteuning nodig hebben. De hulp kan bestaan uit het inzetten van experts/praktijkteams. Ook wordt een toolbox ontwikkeld van trainingsproducten en adviesnetwerken. Deze producten worden – afhankelijk van de dreiging en de weerstand – op maat aangeboden.

Eén van de meest in het oog springende intensiveringen van de komende periode is de aanpak van geradicaliseerde (of anderszins doordraaiende) eenlingen. Er wordt ingezet op kennisvergroting , vroegtijdige detectie van gewelddadige eenlingen en het verminderen van de handelingsverlegenheid. Met name eerstelijnswerkers, zoals wijkagenten, onderwijzers, jeugdzorg, GGZ en buurtwerkers, spelen hierbij een cruciale rol. Zij zijn in een positie om signalen over radicaliserende eenlingen als eerste op te pikken. Zij zullen daar beter op worden toegerust.

Ook wordt het internet gemonitord als één van de wegen om indicaties voor radicalisering van individuen te vinden.
Via wetenschappelijk onderzoek en internationaal overleg (expertmeetings, seminars) zal worden geprobeerd meer inzicht te krijgen in mogelijkheden tot tijdige onderkenning van individuele radicaliseringsprocessen. Deze inzichten zullen ook ten goede komen aan de nog verder te ontwikkelen aanpak.

GEPRIORITEERDE CAPACITEITEN

Bij de inventarisatie van mogelijk te versterken capaciteiten zijn vier capaciteiten benoemd waarop met voorrang een ontwikkelingsslag gemaakt dient te worden die bijdraagt aan het beperken van de risico's en uiteindelijk de effecten van de incidenten in het scenario.
De volgende vier capaciteiten zijn als prioriteit benoemd:

1. Lokaal sociaal calamiteitenplan

In gemeenten en regio's zijn rampenplannen voor fysieke crises en rampen voorhanden, maar op calamiteiten met een sociaal karakter is men niet altijd specifiek voorbereid. Een goede voorbereiding is essentieel om de (mogelijke) escalatie van maatschappelijke onrust in de

kiem te kunnen smoren. Het gaat hierbij om ontwikkelingen, conflicten en incidenten die het risico in zich dragen een bedreiging te vormen voor de sociale en politieke stabiliteit op lokaal, regionaal en/of nationaal niveau. Te denken valt aan bijvoorbeeld de gebeurtenissen rondom de moord op Theo van Gogh, spanningen tussen groepen in Culemborg en incidenten rondom gebedshuizen.

Een sociaal calamiteiten plan is nodig om:
- vroegtijdig zicht te krijgen op ongewenste vormen van polarisatie en radicalisering of andere spanningen;
- voorbereid te zijn op situaties die vragen om een weerwoord of reactie anderszins op gesignaleerde spanningen door de overheid en haar partners;
- in staat te zijn om effectief (de-escalerend) te kunnen handelen in geval van een daadwerkelijke crisis/calamiteit met betrekking tot het escaleren van spanningen door de overheid en haar partners.

Om dit te bereiken is van belang dat het plan voorziet in:
- het opzetten van een systeem van vroegsignalering en daarmee gepaard gaand, het opbouwen van een netwerk van maatschappelijke en hulpverleningsorganisaties en sleutelfiguren in de gemeentelijke samenleving (inzetbaar in koude en warme fase);
- een duidelijk profiel van de sleutelfiguren die nodig zijn binnen het netwerk;
- een crisisorganisatie die goed aansluit op de reguliere crisisorganisatie;
- (voorbereiding op) crisiscommunicatie, waaronder woordvoering, gebruik van sociale media en (evt.) opstellen vraag en antwoord lijst;
- binnen de crisisorganisatie dient, net als bij reguliere crises, een crisiscommunicatieadviseur betrokken te zijn.
- bestrijdingsplannen afgestemd op potentiële scenario's;
- een aanpak voor nazorg en herstel.

Een sociaal calamiteitenplan is tweeledig, het richt zich op preventie met de-escalatie en repressie als sluitstuk.
Het is daarnaast van belang om aan te geven dat de capaciteiten die in deze rapportage als Quick Win 1 en 4 zijn benoemd ("*een betere en meer georganiseerde informatiedeling tussen overheden, inlichtingenapparaat en kennisinstituten*" en "*deskundigheidsbevordering voor signalerende en ook 'ontvangende' personen*") een belangrijk onderdeel (kunnen) zijn van een effectief sociaal calamiteitenplan en daarom in de uitvoering van deze capaciteit dienen te worden meegenomen.

Door te zorgen dat een gemeente/regio en haar samenwerkingspartners voorbereid zijn, kan er adequaat worden opgetreden. Het gaat om – zoals aangegeven in de paragraaf over het huidige beleid – vroegtijdig signaleren, goede duiding van het probleem en samenwerking met relevante partners. Communicatie speelt ook een belangrijke rol, zo wordt ook benadrukt in het onderzoek 'Schaken op verschillende borden: evidence-based strategieën voor communicatie over overlast en verloedering, maatschappelijke onrust, polarisatie en radicalisering'[31].

Tegen deze achtergrond moet door het Rijk verder gestimuleerd worden dat gemeenten, regio's en de rijksoverheid beschikken over een dergelijk plan.

De afgelopen jaren is het ontwikkelen van een lokale sociaal calamiteitenplannen gestimuleerd door de rijksoverheid. Zo is in 2010 de "*Gemeenteprijs polarisatie en radicalisering*" aan de gemeente Weert uitgereikt, onder andere voor de wijze waarop zij een

[31] Marnix Eijsink Smeets, Hans Moors, Ton Baetens, IVA, 2011.

lokaal sociaal calamiteitenplan hebben ontwikkeld en daar ook geregeld mee oefenen.[32] Recent is door het financieren van het Ministerie van Veiligheid en Justitie in vijf gemeenten en één regio de ontwikkeling van een sociaal calamiteitenplan op gang gebracht.

Deze stimuleringsmaatregelen hebben er echter nog niet toe geleid dat alle gemeenten dergelijk plan vanzelf ontwikkelen.

In de expertgroep is de mogelijkheid van het verplicht stellen van een lokaal sociaal calamiteitenplan besproken. Deze optie wordt door de expertgroep echter afgeraden, onder andere vanwege het streven van het huidige kabinet naar het juist verminderen van de regeldruk voor lokale overheden.
Andere opties zijn het beschikbaar stellen van financiële middelen of capaciteit en kennis en expertise, of een combinatie daarvan. Afhankelijk van de vorm en intensiteit van de gekozen ondersteuning, vraagt de uitvoering van deze prioriteit een grotere of kleinere investering. Als illustratie kan hierbij de reeds gegeven ondersteuning in vijf gemeenten en één regio (kosten ca. €75.000) worden gebruikt.

Bij het versterken van deze capaciteit heeft het Rijk een aanjagende en faciliterende rol. De basisverantwoordelijkheid voor ontwikkeling en implementatie van een lokaal sociaal calamiteitenplan ligt bij de lokale overheden.

Voor een succesvolle aanpak van deze prioriteit wordt aangeraden te streven naar een samenhangende aanpak over het gehele veiligheidsdomein; algemene veiligheid, sociale veiligheid en de verantwoordelijkheid voor OOV van het gemeentebestuur. Dit dient te worden geïnitieerd door de ministeries van Veiligheid en Justitie (NCTV en DGRR) en Binnenlandse Zaken en Koninkrijksrelaties gezamenlijk. Deze ministeries wordt geadviseerd in samenwerking met de relevante maatschappelijke instellingen (Forum en anderen) een stimuleringsaanpak (‘aanvalsplan’) te ontwikkelen.

