



Ministerie van Veiligheid en Justitie

Nationale Risicobeoordeling Bevindingenrapportage 2010

30 november 2010

Inhoudsopgave

INHOUDSOPGAVE	3
1. INLEIDING	5
1.1 AANLEIDING	5
1.2 STRATEGIE NATIONALE VEILIGHEID	5
1.3 BEVINDINGENRAPPORTAGE NV 2010	7
1.4 LEESWIJZER.....	7
2. SCENARIO'S EN UITKOMSTEN NATIONALE RISICOBEOORDELING	9
2.1 INLEIDING.....	9
2.2 GEKOZEN SCENARIO'S 2010	9
2.3 HET TOTAAL VAN SCENARIO'S.....	10
2.4 SAMENVATTING NIEUWE SCENARIO'S	12
2.4.1 ICT-uitval.....	12
2.4.2 Grootschalig ongeval	14
2.4.3 Scenario's Schaarste.....	14
2.5 UITKOMSTEN NATIONALE RISICOBEOORDELING.....	16
2.5.1 Leeswijzer risicodiagram	16
2.5.2 De plaats van de nieuwe scenario's in het risicodiagram	17
2.5.3 Overzicht impactscores van de scenario's.....	17
3. ORIËNTATIE OP CAPACITEITEN	19
3.1 INLEIDING.....	19
3.2 ICT-UITVAL.....	19
3.3 GROOTSCHALIG ONGEVAL.....	24
3.4 SCHAARSTE	28
3.5 CONCLUSIE.....	33
4. AGENDERINGSADVIES	35
4.1 INLEIDING	35
4.2 AANBEVELING 2010: BREED INZETBARE CAPACITEITEN.....	35
4.2.1 Integratie nationale veiligheidsbelangen in internationaal beleid	36
4.2.2 informatiewinning, analyse en deling.....	37
4.2.3 Nationale veiligheidsbelangen in publiek private verhoudingen (Governance)	38
4.2.4 Communicatie bij dreiging en crisissituaties	39
4.3 AANBEVELINGEN 2010: SPECIFIEKE CAPACITEITEN	40
4.3.1 ICT-uitval.....	40
4.3.2 Grootschalig ongeval	42
4.3.3 Schaarste	42
4.4 TOT SLOT.....	43

BIJLAGE 1 METHODIEK: VAN SCENARIO'S TOT CAPACITEITEN	45
B1.1 INLEIDING	45
B1.2 SCENARIO'S.....	45
B1.3 NATIONALE RISICOBEOORDELING	46
B1.4 ORIËNTATIE OP CAPACITEITEN	47
BIJLAGE 2 UITGEBREIDE LEESWIJZER RISICODIAGRAM	48
BIJLAGE 3 OPBOUW IMPACTSCORES SCENARIO'S	50
B3.1 NIEUWE SCENARIO'S	50
B3.2 IMPACTSCORES SCENARIO'S VORIGE NRB CYCLI	51
BIJLAGE 4 OVERZICHT WAARSCHIJNLIJKHEID EN IMPACTSCORES VAN DE SCENARIO'S	53

1. Inleiding

1.1 Aanleiding

Risico's zijn in ons dichtbevolkte land, met zijn open karakter, industrieën en drukke transportroutes niet uit te sluiten. Niemand kan een garantie krijgen op 100% veiligheid. Ons land kan op talloze manieren worden bedreigd, bijvoorbeeld door overstromingsgevaar, vogelgriep en internetterreur. De gevolgen van dreigingen en de kans erop kunnen worden beperkt en mensen kunnen zich ook voorbereiden op mogelijke dreigingen.

Het doel van het interdepartementale programma Nationale Veiligheid sluit hier op aan: het beschermen van de vitale belangen van Nederland en het voorkomen van maatschappelijke ontwrichting.

Wat zijn de meest urgente dreigingen voor Nederland? Wat moeten we doen om deze te voorkomen en hoe moet ons land reageren als het toch misgaat? Welke investeringen moeten we doen om dreigingen te voorkomen of de gevolgen ervan te beperken: inkopen van vaccins, bestrijding van computercriminaliteit of aanpak van radicalisering? Om deze vragen te kunnen beantwoorden is een meetlat ontwikkeld waarlangs verschillende dreigingen kunnen worden gelegd. Zo ontstaat een totaal overzicht van de dreigingen die de nationale veiligheid kunnen aantasten. Dit overzicht vormt een afwegingskader voor beslissingen over het al dan niet nemen van maatregelen.

De overheid is echter niet de enige die invloed heeft op het voorkomen van dreigingen of het beperken van de gevolgen ervan. Om risico's te beperken en voorbereid te zijn op rampen en crises is ook een inspanning nodig van het bedrijfsleven, maatschappelijke organisaties en burgers. De Strategie Nationale Veiligheid (mei 2007) biedt een kader voor die gemeenschappelijke inspanning ¹.

1.2 Strategie Nationale Veiligheid

In april 2007 heeft het kabinet de Strategie Nationale Veiligheid vastgesteld. Aanleiding voor de strategie was de constatering dat bedreigingen van onze veiligheid veranderen en steeds meer met elkaar verweven raken. De aanpak moet integraal zijn, samenhang waarborgen en over dreigingen heen kijken. Hierbij blijft de primaire verantwoordelijkheid voor maatregelen bij die partijen die er nu ook al verantwoordelijk voor zijn: het vakministerie, de decentrale overheid, de private sector of de burger.

¹ Tweede Kamer, vergaderjaar 2006-2007, 30 821, nr. 3

Met behulp van de Strategie Nationale Veiligheid wordt een grote diversiteit aan dreigingen langs één meetlat gelegd op basis van de nationale risicobeoordeling. Dreigingsscenario's voor bijvoorbeeld overstromingen, pandemieën en langdurige uitval van nutsvoorzieningen en voor incidenten met een moedwillige oorzaak worden op een eenduidige manier beschreven, onderbouwd met cijfers en geaggregeerd. Deze scenario's zijn verkennend van aard en geven geen voorspelling van de toekomst. Ze zijn een hulpmiddel om de risico's voor de nationale veiligheid vergelijkbaar te maken en een prioritering van maatregelen mogelijk te maken.

Het uiteindelijke doel is het beschermen van de vitale belangen² van Nederland en het voorkomen van maatschappelijke ontwrichting door rijksbrede regievoering. De nationale veiligheid is in het geding als vitale belangen van de Nederlandse staat en samenleving zo geschaad worden dat er maatschappelijke ontwrichting kan optreden. De gehanteerde werkwijze maakt het mogelijk te komen tot identificatie en waar nodig versterking van capaciteiten die ingezet kunnen worden ter vermindering van de waarschijnlijkheid en de impact van dreigingen.

De werkwijze voor de versterking van de nationale veiligheid is een voortdurend proces en bestaat uit de volgende onderdelen (zie figuur 1):



Figuur 1: grafische weergave van de werkwijze Nationale Veiligheid

1) *analyse van dreigingen en beoordeling van risico's*

Om de vitale belangen goed te kunnen beschermen is het van belang continu te beschikken over een scherp beeld van potentiële dreigingen. De werkwijze begint dan ook met het analyseren van de dreigingen die op Nederland af komen. Vervolgens volgt het beoordelen van de dreigingen in termen van risico's (impact en waarschijnlijkheid). Ten slotte worden de verschillende dreigingen ten opzichte van elkaar in beeld gebracht.

2) *strategische planning*

In deze fase wordt bepaald wat Nederland (overheid, burger en bedrijfsleven) moet kunnen om risico's te beperken; wat zij al kan; en wat nog nodig is.

² vitale belangen: territoriale veiligheid, fysieke veiligheid, economische veiligheid, ecologische veiligheid en sociaal politieke stabiliteit
Pagina 6 van 55

3) *opvolging beleid*

Hier worden de politiek-bestuurlijke keuzes uitgewerkt in bijvoorbeeld beleid, wetgeving en concrete maatregelen.

1.3 Bevindingenrapportage NV 2010

In deze derde bevindingenrapportage worden de uitkomsten beschreven van de meest recente NRB-cyclus (2010). De in eerdere cycli ontwikkelde scenario's zijn aangevuld met acht extra scenario's.

In de nu voorliggende derde bevindingenrapportage is het thema "Schaarste" toegevoegd. Daarnaast zijn scenario's toegevoegd aan de al bestaande thema's "ICT-uitval" en "grootschalig ongeval". In de eerste bevindingenrapportage³ waren al risico's op de drie thema's "Klimaatverandering", "Energievoorzieningszekerheid" en "Polarisatie en radicalisering" beoordeeld. In de tweede bevindingenrapportage⁴ zijn naast aanvullende scenario's voor de drie genoemde thema's de nieuwe thema's "Verwevenheid boven- en onderwereld", "ICT-uitval" en "Grootschalig ongeval" toegevoegd.

In deze bevindingenrapportage worden de zes nieuwe scenario's kort geschetst. Zij worden samen met de eerder ontwikkelde scenario's in beeld gebracht in het risicodiagram. Op basis van de nieuwe scenario's zijn vervolgens te versterken capaciteiten in beeld gebracht. Deze zijn deels specifiek van aard (gericht op één scenario/dreigingsthema) en deels breed inzetbaar (toepasbaar bij het reduceren van meerdere dreigingen).

1.4 Leeswijzer

In dit rapport worden de bevindingen van de nationale risicobeoordeling gepresenteerd. Het betreft een beschrijving van de scenario's die input waren voor de NRB en de uitkomsten van de NRB (hoofdstuk 2). In hoofdstuk 3 is een eerste oriëntatie van benodigde capaciteiten uitgewerkt. Dit resulteert in hoofdstuk 4 in een agenderingsadvies voor te versterken (specifieke en breed inzetbare) capaciteiten. In bijlage 1 wordt de gehanteerde methodiek beschreven.

³ Tweede Kamer, vergaderjaar 2007-2008, 30821, nr. 6

⁴ Tweede Kamer, vergaderjaar 2008-2009, 30821, nr. 8

2. Scenario's en uitkomsten nationale risicobeoordeling

2.1 Inleiding

In dit hoofdstuk staan de scenario's centraal die zijn 'doorgerekend' met de nationale risicobeoordeling (NRB). In paragraaf 2.2 wordt toegelicht welke scenario's dit jaar zijn uitgewerkt. In paragraaf 2.3 wordt een kort totaaloverzicht van alle tot nu toe ontwikkelde scenario's gegeven. In paragraaf 2.4 worden de nieuwe scenario's kort samengevat. In paragraaf 2.5 wordt in het risicodiagram een overzicht gegeven van de waarschijnlijkheid en van de impactscores van de 39 scenario's.

2.2 Gekozen scenario's 2010

De scenario's zijn beschrijvingen van incidenten die voorstelbaar en herkenbaar zijn en die zich op de beschreven wijze zouden kunnen ontwikkelen. De gekozen scenario's staan symbool voor een set van gebeurtenissen waar de overheid zich op wil voorbereiden ter bescherming van de vitale belangen⁵. Dit geschiedt in het kader van de Nationale Risicobeoordeling, in de brede range van lage tot hoge waarschijnlijkheid. Door ook scenario's met een lage waarschijnlijkheid op te nemen, ontstaat een integraal beeld van mogelijke dreigingen en te versterken capaciteiten, hetgeen noodzakelijk is voor de afweging om al dan niet te investeren in capaciteiten. Daarnaast kunnen inzichten uit een dergelijk scenario helpen bij beleidsanticipatie voor het geval in de toekomst de waarschijnlijkheid hoger wordt.

Voor de nationale risicobeoordeling 2010 is gekozen voor de nadere uitwerking van acht scenario's als aanvulling op de reeds eerder uitgewerkte scenario's in de twee voorgaande nationale risicobeoordelingen. De scenario's liggen op het terrein van het nieuwe dreigingsthema "Schaarste" en de reeds bestaande thema's "ICT-uitval" en "Grootschalig ongeval".

Schaarste

Er is voor gekozen om twee schaarste-scenario's uit te werken, omdat uit eerdere verkenningen blijkt dat schaarste aan grondstoffen, energie en voedsel één van de grootste uitdagingen voor de wereld dreigt te worden. Huidige mondiale ontwikkelingen, zoals een toenemende bevolking- en welvaartsgroei, veranderende economische machtsverdeling en geopolitieke verhoudingen, maar ook klimaatverandering en biodiversiteitverlies kunnen leiden tot een wereldwijde crisis wegens tekorten in de beschikbaarheid van bijvoorbeeld voedsel, energie en water. Bovendien kan schaarste nieuwe macht geven aan landen die grondstoffen leveren, met mogelijke conflicten tot gevolg. In het licht van deze mondiale ontwikkelingen, alsmede de motie Schuurman die in november 2008 tijdens de Algemene Politieke Beschouwingen door de Eerste Kamer werd aangenomen⁶, is schaarste als thema,

⁵ De scenario's zijn dus geen 'voorspellingen' of 'verwachtingen'

⁶Motie: 4 november 2008, EK 2008-2009 21-700b en antwoord: 23 februari 2009 2009-0000093857

met de scenario's voedselschaarste (sojabonen) en mineraal geopolitiek, in de nationale risicobeoordeling opgenomen.

ICT-uitval (digitale veiligheid)

De digitalisering van de samenleving neemt steeds grotere vormen aan. Dat biedt veel kansen, maar zorgt ook voor nieuwe risico's. Risico's van kleinschalige criminaliteit tot cyberdefence/warfare en verstoring van de nationale veiligheid. Uitval van ICT voorzieningen kan leiden tot aantasting van onze vitale belangen. Te denken valt bijvoorbeeld aan economische schade bij uitval van het betalingsverkeer. Deze steeds dominantere rol van ICT in onze samenleving is aanleiding geweest om digitale veiligheid binnen de strategie Nationale Veiligheid als apart dreigingstype te identificeren. In de voorgaande NRB cycli is al een tweetal scenario's op dit terrein uitgewerkt. In deze cyclus zijn twee scenario's toegevoegd, uitval van de Nederlandse Internet Exchanges en Cyberconflict. Het scenario uitval van de Nederlandse Internet Exchange is gekozen omdat Internet Exchanges volgens velen vitale diensten zijn. Een goed functionerend internet is van groot belang voor de Nederlandse veiligheid en economie. Daarbij komt nog het belang van de transitfunctie die Nederland vervult tussen met name Noord-Amerika en Europa. Daarnaast is gekozen voor het scenario cyberconflict. Er is voor dit scenario gekozen, omdat tot nog de verschillende scenario's op het terrein van digitale veiligheid een geheel civiele insteek hadden. Met het cyberconflict scenario wordt ook het grote belang van de militair-defensieve component binnen een integrale aanpak van digitale veiligheid gedekt.

Grootschalig ongeval

Grootschalige ongevallen kunnen onze vitale belangen aantasten. Te denken valt aan grote aantallen slachtoffers, ontwrichting van vitale infrastructuren of aantasting van de ecologie. In de voorgaande NRB cyclus is voor het thema 'Grootschalig ongeval' een chemisch en een nucleair scenario uitgewerkt. In aanvulling hierop is dit keer gekozen voor het uitwerken van een spoorwegongeval en een maritiem ongeval, waarbij in beide scenario's gevaarlijke stoffen een belangrijke rol spelen.

2.3 Het totaal van scenario's

Met de in drie NRB cycli⁷ geanalyseerde scenario's worden bijna alle dreigingsthema's, die in het kader van de strategie Nationale Veiligheid eerder zijn geïdentificeerd afgedekt. Het thema "Aantasting van de internationale vrede en veiligheid" is nog niet uitgewerkt. Wel is het zo dat veel van de reeds uitgewerkte dreigingen de internationale component in zich hebben en daarmee grensoverschrijdend zijn. De doelstelling om binnen de strategie Nationale Veiligheid een 'all hazard' afweging te kunnen maken ten aanzien van de dreigingen waar de Nederlandse samenleving mee te maken kan krijgen is dus zo goed als gerealiseerd na deze derde analyse. Voor het laatste dreigingsthema: 'Aantasting van de internationale vrede en veiligheid' geldt dat bekeken zal worden hoe dit thema in een volgende cyclus vorm te geven. Daarbij kan worden aangesloten bij één van de

⁷ NRB 2007, NRB 2008-2009, NRB 2009-2010
Pagina 10 van 55

in deze bevindingenrapportage geïdentificeerde breed inzetbare capaciteiten die juist gaat over de relatie tussen de nationale veiligheid en het internationale beleid. De lijst van dreigingsthema's is overigens niet statisch, nieuwe ontwikkelingen kunnen leiden tot aanpassingen. Ook de representativiteit van de set van scenario's is een blijvend punt van aandacht.