Bij het verkrijgen van voldoende bestuurlijk draagvlak voor de ontwikkeling van een lokaal sociaal calamiteitenplan kunnen ook de Veiligheidshuizen en Veiligheidsregio’s betrokken worden. Met betrekking tot de Veiligheidsregio’s kan het versterken van bestuurlijk bewustzijn en draagvlak onder andere vorm krijgen door het onderwerp op te nemen in de jaarlijkse voortgangsgesprekken die het ministerie van Veiligheid en Justitie voert met de verschillende Veiligheidsregio’s of door het onderwerp te agenderen bij het Veiligheidsberaad (*quick win*).

2. Helderheid en uniformiteit over interveniëren in organisaties.

In veel organisaties die betrokken zijn bij de aanpak van polarisatie, escalatie van maatschappelijke onrust en radicalisering bestaat nog onduidelijkheid over de grondslag en het kader waarbinnen deze thema’s door de overheid worden aangepakt. Met name daar waar de problematiek raakt aan geloofsovertuigingen van de betrokken doelgroep, is niet voldoende helder wat de grenzen van het overheidshandelen zijn in het licht van de scheiding tussen kerk en Staat en in gevallen van botsende grondrechten, terwijl daarover in de afgelopen jaren wel de nodige onderzoeken en publicaties zijn uitgevoerd. Dit leidt ertoe dat betrokkenen soms de indruk hebben ‘de verkeerde oorlog’ te voeren.

Om deze handelingsverlegenheid weg te nemen moet er dan ook meer duidelijkheid komen over de grondslag voor het overheidsoptreden met betrekking tot de aanpak van polarisatie en

[32] http://www.rijksoverheid.nl/nieuws/2010/11/24/gemeente-weert-wint-gemeenteprijs-polarisatie-en-radicalisering.html

radicalisering, en de grenzen van overheidsinterventies, met name gelet op grondrechten. Een overheid die daarin transparant en zonder dralen acteert wint aan gezag. Daarbij kunnen eventuele overheidsinterventies weloverwogen, met inachtneming van de relevante grenzen en regelgeving en op een zorgvuldige manier worden uitgevoerd. Van belang hierbij is dat de overheid de plicht heeft om de veiligheid van haar burgers te beschermen, ook als het gaat om de gevolgen van radicalisering. Het is belangrijk om daarbij te onderkennen dat het bij de aanpak van radicalisering niet gaat om het hebben van een extreme gedachte op zich; overheidsinterventie is geoorloofd in verband met een bestaande of vermoede bereidheid om diep ingrijpende veranderingen in de samenleving (eventueel op ondemocratische wijze) na te streven, te ondersteunen of anderen daartoe aan te zetten. Ingrijpende veranderingen zijn ontwikkelingen die een gevaar kunnen opleveren voor de democratische rechtsorde (doel), vaak met ondemocratische methoden (middel), die afbreuk doen aan het functioneren van de democratische rechtsorde (effect).
Zoals in het Tweeluik religie en publiek domein staat, zal de overheid in principe geen inhoudelijke informatie over de juiste interpretatie van welke religie dan ook verspreiden. In bijzondere gevallen is het belangrijk om daarbij aan te geven dat meerdere meningen en interpretaties mogelijk. De overheid neemt daarbij een neutrale houding aan, tenzij de grenzen van de wet of de betamelijkheid (dreigen te) worden overschreden.

Als de beleidsdoelstelling daarbij gebaat is, is het binnen de uitgangspunten van de scheiding van kerk en staat voor de overheid uiteraard onmogelijk om met religieuze partners samen te werken.

Voor een eenduidige en samenhangende aanpak van de Nederlandse overheid moet het gebruik van deze en andere kaderstellende begrippen, gemeengoed worden. Dit leidt ertoe dat noodzakelijke overheidsinterventies zorgvuldig en gebaseerd op eenduidige uitgangspunten plaatsvinden en dat de handelingsverlegenheid van betrokkenen op de momenten dat dat niet nodig is, wordt weggenomen.

De expertgroep adviseert concreet om de ontwikkelde informatie en instrumenten voor overheidsinterventies door te vertalen naar meer praktische situaties en om daarnaast bestaande ervaringen en gedane interventies in kaart te brengen en zichtbaar te maken.

De verantwoordelijkheid voor het versterken van deze capaciteit ligt bij de rijksoverheid, meer specifiek bij het ministerie van Veiligheid en Justitie (NCTV), in overleg met deskundigen en stellers van reeds ontwikkelde instrumenten.
Het Nederlands Genootschap voor burgemeesters wordt genoemd als mogelijke partner bij het uitwerken van deze capaciteit evenals het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

3. Bewustwording en weerbaarheid m.b.t. de waarde van de democratische rechtsstaat

De expertgroep constateert een brede zorg over de positie van, en het gebrek aan vertrouwen in, de democratische rechtsstaat in de Nederlandse samenleving.
Deze capaciteit richt zich desondanks op een specifiek deel van deze zorg, namelijk de ‘risicogroepen’. Op wat dit precies inhoudt wordt later in de uitwerking dieper ingegaan.

Te bereiken resultaat: De overheid wil het draagvlak voor vrijheid, gelijkwaardigheid en solidariteit (de kernwaarden van onze democratische rechtsstaat) en de weerbaarheid tegen antidemocratische uitingen en/of gedragingen vergroten. Een voorwaarde om dit te kunnen doen is het ontwikkelen en toepassen van een strategie en instrumentarium om antwoord te bieden of te kunnen organiseren met betrekking tot antidemocratische boodschappen. Dit zijn vaak manipulatief gebrachte verhalen met een wervend karakter (zij haken aan op gevoelens

van onrecht, loyaliteit, verantwoordelijkheid, trots). Wat nodig is zijn boodschappen en gesprekken vanuit het perspectief van de democratische rechtsstaat die een wervende kracht hebben. Belangrijk aspect daarbij is een doelgroepenbenadering: hoe en met welke boodschap zijn verschillende doelgroepen het beste te benaderen en te bereiken?
Het uitgangspunt is om ruimte te geven aan een veelheid van ideeën en zienswijzen zodat men naar buiten blijft treden, maar om daarbij wel een (inhoudelijke) tegenkracht te organiseren. Met andere woorden; de discussie aangaan.

Bij deze capaciteit zijn drie doelgroepen te onderscheiden: de samenleving in algemene zin, de 'ontvangers' van antidemocratische boodschappen en 'zenders' van antidemocratische boodschappen. Ondanks een brede zorg over de positie van de democratische rechtsstaat in de Nederlandse samenleving, adviseert de expertgroep om bij het versterken van deze capaciteit vooral te richten op de laatste twee doelgroepen, de zogenaamde 'risicogroepen'. Deze beperking wordt geadviseerd met het oog op de haalbaarheid en effectiviteit van de te versterken capaciteit en de grotere urgentie met betrekking tot de 'risicogroepen'.
De expertgroep adviseert om bij de aanpak te richten op de volgende aspecten:

1. Voedingsbodem voor de 'zenders' beperken/wegnemen.
2. Weerbaarheid van de 'ontvangers' vergroten.
3. De confrontatie, op basis van inhoud, aangaan met het gedachtegoed van de 'zenders' en achterban.

Om de doelgroepen te bereiken, kan worden gedacht aan de volgende werkwijze
Zenders:

- De doelgroep in kaart brengen. Dit verschaft meer inzicht in de antidemocratische boodschap en achtergrond en maakt het makkelijker om adequaat te reageren en weerwoord te bieden.
- Kritisch en confronterend het gedachtegoed blootleggen en de discussie aangaan.