Inclusief de 33 reeds ontwikkelde scenario's zijn na afronding van deze NRB-cyclus 39 scenario's ontwikkeld, verdeeld over 7 thema's:

- Klimaatverandering (9 scenario's)
- Energievoorzieningszekerheid (5 scenario's)
- Polarisatie en radicalisering (11 scenario's)
- Verwevenheid onder- en bovenwereld (3 scenario's)
- ICT-uitval (4 scenario's)
- Grootschalig ongeval (5 scenario's)
- Schaarste (2 scenario's)

De scenario's kennen verschillende gradaties van ernst. Het ernstige griep pandemiescenario is een voorbeeld van een scenario met een catastrofale impact en een hoge waarschijnlijkheid. Sommige scenario's (zoals de 'ergst denkbare overstroming') zijn zogenoemde 'worst case scenario's' met een catastrofale impact in combinatie met een lage waarschijnlijkheid. Andere scenario's (zoals het black-out scenario of het rechtsextremisme scenario) zijn minder ernstig wat betreft impact, maar scoren hoger op waarschijnlijkheid.

Het Kabinet heeft uiteraard tevens veel aandacht voor de financieel economische risico's. Op financieel economisch terrein is er de afgelopen periode in Europa veel gebeurd. Het kabinet constateert dat bestaande capaciteiten volstaan voor de lopende crisisbeheersende werkzaamheden in Europees en internationaal kader. Maatregelen strekken van toezicht en early warning, tot versterken van budgettaire en economische regels en de naleving ervan in Europa, tot een omvangrijk noodmechanisme waarop landen die in financiële nood verkeren tegen uitermate strikte voorwaarden een beroep kunnen doen.

Oude scenario's

In de vorige bevindingenrapportages zijn 33 scenario's uitgewerkt, zie onderstaande tabel. De beoordeling van de scenario's wordt (indien nodig) geactualiseerd. Hierbij kunnen recente gebeurtenissen als referentie worden gebruikt. Voor dit jaar geldt dat er geen aanleiding is om de bestaande scenario's aan te passen. Voor de twee griep pandemie scenario's geldt dat de nu lopende evaluatie van de aanpak van de griep pandemie Nieuwe Influenza A (H1N1), zoals die Nederland vorig jaar trof, aanleiding zou kunnen zijn om in de toekomst de beoordeling van deze scenario's aan te passen. De zeven nieuwe scenario's worden in 2.4 kort beschreven.

Klimaatverandering	<ul style="list-style-type: none">○ Scenario westelijke kust (EDO⁸)○ Scenario dijkkring 14 (EDO)○ Extreme droogte-hitte
--------------------	--

⁸ EDO staat voor *Ergst Denkbare Overstromingsscenario's*

	<ul style="list-style-type: none"> o Griep pandemie mild o Griep pandemie ernstig o Zware sneeuwstorm o IJzel o Zeer zware storm o Overstroming Rijn-IJssel
Energievoorzieningszekerheid	<ul style="list-style-type: none"> o Moedwillige verstoring elektriciteit o Oliescenario geopolitiek o Landelijke blackout elektriciteit o Langdurige verstoring elektriciteit o Moedwillige verstoring gaslevering
Polarisatie en radicalisering	<ul style="list-style-type: none"> o Dierenactivisten – vreedzaam massaal protest o Politiek salafisme o Extreemrechts – grootschalige rel op lokaal niveau o Extreemlinks – grootschalige rellen o Extremistische Moslims – ernstige rellen o Enclavevorming o Onrust in probleemwijken o Dierenrechtenextremisme o Massapolarisatie o Confrontaties o Politiek salafisme met geweld
Verwevenheid onder- en bovenwereld	<ul style="list-style-type: none"> o Criminele inmenging in vitale bedrijven o Beïnvloeding aandelenmarkt o Beïnvloeding openbaar bestuur
ICT-uitval	<ul style="list-style-type: none"> o Verstoring IP-netwerk o Moedwillige verstoring ICT van vitale sector
Grootschalig ongeval	<ul style="list-style-type: none"> o Chemisch scenario o Nucleair scenario o Natuurbrandscenario

2.4 Samenvatting nieuwe scenario's

2.4.1 ICT-uitval

Cyberconflict

Nederland wordt getroffen door een grootschalige, gecoördineerde aanval in het digitale domein waarbij een staat betrokken is. De aanvallen op de ICT-infrastructuur beperken het functioneren van overheidsinstanties, delen van de vitale infrastructuur en het bedrijfsleven. De ICT-infrastructuur van diverse ministeries wordt lam gelegd, de stroom in Gelderland en Noord-Holland valt uit, het

telefoonverkeer wordt ernstig beperkt en de verbindingen met satellieten vallen uit (waardoor Defensie maar beperkt kan communiceren met eenheden in het inzetgebied). Ook internationale handel en de financiële sector worden getroffen.

Lang blijft onduidelijk of het om een gecoördineerde aanval gaat en wie daar achter zit, wat het handelingsperspectief voor de overheid beperkt. De respons blijft beperkt tot het zo snel mogelijk herstellen van de gecorrumpeerde systemen en het versterken van de beveiliging van netwerken. De overheid beschikt niet over de capaciteiten om de dreiging het hoofd te bieden en er is geen zicht op doortastend en effectief optreden door de overheid en het bedrijfsleven. Door de aanval verliest de overheid de zeggenschap over delen van de ICT-infrastructuur wat gezien wordt als een schending van het grondgebied. Tevens is er sprake van een aanzienlijke aantasting van de democratische rechtstaat. Hoewel de basis dienstverlening op het terrein van openbare orde en veiligheid niet uitvalt wordt deze wel ernstig gehinderd door de beperkte bereikbaarheid. Het functioneren van grote delen van de Rijksoverheid wordt zeer ernstig gehinderd door grootschalige uitval van ICT-systemen. Ook de Tweede Kamer wordt gehinderd in haar functioneren. De ICT-problemen zijn zeer zichtbaar en een aanzienlijk deel van de bevolking ondervindt daar direct de gevolgen van. Een aantal vitale sectoren wordt geraakt en er is niet direct zicht op herstel. De onzekerheid bij de bevolking is groot en het vertrouwen in de overheid wordt ernstig geschaad.

Hoewel er geen concrete aanwijzingen zijn dat Nederland getroffen zal worden door een grootschalige en gecoördineerde aanval in het digitale domein is het scenario technisch zeker mogelijk en voorstelbaar. Tevens wordt de kwetsbaarheid, ondanks de uitgebreide beveiligingsmaatregelen ter bescherming van netwerken en systemen, als groot aangemerkt.

Uitval Nederlandse internet exchanges

In Nederland bevindt zich een aantal internet exchanges. Een internet exchange is een knooppunt waar de netwerken van Internet Service Providers (ISP's) bij elkaar komen zodat zij internetverkeer kunnen uitwisselen. Aangezien een goed functionerend internet voor de Nederlandse veiligheid en economie van groot belang is en steeds belangrijker wordt, leeft bij velen de gedachte dat IX'en van vitaal belang zijn voor de nationale veiligheid. Eén ervan heeft een zeer belangrijke functie voor het verwerken van het binnenlandse verkeer en als transit voor het buitenlandse verkeer, de Amsterdam Internet Exchange (AMS-IX). Deze specifieke AMS-IX vervult daarnaast een belangrijke transitfunctie tussen met name Noord-Amerika en Europa.

Dit scenario beperkt zich tot deze internet exchange en beschrijft de uitval ervan. Door een softwarefout in de netwerkapparatuur wordt van het ene op het andere moment geen internetverkeer meer over de AMS-IX gerouteerd. De uitval vindt plaats op een doordeweekse dag om 18.00 uur in de vakantieperiode. Het internetverkeer wordt automatisch omgeschakeld naar alternatieve routes. Om 18.30 uur wordt geconstateerd dat de software niet goed functioneert. Door installatie van een vorige versie van de software, wordt om 20.00 uur de escalatie

opgeheven. Uitval van een Nederlandse IX heeft in dit scenario zeer beperkte gevolgen. De uitval van AMS-IX wordt opgevangen door de vele alternatieve routes; aangezien de andere exchanges in Nederland een zeer kleine rol vervullen in het routeren van internetverkeer is de impact van uitval van een dergelijke exchange miniem.

2.4.2 *Grootschalig ongeval*

Spoorwegongeval

Op een druk spoor vindt tijdens de spits een aanrijding plaats tussen een passagierstrein en een ontspoorde goederentrein. Er valt een groot aantal doden en gewonden door de aanrijding. Een van de LPG-tankwagons van de goederentrein ontploft na verhitting door brandende benzine uit een lekkende benzinetankwagon. Hierdoor vallen nog meer slachtoffers, omdat veel mensen niet tijdig uit de passagierstrein gered konden worden. Het getroffen viaduct is door de scharende goederentrein uit zijn verband geduwd. De infrastructuur en de bovenleiding is over een grote afstand vernield. Na het incident duurt het weken tot maanden voordat het spoor en het getroffen viaduct van de nabijgelegen snelweg hersteld zijn.

Maritiemongeval

In de Eurogeul bij de haven van Rotterdam heeft een containerschip een aanvaring met een bulkcarrier. De bulkcarrier kan op zee gerepareerd worden. Na inspectie en stabiliteitsberekeningen besluit de havenmeester dat het containerschip de haven in gesleept mag worden om daar gerepareerd te worden. Tijdens het slepen wordt duidelijk dat de stabiliteitsberekeningen niet kloppen. Het schip maakt slagzij en komt schuin in de Maasmond te liggen. Eén of meerdere containers met gevaarlijke stoffen zijn hierbij tussen het schip en de pier terecht gekomen en gescheurd. Door het kortstondig vrijkomen van gif en paniek tijdens het vluchten valt een groot aantal doden en gewonden. Door het ongeval zal gedurende enkele dagen slechts beperkt scheepvaartverkeer mogelijk zijn van zee naar de haven en vice versa.

2.4.3 *Scenario's Schaarste*

Voedselschaarste (sojabonen)

Een substantieel deel van de sojabonen-import valt weg als gevolg van de ontwikkeling van massaal geproduceerde (nog) niet door Europa geaccepteerde genetische gemodificeerde soorten én een slechte oogst in de niet-gemodificeerde soja in Zuid-Amerika vanwege een enorme uitbraak van roest (plantenziekte). Als reactie daarop geeft China een subsidie op de import van soja om de eigen voedselzekerheid veilig te stellen. De daling van de import van sojabonen dwingt Nederland tot ingrijpende aanpassingen, zoals een verminderde vleesproductie, sterk stijgende veevoederprijzen en daarmee hogere vleesprijzen, werkeloosheid in de voedselproductieketen, verminderde vleesconsumptie en een gewijzigd consumptiepatroon. Desalniettemin blijven de noodzakelijke voedsel ingrediënten voor de Nederlandse bevolking beschikbaar. Wel leidt de wereldwijde onzekerheid

over het verdere verloop van de vlees- en voedselprijzen tot verhitte discussies in de media over de toekomstige houdbaarheid van het huidige niveau van vleesconsumptie. Daarnaast zullen verstoringen in de voedselprijzen leiden tot zeer ernstige sociaal-politieke beroering in landen buiten Europa. Via een dergelijke destabilisatie zou voedselschaarste een aanzienlijk indirect effect kunnen hebben op de Nederlandse nationale veiligheid.

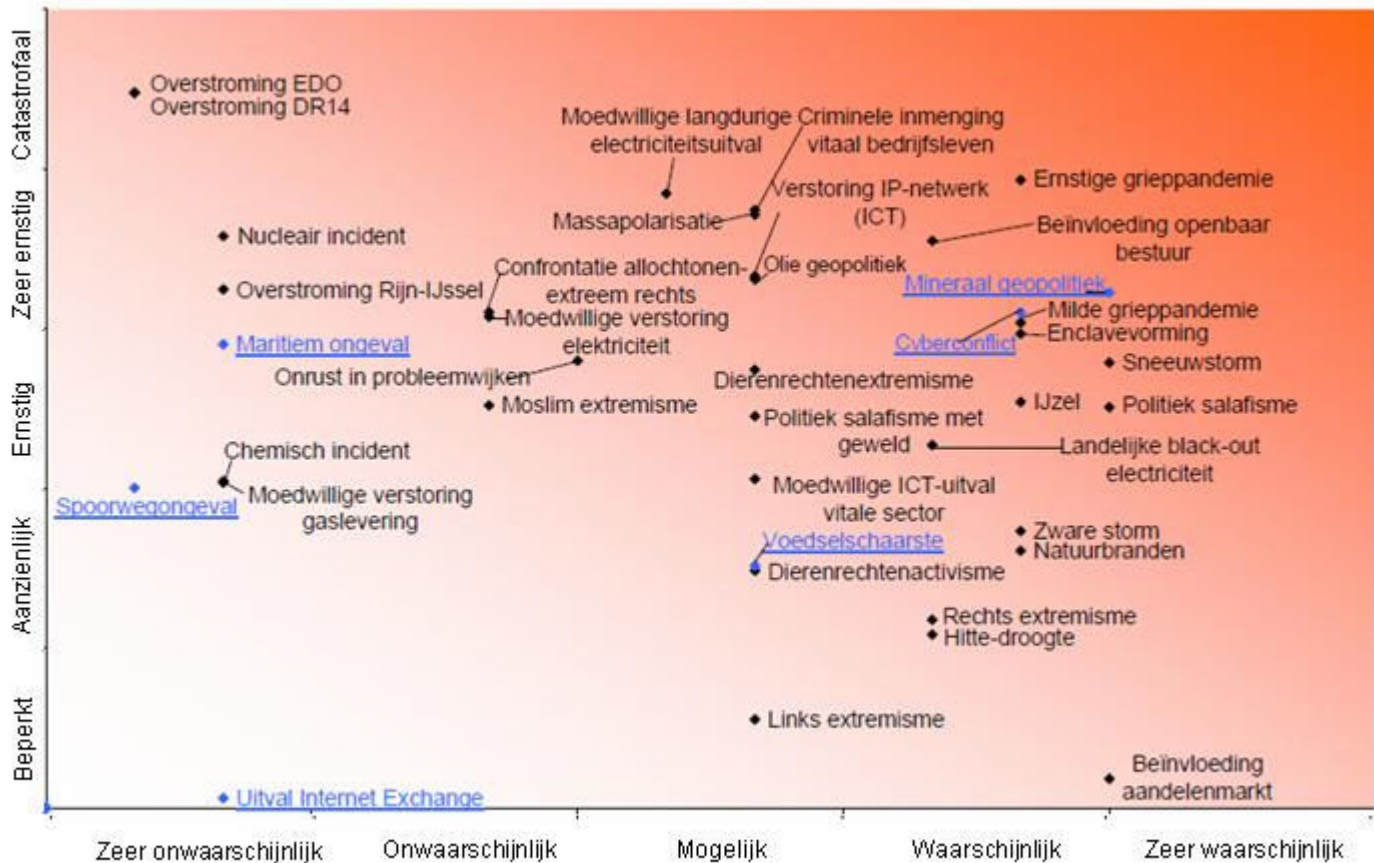
Mineraal geopolitiek

De vraag naar mineralen is exponentieel gestegen vanwege wereldwijde economische groei. Plotseling is er een verstoring in de aanvoer van enkele belangrijke mineralen die onder andere gebruikt worden in de technologieën die nodig zijn om te komen tot een duurzame energievoorziening. Het begint met de implementatie van handelsrestricties door een zeer belangrijke producent van schaarse mineralen met enorme prijsstijgingen tot gevolg. Deze prijsstijgingen worden hard gevoeld in bepaalde onderdelen van de Nederlandse en Europese industrie. Er wordt een geschillenbeslechtingsprocedure bij de Wereldhandelsorganisatie in gang gezet, maar het duurt te lang voordat er een uitspraak wordt gedaan. De gevolgen van een dergelijk scenario raken met name de concurrentiekracht van de Nederlandse en Europese industrie.

2.5 Uitkomsten nationale risicobeoordeling

De NRB levert een uitkomst voor zowel de impact als de waarschijnlijkheid. Deze uitkomst is grafisch weergegeven in het risicodiagram (figuur 2).