Ontvangers:

- Een kritische houding t.a.v. allerlei soorten (antidemocratisch) gedachtegoed stimuleren.
- Ondersteuning bieden waar de doelgroep competenties en vaardigheden mist om weerwoord te bieden of moeite heeft om de boodschappen van de 'zenders' in de juiste context te plaatsen.
- Faciliteren van activiteiten om het gedachtegoed bespreekbaar te maken.
- Er dient aandacht te zijn voor een blijvende inzet van de overheid om achterstanden weg te nemen. Dit kan helpen de geloofwaardigheid van de overheid en de rechtsstaat bij de doelgroepen in stand te houden en vermindert de voedingsbodem.

Concreet wordt geadviseerd om in te zetten op het weerbaarder maken van bijvoorbeeld leerkrachten en eerstelijnswerkers die in aanraking komen met potentieel radicaliserende jongeren en hen in staat te stellen om weerwoord te bieden tegen radicale en antidemocratische boodschappen.

Ondersteunend aan het bovenstaande is het om de bewustwording van de democratische kernwaarden te versterken geboden dat de overheid ook duidelijk aangeeft waar de grenzen liggen. Van handhavend optreden bij normoverschrijding zal een duidelijk signaal uitgaan. Ondersteunend aan het versterken van deze capaciteit is daarom het bevorderen van de bewustwording bij betrokken overheidsinstanties van het bestaan van een bestuursrechtelijk en strafrechtelijk handhavings-instrumentarium dat zich erop richt om direct en effectief handhavend op te kunnen treden als door personen of groepen actief wordt gestreefd naar diep ingrijpende veranderingen in de samenleving (eventueel op ondemocratische wijze), deze te

ondersteunen of anderen daartoe aan te zetten.[33] Het gaat hierbij hoofdzakelijk om het inzichtelijk maken van het reeds beschikbare bestuursrechtelijk en strafrechtelijk handhavings-instrumentarium, zodat daar op een goede en proactieve manier gebruik van kan worden gemaakt bij de bescherming van de openbare orde en veiligheid en ook ter bescherming van bepaalde groepen, grondrechten en de democratische rechtsstaat in algemene zin.

De verantwoordelijkheid voor het versterken van deze capaciteit ligt bij de rijksoverheid, meer specifiek bij het ministerie van Veiligheid en Justitie (NCTV en DGRR) in samenwerking met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

4. Aanpak van eenlingen

Eén van de strategische prioriteiten om extremisme en terrorisme tegen te gaan, betreft de aanpak van dreiging vanuit solistische dreigers. Dit zijn personen die (zonder medewerking van anderen) door middel van gedrag of woord als gevolg van een individueel doorlopen proces richting geweld een dreiging vormen.

Dit betreft een relatief nieuwe dreiging. Met de gebeurtenissen in onder andere Noorwegen nog vers in het geheugen, vindt de expertgroep het van groot belang dat hierin een coherent beleid ontstaat gericht op het (meer) zicht krijgen op het fenomeen en op het verhogen van de weerbaarheid tegen dergelijke dreigers.

Belangrijk aandachtspunt bij deze capaciteit is het risico dat ‘afwijkende’ meningen en gedragingen al gauw en soms ten onrechte als verdacht kunnen worden gezien. Bij de versterking van deze capaciteit moet dan ook de balans worden gezocht; het is ongewenst dat de aanpak ‘te ver doorschiet’.

De expertgroep adviseert de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) op te treden als initiatiefnemer en trekker/coördinator van deze beleidsontwikkeling.

Belangrijke peilers van de aanpak zouden moeten bestaan uit:

- Awareness/preventie: nodig is dat geradicaliseerde eenlingen vroegtijdig kunnen worden gesignaleerd. Deskundigheidsbevordering van eerstelijnswerkers in het onderwijs en welzijnswerk, politie is hierbij van cruciaal belang. Ook de (geestelijke) gezondheidszorg speelt hierbij – naast anderen – een belangrijke signaleren en behandelende rol. De expertgroep vraagt aandacht voor de (interne) regulering binnen de gezondheidssector. Het moet voor (geestelijke) gezondheidsprofessionals mogelijk zijn om signalen van eenlingen die mogelijk een extremistische of terroristische daad zullen plegen met de relevante instanties (politie, justitie) te delen. Eveneens moet zeker gesteld worden dat de genoemde professionals en andere oplettende burgers, weten waar ze met de signalen terecht kunnen.
- Toegang tot middelen: Het gevaar dat uitgaat van eenlingen wordt bepaald door de toegang tot informatie (bedreigingen) en tot middelen die deze groep heeft om hun intenties om te zetten in concrete daden. Te denken valt aan vuurwapens, munitie, explosieve stoffen en/of CBRN-middelen. Het is van cruciaal belang deze toegang tot een minimum te beperken.

[33] Ingrijpende veranderingen zijn ontwikkelingen die een gevaar kunnen opleveren voor de democratische rechtsorde (doel), vaak met ondemocratische methoden (middel), die afbreuk doen aan het functioneren van de democratische rechtsorde (effect).

B1.5 Thema Terrorisme: 'Reactie op exogeen jihadistische dreiging'

Sinds de aanslagen van 11 september 2001 in de Verenigde Staten staat terrorisme wereldwijd op de agenda. Ook in Nederland heeft deze dreiging volop de aandacht. In de afgelopen jaren hebben de verschillende ketenpartners een groot aantal capaciteiten versterkt om er voor te zorgen dat Nederland beter in staat is om te gaan met mogelijke terroristische dreigingen. Op dit terrein heeft de Nederlandse samenleving dan ook veel bereikt en geleerd. Over de voortgang van terrorismebestrijding wordt gerapporteerd via de Voortgangsrapportages Terrorismebestrijding. Voor een analyse van de nationale en internationale terroristische dreiging tegen Nederland, en Nederlandse belangen in het buitenland verwijs ik u naar het Dreigingsbeeld Terrorisme Nederland (DTN) van de NCTV en het Alerteringssysteem Terrorismebestrijding. Waar sprake is van generieke capaciteiten die over en weer bruikbaar zijn wordt intensief samen gewerkt, zodat we op alle gebieden van de nationale veiligheid weerbaarder zijn.

Het voorkomen van terrorisme is van wezenlijk belang. Niet alleen vanwege de vaak ernstige gevolgen van een aanslag in termen van verlies aan mensenlevens en materiële schade, maar evenzeer vanwege de schade die een aanslag of een dreiging toebrengt aan de democratische rechtsorde, de internationale positie van Nederland en niet te vergeten de sociaalpsychologische impact die het heeft. Daarvan is ook sprake als vitale onderdelen van onze samenleving zoals energie, communicatie of het bancaire systeem worden geraakt. Effectieve terrorismebestrijding richt zich daarom zowel op het wegnemen van de oorzaken van terrorisme als op het voorkomen ervan. Daarnaast zorgt terrorismebestrijding voor het treffen van beschermende maatregelen tegen een mogelijke aanslag en het voorbereid zijn op de gevolgen ervan.

Samenhang in de aanpak is noodzakelijk. Sinds 2005 zijn in Nederland diverse beleidsinitiatieven en -instrumenten tot stand gekomen om het risico op een terroristische aanslag te verminderen en de mogelijke schade na een eventuele aanslag te beperken. Ook zijn de nodige wetswijzigingen doorgevoerd om de samenhang, coördinatie en effectiviteit van het Nederlandse contraterrorismebeleid te vergroten. De belangrijkste verworvenheid laat zich echter niet vatten in een wet, regel of instrument. Het feit dat zoveel spelers in uiteenlopende netwerken actief zijn bij terrorismebestrijding vereist samenhang, afstemming en coördinatie. De samenhang tussen inlichtingen, beleid en operatie is de laatste jaren gegroeid en verstevigd door een centrale coördinatiestructuur. Een integrale en strategische visie op de toekomst van contraterrorisme in Nederland en regelmatige oefening en evaluatie blijven echter noodzakelijk om richting te geven aan alle partijen die bij contraterrorisme zijn betrokken en om alle schakels van de veiligheidsketen op sterkte te houden. De Nationale Risicobeoordeling draagt hier aan bij.

Het huidige contraterrorismebeleid kenmerkt zich door de zogeheten 'brede benadering'. Het streven is daarbij gericht op het vroegtijdig onderkennen van radicaliseringsprocessen bij groepen en individuen in binnen- en buitenland, zodat met behulp van gerichte interventiestrategieën voorkomen kan worden dat zij terroristisch geweld gaan plegen. Voor degenen die de stap naar geweldpleging reeds hebben gezet of op het punt staan dit te doen, zijn andersoortige ingrepen vereist van meer repressieve aard.

Op dit moment komt de terroristische dreiging voor Nederland nog altijd overwegend vanuit jihadistische hoek. Andere vormen van ideologisch gemotiveerd extremisme krijgen echter ook de nodige aandacht. Indien de inlichtingen- en veiligheidsdiensten daar de komende jaren

aanleiding toe zien , zullen ook deze vormen van extremisme vanuit CT-perspectief worden aangepakt.

Voor de periode 2011-2015 is in de aanpak van het internationaal jihadisme, de inzet gericht op het voorkomen en neutraliseren van verdere escalatie in de jihadistische strijdgebieden, het tegengaan van de verspreiding van jihadistische propaganda en het stimuleren van tegengeluiden. Om CT risico's van migratie en reisbewegingen te beperken zet de overheid in op de verbetering van de grensbewaking en de migratieketen, een betere informatiepositie van gemeenten en inlichtingendiensten en een verhoging van het veiligheidsbewustzijn bij de medewerkers van betrokken diensten. Door strategische samenwerking, het monitoren van relevante ontwikkelingen en de ondersteuning van fundamenteel onderzoek wordt de komende periode ingezet op het optimaal omgaan met de kansen en bedreigingen die technologie en innovatie bieden. Ten aanzien van Internet en CBRN/E worden maatregelen getroffen in samenwerking met partners in binnen- en buitenland. Ten slotte zijn onder andere de aanpak van geradicaliseerde eenlingen en het vergroten van 'security awareness & performance' onderdeel van de doorontwikkeling van het stelsel Bewaken en Beveiligen.

De Minister van Buitenlandse Zaken zorgt ervoor dat periodiek een graadmeter van relevante ontwikkelingen in het buitenland komt en dat de bevindingen worden gedeeld met alle relevante diensten. Daarnaast worden aparte instructies ingezet, indien daar aanleiding toe is. Bij de inzet van public diplomacy, woordvoering richting buitenlandse media en richting buitenlandse autoriteiten, worden de daarvoor relevante partijen betrokken. Deze aanpak heeft in meerdere gevallen, waaronder vóór, tijdens en na het uitbrengen van de film Fitna goede resultaten geboekt.

De onderstaande mogelijk te versterken capaciteiten zullen bijdragen aan de ondersteuning van het bestaande beleid en de te behalen resultaten voor de komende periode.

Geprioriteerde capaciteiten
Uit de Nationale Risicobeoordeling 2011 blijkt dat een terroristische dreiging altijd twee aspecten bevat: de mogelijkheid van een aanslag en de angst voor een aanslag. De dynamiek die de reactie van overheid, media en publiek op een dergelijke dreiging teweeg brengt, kan op zichzelf reeds in ernstige mate angstverhogend en ontwrichtend werken. Deze situatie leidt tot een grote impact op de integriteit van de internationale positie van Nederland, de democratische rechtsstaat en een grote sociaal-psychologische impact. De focus van de capaciteitenanalyse lag daarom op de vraag *of* en *hoe* de impact op deze drie belangrijke impactcriteria te verkleinen is.

1. Het vermogen om escalatie van maatschappelijke onrust in de kiem te kunnen smoren: Het sociaal calamiteitenplan[34]

Een sociaal calamiteiten plan is nodig om:
- vroegtijdig zicht te krijgen op ongewenste vormen van polarisatie en radicalisering of andere spanningen;
- voorbereid te zijn op situaties die vragen om een weerwoord of reactie anderszins op gesignaleerde spanningen door de overheid en haar partners;

[34] Omdat deze capaciteit ook als prioriteit is gesteld in de werkgroep voor de capaciteitenanalyse op het thema polarisatie en radicalisering, is de tekst in samenwerking met deze werkgroep tot stand gekomen. I.v.m. eventuele aanpassingen is de tekst van de werkgroep polarisatie en radicalisering leidend.

- in staat te zijn om effectief (de-escalerend) te kunnen handelen in geval van een daadwerkelijke crisis/calamiteit met betrekking tot het escaleren van spanningen door de overheid en haar partners.

Om dit te bereiken is van belang dat het plan voorziet in:
- het opzetten van een systeem van vroegsignalering en daarmee gepaard gaand, het opbouwen en onderhouden van een netwerk van maatschappelijke en hulpverleningsorganisaties en sleutelfiguren in de gemeentelijke samenleving (inzetbaar in koude en warme fase);
- een duidelijk profiel van de sleutelfiguren die nodig zijn binnen het netwerk;
- een crisisorganisatie die goed aansluit op de reguliere crisisorganisatie;
- (voorbereiding op) crisiscommunicatie, waaronder woordvoering, gebruik van sociale media en (evt.) opstellen vraag en antwoord lijst;
- een crisiscommunicatieadviseur ;
- bestrijdingsplannen afgestemd op potentiële scenario's;
- een aanpak voor nazorg en herstel.

Een sociaal calamiteitenplan is tweeledig, het richt zich op preventie met de-escalatie en repressie als sluitstuk. Door te zorgen dat vooral een gemeente/regio en haar samenwerkingspartners voorbereid zijn, kan er adequaat worden opgetreden. Het gaat om vroegtijdig signaleren, goede duiding geven van het probleem en samenwerking met relevante partners. Communicatie speelt ook een belangrijke rol. Tegen deze achtergrond moet door het Rijk verder gestimuleerd worden dat gemeenten, regio's en de rijksoverheid beschikken over een dergelijk plan. De basisverantwoordelijkheid voor ontwikkeling en implementatie van een lokaal sociaal calamiteitenplan ligt bij de lokale overheden. Bij het verkrijgen van voldoende bestuurlijk draagvlak voor de ontwikkeling van een lokaal sociaal calamiteitenplan dienen ook de Veiligheidsregio's betrokken te worden. Met betrekking tot dit laatste kan dit onder andere vorm krijgen door het onderwerp op te nemen in de jaarlijkse voortgangsgesprekken die het ministerie van Veiligheid en Justitie voert met de verschillende Veiligheidsregio's en door het onderwerp te agenderen bij het Veiligheidsberaad.

2. <u>Het vermogen van inlichtingen-, veiligheids- en opsporingsdiensten om onderzoek te doen naar potentiële dreigingen.</u>

Het gaat daarbij om het op peil houden en waar nodig versterken van de onderzoeksmogelijkheden van inlichtingen-, veiligheids- en opsporingsdiensten, bijvoorbeeld om in de technische wedloop een voorsprong te behouden op de 'targets'. Dit is nodig omdat inlichtingen-, veiligheids- en opsporingsdiensten in de uitvoering van hun wettelijke taken worden geconfronteerd met twee belangrijke, met elkaar samenhangende trends: 'internationalisering' en 'technologisering'. Deze trends beïnvloeden de te beschermen nationale veiligheidsbelangen, de bedreiging daarvan en het te organiseren weerstandsvermogen. Zo worden de risico's en bedreigingen voor de Nederlandse veiligheidsbelangen sterk beïnvloed door de snelle ontwikkelingen op het gebied van informatie- en communicatietechnologie. De nieuwste toepassingen vinden hun weg snel, ook naar de onderzoekssubjecten van de diensten. Het belang om deze 'wedloop' bij te houden is cruciaal.