Risicodiagram



EDO = ergst denkbare overstroming; DR14 = dijkkring 14

Figuur 2: Het risicodiagram

2.5.1 Leeswijzer risicodiagram

Op de verticale as is de impact uitgezet. De maximale waarde van de as komt overeen met een (fictief) scenario dat op de tien NRB-impactcriteria⁹ de maximale score (catastrofaal) oplevert (100%). De indeling van de verticale as in categorieën is logaritmisch van aard en zo gekozen dat iedere volgende categorie een drie keer hogere impact aangeeft dan de vorige.

⁹ zie bijlage 1..3 van de bevindingenrapportage nationale veiligheid 2010 voor een beschrijving van de impactcriteria
Pagina 16 van 55

Op de horizontale as is de waarschijnlijkheid van het scenario weergegeven. De indeling van deze as is zo dat iedere volgende categorie een tien keer hogere waarschijnlijkheid aangeeft dan de vorige categorie.

Het kleurverloop in het diagram geeft aan dat scenario's van de linker benedenhoek naar rechts en naar boven steeds ernstiger worden (in impact en in waarschijnlijkheid). Scenario's die in 2010 zijn ontwikkeld zijn onderstreept weergegeven. De scenario's kunnen globaal in vier kwadranten van zwaarte of ernst worden ingedeeld (voor een meer uitgebreide leeswijzer, zie bijlage 2).

2.5.2 *De plaats van de nieuwe scenario's in het risicodiagram*

Het nieuw ontwikkelde scenario *Mineraal geopolitiek* valt op basis van de analyse van de beperkte informatie die nu beschikbaar is bij de betrokken experts binnen het gebied met een hoge waarschijnlijkheid en een hoge impact. Achtergrond hiervan is ondermeer dat vanwege geopolitieke ontwikkelingen schaarste zou kunnen ontstaan, zie bijvoorbeeld het afsluiten van gastransporten door Rusland. Van belang is te vermelden dat er maar beperkte informatie over dit onderwerp en de potentiële implicaties voor Nederland aanwezig is, zeker wat betreft de te voorziene economische effecten. In deze bevindingenrapportage wordt dan ook onder andere geadviseerd om de komende jaren meer inzicht te gaan vergaren over dit onderwerp. Hierbij gaat het om zaken als 'van welke mineralen zijn we afhankelijk', 'hoe groot is die afhankelijkheid en welke partijen zijn afhankelijk'. Ook zou deze afhankelijkheidsvraag meer in het perspectief van geopolitieke machtsverhoudingen geplaatst moeten worden. Dit kan mogelijk leiden tot een verschuiving van het scenario in het risicodiagram.

Het andere schaarstescenario (voedselschaarste (sojabonen)) scoort lager qua impact, maar kent ook een hoge waarschijnlijkheid. Het valt daarmee in het kwadrant 'hoge waarschijnlijkheid en (relatief) lage impact.

Het scenario *cyberconflict* scoort hoog op impact en waarschijnlijkheid. Het scenario is voorstelbaar (waarschijnlijkheidsklasse C) omdat alle activiteiten beschreven in het scenario technisch kunnen worden uitgevoerd. De kwetsbaarheid is hoog omdat het waarschijnlijk is dat de verdediging tegen de aanval tekort zal schieten. Het is op dit moment namelijk nagenoeg onmogelijk om snel vast te stellen waar een aanval vandaan komt en wie daar achter zit. Doordat de kwetsbaarheid hoog is, wordt het scenario volgens de gehanteerde methode waarschijnlijk geacht (waarschijnlijkheidsklasse D).

Uit het risicodiagram blijkt dat vier van de nieuwe scenario's in het gebied vallen met een lage waarschijnlijkheid en/of een beperkte impact. Dit zijn de scenario's *maritiemongeval*, *spoorwegongeval* en *uitval van één Internet Exchange*.

2.5.3 *Overzicht impactscores van de scenario's*

In de acht nieuw ontwikkelde scenario's is in bijna alle gevallen sprake van een grote sociaal-psychologische impact. Verder valt op dat het scenario '*mineraal geopolitiek*' ook een grote verstoring van het dagelijks leven met zich meebrengt terwijl schaarste aan sojabonen voor alle impactcriteria relatief beperkte gevolgen

heeft. Tot slot blijkt dat het scenario 'uitval van één Internet Exchange' alleen (beperkt) scoort op het criterium kosten.

In bijlage 3 zijn de impactscores van de nieuw ontwikkelde en de 33 eerder uitgewerkte scenario's opgenomen. Dit inzicht biedt aanknopingspunten voor de versterking van capaciteiten.

Impactscores van alle scenario's

Bij de meeste (oude en nieuwe) scenario's wordt de impactscore voor een belangrijk deel bepaald door hoge scores op slechts een beperkt aantal criteria. Zo is de impact bij de energiescenario's voornamelijk bepaald door verstoring van het dagelijkse leven en scoren scenario's op het gebied van polarisatie en radicalisering hoog op sociaal-psychologische impact en aantasting van de democratie.

De drie meest dominante impactcriteria in de 39 ontwikkelde scenario's zijn sociaal-psychologische impact, verstoring van het dagelijkse leven en kosten. De aantasting van de rechtstaat scoort hoog bij scenario's over verwevenheid, polarisatie en radicalisering, energievoorzieningszekerheid en ICT-uitval. Bij de laatste twee thema's heeft dat te maken met het gegeven dat de scenario's gepaard gaan met moedwillige aanslagen.

In bijlage 4 is een tabel opgenomen met een overzicht van de waarschijnlijkheid en de verschillende impactscores van de 39 scenario's.

Bij de uiteindelijke agendering van te versterken capaciteiten is het met name van belang om in te zetten op capaciteiten waarmee de impact op bovengenoemde criteria verminderd kan worden. Op deze wijze kan de totale impact van meerdere dreigingen beperkt worden. In hoofdstuk 3 en 4 wordt de oriëntatie op capaciteiten en de aanbevelingen beschreven.

3. Oriëntatie op capaciteiten

3.1 Inleiding

Dit hoofdstuk is een eerste oriëntatie op capaciteiten. In paragraaf 3.2. tot en met 3.5 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. Waar nodig wordt binnen een thema onderscheid gemaakt naar verschillende scenario's. In paragraaf 3.6 wordt het hoofdstuk afgesloten met een conclusie. In hoofdstuk vier wordt vervolgens op basis van verschillende criteria, bijvoorbeeld 'kosten-baten', een voorstel gedaan voor agendering van de meest kansrijke te versterken capaciteiten.

3.2 ICT-uitval

Cyberconflict

Conflicten in cyberspace zijn niet nieuw. Al sinds eind jaren negentig van de vorige eeuw leiden interne en interstatelijke conflicten ook in het digitale domein tot versturende activiteiten. Eerst betrof dit nog samenspannende hackers en cyber-activisten. Voorbeelden zijn de wederzijdse hackeraanvallen tussen India en Pakistan na kernproeven in 1998 en internationale protestacties tegen de Mexicaanse overheid, het Pentagon en de beurs van Frankfurt met door het Electronic Disturbance Theater beschikbaar gestelde denial-of-service programmatuurⁱ. Inmiddels zijn tijdens interstatelijke conflicten ook gecoördineerde cyber en fysieke aanvallen door overheden of aan overheden gelieerde actoren geconstateerd. Voorbeelden zijn de cyberaanvallen op Estland (april-mei 2007)ⁱⁱ, Georgië (augustus 2008)ⁱⁱⁱ en Kirgizië (februari 2009)^{iv}. Een recent voorbeeld in Nederland is dat Siemens bij veertien fabrieken de Stuxnet worm heeft aangetroffen. Aangezien veel aspecten van deze soort dreiging niet publiek bekend zijn, is men in het algemeen in eerste instantie sceptisch. Echter, experts vermoeden dat dergelijke dreigingen veel vaker en in meer ernstige vormen zullen gaan voorkomen. Het Verenigd Koninkrijk heeft in de Nationale Veiligheidsstrategie weergegeven dat ICT dreigingen als een van de grootste dreigingen worden aangemerkt.