Hier kan worden aangesloten bij bestaand beleid en zonodig zal nieuwe wetgeving moeten worden gerealiseerd. Zo is er thans een wijziging van de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 in voorbereiding, om zeker stellen dat deze actueel genoeg is voor nieuwe technische ontwikkelingen.

Op dit moment is het niet zo dat de huidige investeringen tekort schieten om de inlichtingenpositie op peil te houden, maar in de toekomst kan een extra investeringsinzet noodzakelijk zijn om geen achterstand op te lopen. Nieuwe bedreigingen zijn vaak (nog) niet zichtbaar, wat kan betekenen dat argumenten ter onderbouwing van het nut en de noodzakelijkheid van nieuwe maatregelen een uitdaging vormt. Indien nut en noodzaak echter onvoldoende voor het voetlicht gebracht worden, kan dit de realisatie van deze capaciteit in de weg staan. Uiteraard gelden ook de eisen van proportionaliteit en subsidiariteit t.a.v. de mogelijkheden voor de diensten.

3. Het vermogen om de goede positie van Nederland in het buitenland te handhaven; De inzet van diplomatie

De ervaringen met het uitbrengen van de film Fitna leren dat de in Nederland gebruikte opzet en aanpak voor *public diplomacy* en woordvoering richting buitenlandse media en autoriteiten succesvol was en dat de *sense of urgency* bij alle betrokkenen voldoende aanwezig is. Op dit moment is het echter de praktijk dat deze cyclus alleen wordt doorlopen bij een daadwerkelijke aanleiding: er vindt geen oefening van deze cyclus plaats. Het is verstandig als de actoren uit deze samenwerkingscyclus vaker bijeen komen. Het is van belang om deze samenwerkingscyclus op te nemen in de oefenprogramma's van de NCTV. Het gaat daarbij met name om het oefenen van de samenwerkingscyclus op het niveau van adviesteams.

4. Het vermogen van bestuurders om op het juiste moment en op de juiste wijze de juiste beslissing te nemen: Opleiden, trainen, oefenen, testen, evalueren, lessen leren.

Geconcludeerd is dat, ofschoon er in Nederland sprake is van zeer capabele bestuurders en voldoende CT-beleid en –maatregelen, deze zelfde bestuurders weinig ervaring kunnen opdoen met de in het scenario geschetste ontwikkelingen. Het is, gelukkig, onze huidige werkelijkheid dat zich niet vaak genoeg crises in de realiteit voordoen om de kennis en vaardigheden die nodig zijn in de praktijk te trainen. Geconstateerd is dat deze ervaring juist wel een maak- of breekpunt voor capabel optreden in crisissituaties vormt. Het belang van trainen en oefenen is daarom groot om zo de lacune van daadwerkelijke ervaringen in de realiteit op te vullen. Bovendien leveren de evaluaties van zowel oefeningen als incidenten waardevolle inzichten op. Met de lessons learned en de geconstateerde verbeterpunten worden procedures en protocollen aangescherpt dan wel aangepast. Daarom is het noodzakelijk dat deze lacune voldoende wordt aangevuld met gesimuleerde mogelijkheden. Juist daarvoor is OTOTEL (Opleiden, Trainen, Oefenen, Testen, Evalueren, Lessen leren) de aangewezen functionaliteit.

Op hoog bestuurlijk niveau is ruimte om met meer trainen van vaardigheden het optreden te professionaliseren, bijv. door het instellen van een permanente OTOTEL-cyclus voor bewindspersonen. Het is mogelijk om in vaardigheidstrainingen accenten te kiezen en maatwerk te leveren, toegespitst op de aard van een crisis of op de persoon van de getrainde. Deze trainingen werpen niet alleen vruchten af bij een crisis, maar zullen de bewindspersonen ook op andere momenten van dienst kunnen zijn.

Daarbij moet worden aangetekend dat het effect van een oefening alleen kan worden gemaximaliseerd wanneer *alle* oefenonderdelen met gelijke aandacht en intensiteit worden doorlopen. Helaas gebeurt dit niet altijd. Zo vormt bijvoorbeeld de crisis*communicatie* door bestuurders een onderdeel van alle oefeningen, maar wordt dit niet altijd even consciëntieus uitgevoerd als de onderdelen crisis*besluitvorming*. Dit zal moeten veranderen: pas als alle onderdelen van een oefening even serieus worden genomen kan het doel, dat de oefening beoogd, worden bereikt.

De maatschappelijke en/of veiligheids- opbrengst van het verbeteren van de functionaliteit OTOTEL is dat we door opleiden, trainen en oefenen (OTO) kunnen bereiken dat bestuurders de juiste beslissingen nemen, daarover op een gepaste wijze communiceren, bestand zijn tegen druk, de middelen die ze hebben goed inzetten, en daardoor maatschappelijke onrust beter kunnen bezweren. Door testen, evalueren en lessen leren (TEL) kunnen we bereiken dat we flexibel zijn in het adresseren van (nieuwe) ontwikkelingen/tekortkomingen die voor een adequate crisisbestrijding relevant zijn. Zo komt op dit moment beeldvorming via en gebruik van sociale media als belangrijk aandachtspunt uit evaluaties naar voren. Maar dat kan over een paar jaar hebben plaatsgemaakt voor een ander aandachtspunt.

De condities voor goed functioneren van OTOTEL kunnen nog worden verbeterd. Vanzelfsprekend gaat het bij essentiële randvoorwaarden om: helderheid over de doelstelling van de organisatie en helderheid over rolverdeling en inhoud van rollen. Daarnaast staat een veilige leeromgeving centraal en moet er bereidheid zijn om voor het leveren van maatwerk extra middelen in te zetten. Maar bovenal is draagvlak en *commitment* op hoog ambtelijk en politiek niveau essentieel, vooral als het gaat om Testen, Evalueren en Lessen leren. De organisatie die uitvoering kan geven aan de (realisatie van de) capaciteit is in eerste instantie de afdeling OTOTEL (in oprichting) van de NCTV van het ministerie van Veiligheid en Justitie. Deze afdeling coördineert alle aspecten van de OTOTEL-cyclus en speelt een grote rol in de organisatie van zowel specifieke antiterrorisme-oefeningen als voor grote interdepartementale oefeningen op ministerieel niveau.

B1.6 Thema Internationaal: 'Crisis buiten de EU'

Inleiding
Steeds meer raken gebeurtenissen en ontwikkelingen die zich in het buitenland afspelen, de veiligheid van Nederland. Nederland is een open maatschappij en kan zich niet isoleren van het buitenland. Het is belangrijk na te gaan hoe die processen werken en de nationale veiligheid beïnvloeden. Het Ministerie van Buitenlandse Zaken (BZ) heeft het afgelopen jaar geparticipeerd in de NRB. Daarbij is gebleken dat de systematiek van de NRB kan werken voor een scenario dat zich in het buitenland afspeelt en waarvan de gevolgen in Nederland worden gevoeld maar dat voor een volgend internationaal scenario de procedure enige aanpassing behoeft gezien de complexiteit en diversiteit in een internationale context.

Scenario
Voor de capaciteitenanalyse internationaal is gebruik gemaakt van een scenario dat een reeks gebeurtenissen in het buitenland beschrijft. Deze ontwikkelingen vormen een complex geheel en hebben impact op Nederland, en op Nederlandse belangen en burgers in het buitenland. Het scenario verschilt van gebruikelijke NRB (incident-)scenario's: er is geen sprake van één gebeurtenis die bepalend is voor de impact. Het betreft een complex geheel van diverse op elkaar volgende gebeurtenissen, waardoor volgens het scenario de overheid tegelijkertijd te maken krijgt met een handelsconflict, spanningen in bilaterale en multilaterale relaties, verminderde technologische capaciteit op een ambassade en consulaire ontwikkelingen.