Ten aanzien van het scenario cyberconflict zijn er drie impactcriteria die in het bijzonder bijdragen aan de beschreven ontwrichting van Nederland: sociaal psychologische impact, verstoring dagelijks leven en lichamelijk lijden (door de gevolgen van langdurig stroomuitval in 2 provincies).

Te versterken capaciteiten

Momenteel is het Nederlandse beleid ten aanzien van het vraagstuk cyberveiligheid in ontwikkeling. Op dit moment wordt in nauwe samenwerking met private partijen aan een Nationale Cyber Security Strategie en een bijbehorend actieplan gewerkt.

Uit de capaciteitanalyse komt een aantal zaken naar voren dat in ieder geval zou moeten worden opgepakt.

1. Eenduidige regie op het cyberveiligheidsvraagstuk
2. Integratie nationale cyberveiligheidsbelangen in internationaal beleid
3. Informatiewinning, -analyse en -deling
4. Nationale en flexibele inzet cybersecurity kennis
5. Nationaal beleidskader defensieve capaciteiten

Eenduidige regie op het cyberveiligheidsvraagstuk

Het functioneren van vitale infrastructuren, de overheid en het bedrijfsleven is afhankelijk van netwerken en systemen die steeds vaker aan elkaar verbonden zijn. Initiatieven ter versterking van de digitale veiligheid worden veelal voor een specifiek onderwerp of (vitale) sector opgestart. Meer aandacht voor de meerwaarde en effectiviteit van een brede gezamenlijke aanpak is van belang. Wil de overheid daadkrachtig kunnen optreden bij een cyberconflict en bij het voorkomen daarvan, dan zal inzichtelijk moeten worden gemaakt welke partijen (al dan niet met een wettelijke taak) welke rol en taak moeten vervullen en welke capaciteit deze moeten inrichten om een effectieve nationale aanpak mogelijk te maken.

Integratie nationale cyberveiligheidsbelangen in internationaal beleid

Informatiesystemen en netwerken in Nederland zijn op veel verschillende manieren verbonden met elkaar en met wereldwijde informatie-infrastructuren, bijvoorbeeld via glasvezel-, internet-, telefonie- en satellietverbindingen. Veel ICT-apparatuur en programmatuur wordt buiten Nederland ontwikkeld en geproduceerd. De nationale veiligheid in het cyberdomein is daarom mede afhankelijk van ontwikkelingen en beschermingscapaciteiten in het buitenland. Omgekeerd is het buitenland qua cyberveiligheid afhankelijk van de in Nederland getroffen maatregelen ter voorkoming van- of voorbereiding en respons op het cyberrisico. Op dit moment wordt het internationale cyberveiligheidsbeleid veelal vanuit afzonderlijke departementen gevoed. De integratie van nationale veiligheidsbelangen in het cyberdomein in internationaal beleid vereist een nationaal gecoördineerde internationale agendering en sturing. Voorbeelden van internationale cyberthema's zijn: de verhouding van cyberconflicten tot het NAVO-verdrag (is bij een cyberaanval sprake van een oorlog?) of de ontwikkeling van EU-beleid voor software productaansprakelijkheid.

Informatiewinning, -analyse en -deling

Een cyberdreiging of -aanval kan zich razendsnel ontwikkelen. Cyberdreigingen kunnen zich echter ook sluimerend en daarmee mogelijk onzichtbaar ontwikkelen. In beide gevallen is het van groot belang om in een zo vroeg mogelijk stadium zicht te krijgen op mogelijke cyberdreigingen en -ontwikkelingen en om interferenties tussen dreigingen bij een veelheid aan publieke en private partijen in beeld te brengen. Er is dan ook bij zowel publieke als private partijen behoefte aan een actueel gedeeld situationeel inzicht over de nationale cyberveiligheidsstatus.

Nationale en flexibele inzet cybersecurity kennis

Geconstateerd is dat de huidige cyberveiligheidscapaciteiten van de overheid enerzijds schaars zijn en anderzijds sterk verdeeld zijn over departementen en operationale diensten. Voor het daadwerkelijk pareren van een cyber aanval gedurende dagen tot weken heeft de nationale overheid en haar diensten te weinig beschikbare specialistische kennis en capaciteit. Dit kan worden verbeterd door flexibilisering van inzet en poolvorming van specialisten uit zowel de publieke als de private sector. Daarnaast kan versterking van de capaciteit van een aantal diensten op het cyberveiligheidsgebied helpen.

Nationaal beleidskader defensieve cybercapaciteiten

Mede naar aanleiding van de Motie Knops ontwikkelt Defensie op dit moment beleid op het terrein van defensieve cybercapaciteiten. Echter, om aanvallen te kunnen voorkomen en af te schrikken is samenwerking met meerdere partijen nodig. Het is dan ook van belang om een nationaal beleidskader defensieve capaciteiten cyberveiligheid te ontwikkelen, dat nauw aansluit bij de te ontwikkelen nationale cybersecuritystrategie en waarin ook de rol en betrokkenheid van andere publieke en private partijen wordt beschreven.

Huidig beleid

In 2002 werd door de EU het Europe Action plan gepresenteerd met de ICT ambities voor Europa. Europa moet hierin een wereldwijd leidende rol spelen op het gebied van ICT en dienstverlening. ICT veiligheid kreeg echter pas later meer aandacht. In 2006 nam de Europese Commissie de Communicatie *'Dialogue, partnership and empowerment'* aan: *'A Strategy for a Secure Information Society'* die in het teken stond van veiligheid. De focus hierbij is echter op algemene kwetsbaarheden en minder op bewuste ondermijning of het misbruik van ICT. De Commissie oordeelde dat te weinig partijen zich iets gelegen voelden bij de uitvoering van deze strategie. In maart 2009 werd derhalve in de Communicatie *'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'* verdere nadruk gegeven aan de noodzaak tot een meer geharmoniseerde Europese aanpak, de ontwikkeling van monitoring mechanismes en informatie-uitwisseling tussen lidstaten en een betere publiek-private samenwerking. In de context van de Europese Veiligheidsstrategie wordt de aandacht op cyber security ook vergroot. In een document van huidig EU-voorzitter Spanje, samen met de komende voorzitters België en Hongarije wordt cybercrime een van de vijf dreigingen voor de interne veiligheid van Europa genoemd.

Binnen de NAVO zijn diverse organen opgericht om de weerbaarheid in het digitale domein te vergroten. Zo zijn er diverse organen opgericht om hier inhoud aan te geven (de *Cyber Defence Management Authority*, het *Cooperative Cyber Defence Centre of Excellence*, en een *Computer Incident Response Capability*). Er bestaan echter nog aanzienlijke gaten in de cyberdefensie capaciteiten. Deze capaciteiten moeten zich aan de ene kant richten op het verhogen van het training- en kennisniveau, verbeteren van het monitoren van NAVO-netwerken en, op termijn, het ontwikkelen van passieve en actieve defensiecapaciteiten.

Op dit moment wordt door de ministeries van Economische Zaken, Landbouw en Innovatie, Defensie en Veiligheid en Justitie gewerkt aan een Nationale Cyber Security Strategie en bijbehorend actieplan. De uitkomsten van de capaciteitanalyse kunnen worden opgenomen in het actieplan. Andere activiteiten die moeten bijdragen aan de strategie zijn onder andere: de oefening cyberstorm en de defensie visie cybersecurity.

Sinds 2007 heeft de Rijksoverheid een agenda ICT en Veiligheid waaraan de ministeries van Economische Zaken, Landbouw en Innovatie, Veiligheid en Justitie en Binnenlandse Zaken en Koninkrijkrelaties samen werken. De agenda gaat onder andere over grootschalige ICT verstoringen en strafrechtelijke vervolging van cyber criminaliteit.

Ook is naar aanleiding van uitgewerkte scenario's digitale veiligheid in eerdere bevindingenrapportages het vergroten van de weerbaarheid van de vitale sectoren en de burger tegen verstoringen in ICT geagendeerd. In dit kader wordt onder andere ingezet op continuïteitsplanning bij uitval van ICT binnen de vitale sectoren Openbaar Bestuur en Openbare Orde en Veiligheid.

Tevens wordt samengewerkt aan maatregelen om de respons op ICT verstoringen te verbeteren. In dit kader wordt op dit moment een publiek privaat ICT Response Board ingericht. Het doel van dit Response Board is 1) een snel beeld van de situatie kunnen geven dat vervolgens gedeeld wordt met de relevante private en publieke partijen en 2) een advies te genereren aan de reguliere interdepartementale crisisorganisatie en andere betrokken partijen over te nemen maatregelen. Daarnaast komt er een nationaal crisisplan (NCP) voor uitval van ICT. Dit plan zal ingaan op de hoofdlijnen van de organisatie, taken, verantwoordelijkheden en bevoegdheden van crisisbeheersing op nationaal niveau.

Conclusie

De mogelijkheid dat Nederland onverhoopt verwickeld raakt in een Cyberconflict is niet uit te sluiten. Een aantal maatregelen is noodzakelijk om de nationale cyberveiligheidscapaciteiten te versterken. De belangrijkste maatregelen zijn:

- Eenduidige regie op het cyberveiligheidsvraagstuk
- Integratie nationale cyberveiligheidsbelangen in internationaal beleid
- Informatiewinning, -analyse en -deling
- Nationale en flexibele inzet cybersecurity kennis
- Nationaal beleidskader defensieve capaciteiten op het terrein van cyberveiligheid

'Uitval Nederlandse Internet Exchanges'

In het uitgewerkte scenario heeft uitval van alleen Nederlandse Internet Exchanges door allerlei 'fall back opties' nauwelijks gevolgen voor de Nationale Veiligheid. In een scenario waarbij tevens meerdere grote buitenlandse internet exchanges uitvallen is het denkbaar dat er wel grotere gevolgen zijn.

Te versterken capaciteiten

Uit de scenarioanalyse komt naar voren dat op dit moment onvoldoende duidelijk is welke afspraken er bestaan tussen verschillende Internet Exchanges waar het gaat om het overnemen van elkaars dataverkeer bij uitval. Het is dan ook nodig om duidelijkheid te krijgen over wat hieromtrent is afgesproken tussen de verschillende Internet Exchanges in de ons omringende landen. T.b.v. het publieke belang is het van belang om te weten onder welke omstandigheden er problemen kunnen ontstaan met de doorstroom van het dataverkeer. Het is aan te bevelen deze inzichtelijk te maken. Afstemming met andere nationale overheden is hierbij noodzakelijk, omdat er een mogelijke afhankelijkheid kan bestaan tussen de Europese Internet Exchanges.

De vraag of verstoring van het internetverkeer van een Internet Service Provider (ISP) door uitval van een Internet Exchange gevolgen heeft voor de nationale veiligheid kan worden beantwoord als duidelijk is of de ISP diensten levert aan een vitale organisatie. Aanbevolen wordt dat vitale organisaties die diensten afnemen bij een ISP er voor zorgen dat hun dataverkeer via meer dan één Internet Exchange-platform kan routeren. Een mogelijkheid is dat zij in hun service level agreement (SLA) met de ISP voorwaarden daaromtrent opnemen. Een aantal grotere vitale klanten heeft zelf een telecommunicatienetwerk in eigen beheer (of bezit). Het is aan te bevelen dat zij via meer dan één Internet Exchange-platform kunnen routeren.

Het is aan te bevelen om de Internet Exchange Functie en de daarbij behorende organisaties aan te laten sluiten bij de verdere uitwerking van de *ICT Respons Board*, een van de maatregelen om de respons op grootschalige verstoring van ICT te verbeteren, zoals aangekondigd in de derde voortgangsbrief Nationale Veiligheid¹⁰.

Huidig beleid

Zie beschrijving ' huidig beleid ' bij het scenario ' cyberconflict '.

Conclusie

Bij de afbakening van het scenario is gekozen voor het uitvallen van één Nederlandse Internet Exchange, AMS-IX, welke het grootste deel van het internetverkeer verwerkt. Of bij uitval van deze exchange de resterende buitenlandse Internet Exchanges de extra toevloed aan kunnen, is op dit moment niet bekend en zal nader worden onderzocht.

Terugkijkend blijkt gelijktijdige uitval van meerdere Internet Exchanges in Europa een te onderzoeken scenario. De kans is groot dat bij een softwarematig probleem de Internet Exchanges, ook in andere Europese landen, die gebruik maken van dezelfde apparatuur en software een vergrote kans op uitval hebben.

Ingezet zou moeten worden op:

¹⁰ TK 2009-2010, 30821, nr. 10

- Het inzichtelijk maken onder welke omstandigheden problemen kunnen ontstaan met de doorstroom van het dataverkeer
- Het onder de aandacht brengen bij vitale organisaties dat ze voor het door hen zelf als vitaal benoemd internetverkeer de daarvoor in te kopen diensten bij een ISP via een passend service level agreement (SLA) afstemmen. Daarmee kan bijvoorbeeld worden voorkomen dat men afhankelijk zou zijn van één Internet Exchange.
- Aansluiting van de Internet Exchange-functie en de daarbij behorende organisaties bij de verdere uitwerking van de *ICT Response Board*.

3.3 Grootschalig ongeval

Spoorwegongeval

In het spoorwegongeval scenario vallen veel doden en gewonden. Het ongeval heeft een grote sociaal-psychologische impact op de maatschappij.

Te versterken capaciteiten

De fysieke spooromgeving is vanuit veiligheidsoverwegingen afgeschermd van de openbare ruimte. Ook geluidswerende maatregelen zorgen voor een afscherming van de spooromgeving. De afweging tussen deze veiligheidsmaatregelen en de benodigde bereikbaarheid voor hulpverleners na een ongeval dient een continu punt van aandacht te zijn bij de fysieke vormgeving van de spooromgeving. Daarnaast moet in die afweging naast de bereikbaarheid ook de beschikbaarheid van bv. bluswater gezien worden en de mogelijkheid om het spoor snel(ler) veilig te stellen in verband met de bovenleiding, al dan niet door het ongeval beschadigd.

Na een ongeval is er communicatie nodig tussen hulpverleners, NS en andere professionals. Doordat deze kolommen niet dagelijks met elkaar samenwerken kan kostbare tijd verloren gaan.

Crisiscommunicatie geldt ook in dit scenario als voorwaardelijk instrument om de gevolgen in te perken. Door de vele verschillende actoren is aandacht nodig voor een eensluidende en snelle communicatieboodschap.

Huidig beleid

Uit de evaluatie van de Tweede Kadernota Railveiligheid komt onder meer naar voren dat de calamiteitenorganisatie en crisisbeheersing in de afgelopen periode zijn verbeterd. Door de spoorsector is een adequate calamiteitenorganisatie opgezet. Een aantal veiligheidsregio's werkt nog aan de uitwerking van de rampenbestrijding door de hulpverleners in hun regio. De in juni 2010 door de toenmalige minister van Verkeer en Waterstaat aan de Tweede Kamer gezonden Derde Kadernota Railveiligheid¹¹ noemt als voorgenomen activiteiten:

1. Uitwerken en implementeren van de rampenbestrijding in alle veiligheidsregio's

¹¹ Tweede Kamer, vergaderjaar 2009 – 2010, 29 893, nr. 106
Pagina 24 van 55

2. Uitbouwen van de opgedane kennis met betrekking tot de crisisbeheersing bij de Betuweroute en HSL-Zuid binnen het recent opgerichte Platform Transportveiligheid.
3. Opstellen en uitvoeren van een sectorbreed implementatieplan gericht op het vergroten van de zelfredzaamheid van de reiziger bij calamiteiten.

Momenteel wordt het gehele Nederlandse spoorwegnet voorzien van hot-box-detectie apparatuur, waardoor circa 85% van de treinen regelmatig zal worden gecontroleerd op warmlopende assen.

Het Kabinet heeft de Tweede Kamer periodiek geïnformeerd over de maatregelen die het in het kader van de zo genaamde Ketenstudies¹² en Basisnet¹³ wil nemen en heeft genomen en zal dat blijven doen.

De samenwerking tussen hulpverleningsdiensten boven regionaal en met veiligheidspartners buiten de openbare orde en veiligheidskolom (publiek en privaat) is een belangrijk aandachtspunt waarvoor verschillende activiteiten in gang zijn gezet. Zo wordt op initiatief van het veiligheidsberaad de samenwerking tussen veiligheidsregio's en vitale sectoren versterkt, dit door middel van het maken van (model)convenanten die ook ingaan op het versterken van de gezamenlijke geoefendheid. In vervolg op dit traject wordt ook gekeken hoe de samenwerking tussen spoorpartijen (o.a. proram) en veiligheidsregio's verder versterkt kan worden.