Bestaand beleid ten aanzien van crises in het buitenland
Met enige regelmaat krijgt het ministerie van BZ te maken met crises op een aantal beleidsterreinen, waaronder consulaire zaken, humanitaire hulpverlening en politieke zaken. Het volgen van en inspelen op politieke ontwikkelingen in het buitenland is een kerntaak van BZ. Ook hierbij kunnen zich situaties voordoen die crisisachtige vormen aannemen en waarvoor een routinematige aanpak niet meer volstaat. Het ministerie heeft een eigen Crisis Coördinator die direct onder de departementsleiding is geplaatst. Deze verzorgt de dagelijkse werkzaamheden met betrekking tot crisismanagement, treedt coördinerend op tijdens crises en vertegenwoordigt BZ in interdepartementaal crisisoverleg.

Beschrijving en uitwerking van mogelijk te versterken capaciteiten
Zich baserend op het voorliggende scenario zijn door de expertgroep capaciteiten geïdentificeerd die van belang zijn om in het scenario beschreven ontwikkelingen te voorkomen of om adequaat te kunnen optreden als deze zich toch voordoen. Vier capaciteiten krijgen prioriteit.

Capaciteit 1: strategische analyse en besluitvorming

De experts constateren dat de complexiteit van buitenlandse ontwikkelingen meer in samenhang kan worden geanalyseerd. Om dit te versterken beveelt de expertgroep aan om een structuur te organiseren met het doel om op basis van periodieke risicoanalyse, potentiële dreigingen voor de Nederlandse veiligheid te benoemen. Hierdoor kunnen in het buitenland ontwikkelende crises zoveel mogelijk vroegtijdig worden geïdentificeerd, zodat ook beleidsinterventies tijdig kunnen worden geformuleerd.

Capaciteit 2: uitvoering van een regiefunctie

Ten tijde van een crisis in het buitenland die Nederlandse belangen raakt is het optreden van de overheid cruciaal. Het vermogen tot handelen op basis van beschikbare analyses, en het afwegen van de verschillende belangen zijn van politiek, economisch en soms levensbelang. De experts constateren dat de regiefunctie in de praktijk anders verloopt dan wenselijk. Omdat de complexiteit van buitenlandse ontwikkelingen en de mogelijke effecten op de nationale veiligheid, in combinatie met een goed inzicht in de Nederlandse belangen in het buitenland, beter kunnen worden geanalyseerd (capaciteit 1) verloopt het gestructureerd en georganiseerd handelen ten tijde van een crisis niet optimaal. Op basis hiervan adviseren de experts om de regie rondom een zich in het buitenland ontwikkelende crisis te verbeteren, en om de coherentie en reactiesnelheid te verbeteren.

Capaciteit 3: inzet diplomatie

De inzet van diplomatie is één van de belangrijkste capaciteiten die de overheid tot haar beschikking heeft vóór, tijdens en ná een internationale crisis. In termen van kwantiteit is de diplomatieke dienst voldoende toegerust, de experts constateren echter dat het optreden voorafgaand aan crises kan worden verbeterd. Het gaat dan vooral om het rijksbrede vermogen vroeg te signaleren dat ontwikkelingen het potentieel voor een crisis hebben en volledig inzicht op waar dit de Nederlandse belangen kan raken. Deze capaciteit geeft input voor strategische analyse (capaciteit 1).

Capaciteit 4: inzet inlichtingendiensten

De experts constateren dat het gebruik van inlichtingen door departementen niet optimaal is,. De bestuurlijke top kan bij crises meer gebruik maken van de kennispositie van inlichtingendiensten. De inlichtingendiensten kunnen een sterkere positie krijgen in de strategische analyse en besluitvorming (zie capaciteit 1). Tevens kunnen de diensten een permanente relatie ontwikkelen met een regie-functie (zie capaciteit 2). Dergelijke maatregelen waarborgen de beschikbaarheid van analyses aan het begin van een crisis en geven de mogelijkheid om de bijzondere capaciteiten van de diensten in te zetten.

B1.7 Thema klimaat: ‘Milde en Ernstige grieppandemie’

Inleiding

Grieppandemieën ontstaan zeer onvoorspelbaar, maar komen wel met een zekere regelmaat voor. In 2009 werd de wereld geconfronteerd met een nieuwe virusvariant: Influenza A H1N1 2009, in de volksmond Mexicaanse griep genoemd. Deze pandemie was in zijn effect mild te noemen. Mild in de zin van het aantal besmette personen en de kans op overlijden ten gevolge van de griep. Het was ook de eerste pandemie waar wereldwijd vooraf enige mate van preparatie heeft plaatsgevonden. Zo hebben overheden plannen ontwikkeld om voorbereid te zijn op een pandemie en er zijn antivirale middelen op voorraad genomen.
Het handelen van de overheid en de World Health Organisation (WHO) is geëvalueerd en een nieuwe stroom van wetenschappelijke publicaties over interventiestrategieën is op gang gekomen. Vele facetten die bij voorbereiding van de pandemie zijn ontwikkeld zijn tijdens de pandemie in 2009 aan de orde gekomen, en in zekere zin geoefend. Door het milde verloop van de pandemie is echter de bereidheid om voorbereidingen te treffen voor een volgende pandemie waarschijnlijk afgenomen.

De afgelopen jaren is er veel gebeurd om de voorbereiding op grote uitbraken, zoals een grieppandemie, te verbeteren. Het Centrum Infectieziektebestrijding dat in 2005 is opgericht bij het RIVM heeft hiertoe verschillende activiteiten ondernomen. Er zijn protocollen en draaiboeken ontwikkeld en het RIVM heeft vele activiteiten ondernomen om GGD’en te ondersteunen bij het uitvoeren van epidemiologisch onderzoek of bij de bestrijding van een uitbraak van infectieziekten. Het CIb is in 2010 positief geëvalueerd. Vanaf december 2008 zijn de mondiale afspraken om infectieziekten snel op te kunnen sporen, te melden en te bestrijden, de zogenaamde International Health Regulations, opgenomen in de Nederlandse Wet publieke gezondheid. Tot slot is de afgelopen jaren gewerkt aan schaalvergroting binnen de infectieziektebestrijding. Met de totstandkoming van de Wet veiligheidsregio’s (oktober 2010) en de wijziging van de Wet publieke gezondheid in aansluiting daarop (januari 2012), is het bestuur van de veiligheidsregio verantwoordelijk geworden voor de voorbereiding en bestrijding van een grootschalige infectieziektecrisis. Hierdoor liggen bij een infectieziektecrisis de bevoegdheden voor de infectieziektebestrijding en veiligheid in elke regio in één hand. Het crisisplan moet gezamenlijk worden vastgesteld door het bestuur van de veiligheidsregio en het bestuur van de GGD en gaat ondermeer in op de rol van de GGD/GHOR en de afstemming met het RIVM en (private) zorgpartijen. Het moet aandacht besteden aan de communicatie richting burgers, bedrijven en scholen en gaat in op het treffen van diverse maatregelen, zoals het afgelasten van evenementen en handhaven daarvan door de politie.

Tevens is met de wijziging van de Wet publieke gezondheid de GGD organisatie en GHOR organisatie onder één directeur gebracht, de directeur publieke gezondheid (DPG). In tijd van crisis treedt de DPG coördinerend en adviserend op, op het terrein van de infectieziektebestrijding en volksgezondheidsvraagstukken en geeft leiding aan de geneeskundige hulpverlening door de gehele ‘witte kolom’.

De bestrijding van de pandemie in Nederland is geëvalueerd. De bestrijding is in grote lijnen snel en adequaat verlopen. Dat het geeft vertrouwen voor toekomstige grootschalige infectieziekte-uitbraken, maar betekent niet dat geen verbeteringen mogelijk zijn. De verbinding tussen de infectieziektebestrijding en de curatieve sector kan worden verbeterd. Op nationaal niveau kan het Centrum Infectieziektebestrijding van het RIVM hierin een rol

vervullen door meer curatieve partners in hun netwerk te betrekken. Op regionaal niveau heeft de GHOR een belangrijke schakelfunctie. De IGZ heeft het functioneren van de GHOR tijdens de Mexicaanse griep onderzocht. De IGZ constateert dat de GHOR haar wettelijke taken goed heeft uitgevoerd, maar dat het imago en de zichtbaarheid van de GHOR verbeterd kunnen worden. Ook wijzen zij op het belang van meer (multidisciplinair) oefenen met het pandemiescenario.. De ministers van VenJ en VWS hebbende aanbevelingen uit dit onderzoek onder de aandacht gebracht van de verantwoordelijke bestuurders. Ook is geconcludeerd dat de verbinding met andere (niet medische) sectoren kan worden verbeterd. In het influenza pandemie beleidsdraaiboek dat nu wordt geactualiseerd zal daarom ook de breedte van de maatschappelijke consequenties van de bestrijdingsmaatregelen worden gewogen.
Daarnaast is bij de evaluatie geconcludeerd dat er maar op beperkte schaal internationale afstemming plaatsvond. De Europese Commissie heeft inmiddels een voorstel gedaan voor de stroomlijning en versterking van de capaciteiten en structuren van de Europese Unie om doeltreffend te reageren op ernstige grensoverschrijdende gezondheidsbedreigingen. Nederland heeft met enkele kritische kanttekeningen positief gereageerd op het voorstel.

Scenario's

In 2007 zijn voor de Nationale Risico Beoordeling twee grieppandemie scenario's ontwikkeld De bevindingen van de grieppandemie uit 2009 hebben geleid tot de behoefte om het onderwerp grieppandemie in de NRB opnieuw tegen het licht te houden en daarin de ervaringen van de Mexicaanse griep te betrekken. In opdracht van het analistennetwerk Nationale Veiligheid zijn twee nieuwe grieppandemie scenario's uitgewerkt: een mild scenario en een scenario met ernstiger gevolgen. Uitgangspunt voor deze scenario's is gebruik te maken van meer recente (wetenschappelijke) inzichten – waaronder de ervaringen met de Mexicaanse griep – en van recente studies naar maatschappelijke onrust.

Beschrijving en uitwerking van mogelijk te versterken capaciteiten

Gebaseerd op deze scenario's en de ervaringen van de pandemie van 2009 hebben experts capaciteiten geïdentificeerd die van belang zijn om verder op te pakken. Onderstaand volgt een selectie van de capaciteiten die met voorrang opgepakt worden.

Optimaal benutten zorgcapaciteit

Tijdens grote uitbraken van infectieziekten kan een ernstig capaciteitgebrek in de zorg ontstaan, vooral wat betreft het aantal beschikbare bedden op de intensive care. Ziekenhuizen beschikken over een ziekenhuisrampenopvangplan (ZIROP) waarin rekening wordt gehouden met pandemieën. Ze zijn in staat om IC capaciteit te organiseren en een triagering te implementeren om de capaciteit optimaal in te zetten. De medische beroepsgroepen kunnen over gaan op selectieve zorg en niet noodzakelijke afdelingen sluiten.

Er komt een moment dat zware beslissingen moeten worden genomen over het prioriteren van zorg omdat de capaciteit, ondanks bovengenoemde maatregelen, onvoldoende blijkt. Afspraken over wie deze beslissingen maakt, op basis van welke informatie, moeten verder worden uitgewerkt en vastgelegd. Hierover voert VWS momenteel overleg met de diverse betrokken

Verbeteren risicocommunicatie

Tijdens een pandemie zal een groot beroep worden gedaan op het vermogen van bestuurders en operationele diensten om goed over risico's te communiceren. Ook in andere evaluaties naar het overheidsoptreden bij crises komt dit onderwerp nadrukkelijk aan de orde. Het meest recente is de evaluatie van de afhandeling van de brand bij Chemie-Pack in Moerdijk. De kennis over risicocommunicatie en de bewustwording van de rol die dit inneemt behoeft versterking. In de reactie op het rapport van de Onderzoeksraad voor veiligheid naar de brand bij Chemie-Pack d.d. 10 februari 2012[35] benoemt de Minister van V&J verschillende algemene activiteiten die nationaal worden genomen om de crisiscommunicatie, inclusief de regionale ondersteuning, te versterken.

Versterk de rol van 'eerstelijnszorg' (huisartsen, verpleegkundigen) in communicatie richting burger.

Specifiek voor een gezondheidskundige crisis zijn de eerstelijnszorgverleners (o.a. huisartsen en verloskundigen) van cruciaal belang. Dit is ook gebleken bij de grieppandemie in 2009. De overheid communiceerde centraal over de handelingsperspectieven voor burgers. Er bleek een duidelijke wisselwerking te bestaan tussen de nationale communicatie en de toeloop van mensen (patiënten en '*worried well*') naar de eerstelijnszorg. Hoewel eerstelijns zorgverleners voldoende worden geïnformeerd via de reguliere kanalen (RIVM en GGD'en), zouden zij actiever betrokken kunnen worden bij de vormgeving van de communicatie richting publiek. Huisartsen en verloskundigen zijn in de aanloop en tijdens de pandemie immers een belangrijke bron van informatie voor hun patiënten. Zij moeten de algemene adviezen van CIb en GGD omzetten in op de individuele patiënt toegesneden handelingsperspectieven. Het ministerie van VWS zal daarom, ten tijde van een pandemie, met vertegenwoordigers van de eerstelijnszorg overleggen over de inhoud van de communicatieboodschappen om tot een optimale afstemming te komen. In het nationale draaiboek grieppandemie zal hieraan aandacht besteed worden. Ook worden de bijdrage die eerstelijn zorgverleners kunnen leveren expliciet meegenomen in de regionale crisisplannen.

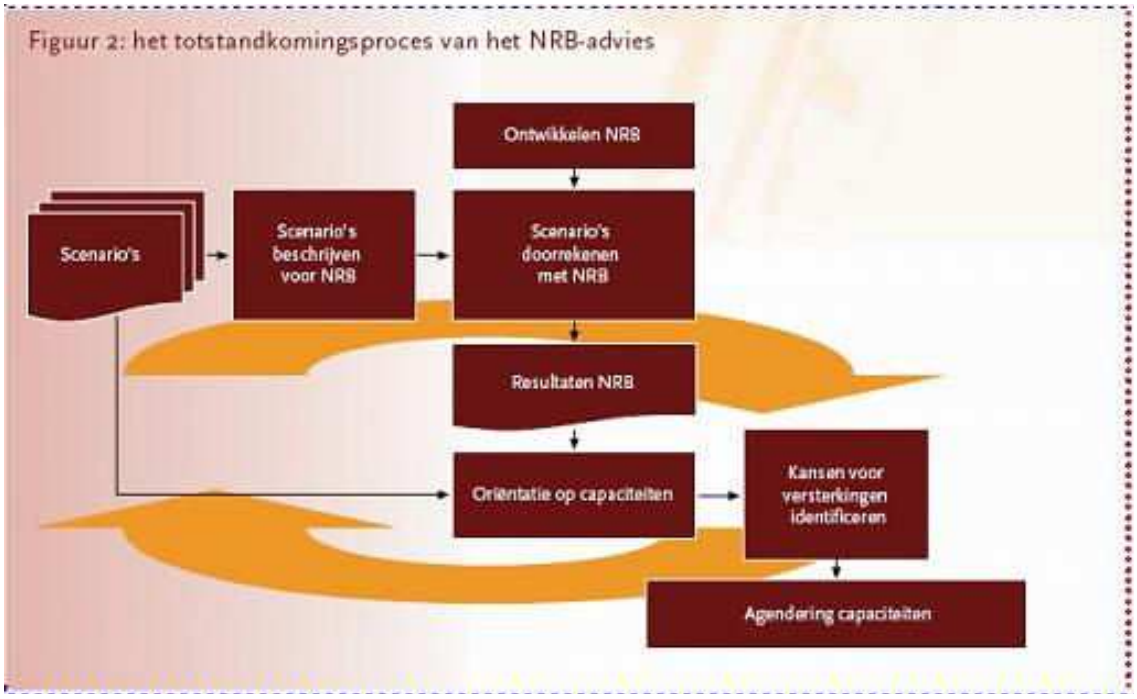
[35] Tweede Kamer 2011-2012, 26956, nr 116.

Bijlage 2 Methodiek: van scenario's tot capaciteiten

B2.1 Inleiding

In deze paragraaf wordt de methodiek van de onderdelen van de bevindingenrapportage beschreven (zie onderstaande figuur 3). De belangrijkste onderdelen zijn:

- Scenario's (B3.2);
- Nationale RisicoBeoordeling (NRB) (B3.3)
- Oriëntatie op capaciteiten (B3.4)



Figuur 3: het totstandkomingsproces van het NRB-advies

Een meer uitgebreide beschrijving van de methodiek staat in het document 'Werken met scenario's, risicobeoordeling en capaciteiten in de strategie Nationale Veiligheid' van oktober 2009.

B2.2 Scenario's

Een scenario biedt een manier om te communiceren over en een (gezamenlijk) gevoel te krijgen voor toekomstige onzekerheden en factoren die van invloed zijn op beslissingen van nu. De scenario's zijn echter geen toekomstvoorspellingen. Een scenario is in de context van de nationale risicobeoordeling een beschrijving van één of meer met elkaar verband houdende gebeurtenissen ('incidenten') die gevolgen hebben voor de nationale veiligheid. Het scenario beschrijft de aanloop tot de gebeurtenis(sen), de context en de gevolgen van de gebeurtenis(sen).

Voor de ontwikkeling van scenario's gelden de volgende uitgangspunten. Alle scenario's zijn in beginsel mogelijk ('het kan gebeuren') maar niet met dezelfde waarschijnlijkheid. Er wordt rekening gehouden met bestaande maatregelen voor preventie, preparatie, repressie en nazorg.

Scenario's moeten een impact hebben op nationale schaal en op minstens één van de vitale belangen (territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid, en sociale en politieke stabiliteit) om opgenomen te worden in de nationale risicobeoordeling.

B2.3 Nationale Risicobeoordeling

De NRB-methode is een wetenschappelijk verantwoorde methode voor het vergelijken en rangschikken van risico's voor de nationale veiligheid. Deze methode is ontwikkeld in een werkgroep met deelnemers uit de wetenschappelijke wereld[36]. In deze methode worden incidentscenario's beoordeeld aan de hand van tien impactcriteria en de waarschijnlijkheid van het scenario. De NRB-methode is geschikt voor alle typen scenario's en biedt de ingrediënten en de werkwijze om scenario's vanuit een multidisciplinair perspectief te beoordelen naar impact en waarschijnlijkheid.

Impactbeoordeling

De gekozen impactcriteria voor de nationale risicobeoordeling zijn de directe vertaling van de Strategie Nationale veiligheid: bescherming van de vitale belangen van Nederland. Elk van de vijf vitale belangen is vertaald naar één tot maximaal drie impactcriteria. De tien gekozen criteria worden samen representatief geacht voor het kunnen beoordelen en rangschikken van alle mogelijke incidentscenario's op basis van impact (schade, verlies, kosten e.d.).

Territoriale veiligheid	1.1 Aantasting van de integriteit van het grondgebied
	1.2 Aantasting van de integriteit van de internationale positie van Nederland.
Fysieke veiligheid	2.1 Doden
	2.2 Gewonden en chronisch zieken
	2.3 Gebrek aan primaire levensbehoeften
Economische veiligheid	3.1 Kosten
Ecologische veiligheid	4.1 Langdurige aantasting van milieu en natuur (flora en fauna)

[36] Technische Universiteit Delft, het Sociaal en Cultureel Planbureau, TNO Defensie en Veiligheid, AON Global Risk Consulting, hetRijksinstituut voor Volksgezondheid en Milieu, het Milieu en Natuur Planbureau (nu Planbureau voor de Leefomgeving (PBL)), de AIVD en het ministerie van Veiligheid en Justitie.

Sociale en politieke stabiliteit	5.1 Verstoring van het dagelijkse leven
	5.2 Aantasting van de democratische rechtsstaat
	5.3 Sociaal-psychologische impact: angst en woede

De scores van een scenario op alle impactcriteria worden geaggregeerd tot een eindscore voor de totale impact van een scenario.

Waarschijnlijkheidsbeoordeling
Waarschijnlijkheid is de verwachting over het optreden van het scenario-incident met zijn gevolgen in de komende vijf jaar. Elk scenario wordt geanalyseerd en beoordeeld op de waarschijnlijkheid dat het zich voordoet. Daarbij wordt een onderscheid gemaakt naar opzettelijk veroorzaakte en niet opzettelijk veroorzaakte dreiging.

Het resultaat
De scores van de scenario's worden uitgezet in een (logaritmisch opgebouwd) risicodiagram. Op de verticale as is de impact uitgezet. Op de horizontale as is de waarschijnlijkheid uitgezet. Het risicodiagram kan ondersteuning bieden bij het bepalen van de capaciteiten[37] die versterking behoeven en de prioritering die hierin aangebracht kan worden. In de fase van de strategische planning wordt met behulp van deze prioritering bekeken welke capaciteiten versterkt moeten worden ter voorkoming van deze dreigingen, of voor een adequate bestrijding van de gevolgen.

B2.4 Oriëntatie op capaciteiten

Om te kunnen bepalen welke risico's met voorrang moeten worden aangepakt en welke capaciteiten daarvoor moeten worden versterkt, worden de scenario's met behulp van de uitkomsten van de NRB geanalyseerd. De analyse richt zich vooral op aangrijpingspunten voor vermindering van de waarschijnlijkheid (preventie) of de omvang van de gevolgen van een risico (door middel van preparatie, respons en nafase). In deze oriëntatie op capaciteiten (capaciteitenanalyse) gaat het niet alleen om (versterking van) capaciteiten van de rijksoverheid, maar ook die van medeoverheden, die van burgers en maatschappelijke instellingen en bedrijven (met name bedrijven in vitale sectoren). Doel van de capaciteitenanalyse is te komen tot een agenda voor mogelijk te ontwikkelen en/of te

[37] Een capaciteit is het vermogen van de (rijks)overheid en private partners om taken uit te voeren op het gebied van nationale veiligheid. Het gaat hierbij om bepaalde combinaties van middelen (bijv. materiaal of informatiesystemen), mensen (civiel, militair, et cetera) en methoden (zoals procedures, plannen, oefenen, PPS-verbanden).

Capaciteiten helpen de kans en/of de impact van een of meerdere dreigingen te reduceren.

versterken capaciteiten. De capaciteitenanalyses zijn uitgewerkt door thematische expertgroepen.

Na iedere cyclus worden verbeterpunten geïdentificeerd en geïmplementeerd.