Maritiemongeval

In het scenario maritiem ongeval is sprake van veel doden en gewonden, hoge kosten en een grote sociaal psychologische impact op de maatschappij.

Te versterken capaciteiten

Samenwerking is bij een groot ongeval zoals in het scenario beschreven van essentieel belang. Er zijn veel partijen met verschillende verantwoordelijkheden betrokken. Ook partijen die normaal niet met elkaar samenwerken en ook niet beschikken over standaard informatie-uitwisseling moeten in deze situatie, afwijkend van een normale situatie, snel informatie en kennis delen en besluiten op elkaar afstemmen. Het informatieproces moet als structureel onderliggend proces vorm gegeven worden. Op basis van deze informatie kan kennis en besluitvorming bij elkaar gebracht worden. In dit specifieke scenario is met name ten aanzien van het havenbedrijf en de veiligheidsregio geconstateerd dat nadere samenwerking noodzakelijk is.

Crisiscommunicatie geldt ook in dit scenario als voorwaardelijk instrument om de gevolgen in te perken. Doordat er vele verschillende actoren betrokken zijn is aandacht nodig voor een eensluidende en snelle communicatieboodschap.

¹² <http://www.rijksoverheid.nl/documenten-enpublicaties/rapporten/2010/09/30/ketenstudies-chloor-ammoniak-en-lpg.html>

¹³ <http://www.rijksoverheid.nl/onderwerpen/vervoer-gevaarlijke-stoffen/basisnet-vervoer-gevaarlijke-stoffen>

Tijdens een ongeval met gevaarlijke stoffen zijn hulpverleners van verschillende disciplines actief in het gebied. De gevaarniveaus in de omgeving variëren en maken persoonlijke beschermingsmaatregelen voor de verschillende hulpverleners noodzakelijk. Bij het ontbreken van deze middelen voor een bepaalde groep hulpverleners kunnen zij hun taak niet uitvoeren in dit gebied. Gevaarniveaus, taken en persoonlijke beschermingsmiddelen voor de verschillende hulpverleners moeten op elkaar afgestemd zijn. In dit specifieke scenario is geconstateerd dat door het ontbreken van persoonlijke beschermingsmiddelen met name de inzet van de medische hulpverleners is vertraagd.

Huidig beleid

Door de groei van de wereldhandel neme de goederenstromen toe en worden ze ingewikkelder. Het wereldwijde containervervoer groeit explosief. De Noordzee is één van drukst bevaren zeeën ter wereld met zeer intensief zeevaartverkeer voor de kust en bij de zeehavens. Het opvangen van de groei vraagt investeringen niet alleen in infrastructuur en logistiek maar ook in de vorm van veiligheidsbeleid. De veiligheid op de Noordzee is immers continu onderwerp van politieke, bestuurlijke en maatschappelijke zorg.

Ten aanzien van de capaciteiten voor informatiemanagement- en communicatiesystemen wordt scheepvaartwetgeving gemonitord en aangepast waar het gaat om veiligheidsmaatregelen die te maken hebben met verkeersbegeleiding, routing, beloodsing, informatieverlening etc.

Mede gezien de toenemende grootte van zeeschepen richt het beleid zich vooral op het terugdringen van het risico van het optreden van ongevallen. Goed werkende, internationaal geldende veiligheidsregels en adequaat toezicht zijn belangrijke instrumenten voor de veiligheid op zee. Via de IMO (Internationale Maritieme Organisatie) en de EU wordt doorlopend gewerkt aan de verbetering van het stelsel van regelgeving, waarbij deze wordt aangepast aan nieuwe ontwikkelingen.

Belangrijke activiteiten van het ministerie van Infrastructuur en Milieu zijn:

- implementatie in nationale wetgeving van het STCW-Verdrag (Standards of Training Certification and Watchkeeping) voor het veilig bemannen van schepen
- de herziening van de EU-Richtlijn inzake minimumopleidingseisen van zeevarenden
- De ontwikkeling in IMO-verband van stabiliteitscriteria voor zeeschepen
- internationaal onderzoek voor aanpassing van de berekening van de tonnage van schepen
- project Lashing Sea over het bevestigen van containers aan boord van schepen
- subsidiëring van de Koninklijke Nederlandse Redding Maatschappij (KNRM)
- aanpassing Scheepvaartverkeerswet om een mix van veiligheidsmaatregelen in havengebieden te kunnen nemen

Door de toename van het verkeer op de binnenwateren (snellere en grotere schepen, meer recreatievaart en schepen met gevaarlijke stoffen) neemt de druk op

de veiligheid op het water verder toe. De belangrijke instrumenten om dit aan te pakken zijn:

- binnen de EU harmoniseren van voorschriften op het gebied van bemanning, examens, constructie en uitrusting van schepen en het vervoer van gevaarlijke stoffen
- verkeersmanagement: invoeren van River Information Services waarbij inbegrepen het uitrusten van schepen met automatic Identification System (AIS) transponders.

In geval van een groot maritiem ongeval zoals beschreven in het scenario kan het BeleidsOndersteunend Team-milieuincidenten (BOTMI) vanuit verschillende disciplines/expertisevelden, waaronder het RIVM, de Waterdienst van Rijkswaterstaat, het KNMI en DCMR milieudienst Rotterdam, advies aan het veld bij grote en kleinere calamiteiten verlenen.

De samenwerking tussen hulpverleningsdiensten boven regionaal en met veiligheidspartners buiten de OOV kolom (publiek en privaat) is een belangrijk aandachtspunt waarvoor verschillende activiteiten in gang zijn gezet. Zo wordt op initiatief van het veiligheidsberaad de samenwerking tussen veiligheidsregio's en vitale sectoren versterkt. En wordt ten behoeve van onder meer de boven regionale samenwerking een landelijk operationele staf (LOS) ingericht.

Er loopt momenteel een project Netcentrisch Werken, dat de Veiligheidsregio's ondersteunt bij het invullen van het aspect informatievoorziening van het Besluit Veiligheidsregio's. Dit maakt het mogelijk om bij opschalingsituaties snel te komen tot eenduidig totaalbeeld van de situatie. Dit totaalbeeld dient als basis voor de te nemen besluiten en in te zetten acties.

Binnen het landelijke project Multi-respons CBRN lopen in dit kader twee initiatieven. Ten eerste de proeftuin Centrex die er op gericht is om als schakel te kunnen dienen tussen de CBRN 'kennis' en de operatie op de grond. Ten tweede een multidisciplinaire aanpak CBRN respons welke, op basis van het referentiekader crisisplan, inzicht geeft in de rollen, taken en verantwoordelijkheden van de hulpverleningsdiensten binnen de verschillende rampenbestrijdingsprocessen (in zowel de hot- als de warmzone). Hierin wordt het vraagstuk van persoonlijke beschermingsmaatregelen meegenomen.

Conclusie spoorwegongeval en maritiemongeval

Bij grote ongevallen vallen doden en gewonden, dit heeft een grote sociaal psychologische impact op de maatschappij. Om het aantal doden en gewonden en de sociaal psychologische impact zoveel als mogelijk te beperken is het van belang dat de bevolking tijdig heldere berichten ontvangt van de overheid. Deze berichten zijn zoveel als mogelijk voorzien van informatie over de situatie en wat te doen. In beide scenario's is crisiscommunicatie dan ook als te versterken capaciteit geagendeerd.

3.4 Schaarste

Voedselschaarste (sojabonen)

Het Europese voedselproducerende systeem is behoorlijk robuust uit het oogpunt van voedselbeschikbaarheid met een overschot aan productie. Er is een grote koopkracht om voedsel aan te kopen op de internationale markt. Wèl zijn er mogelijke spanningen in de vraag-en-aanbod-balans ten gevolge van fluctuaties en calamiteiten. Eén van de mogelijke ontwrichtingen is het wegvallen van de soja-importen van buiten de EU. Voor deze eiwitrijke grondstoffen voor de veevoederindustrie is Nederland/Europa geheel afhankelijk van landen buiten de Europese Unie.¹⁴ Dergelijke verstoringen geven schokken in de voedselprijzen. Met name snelle prijsverhogingen geven aanleiding tot maatschappelijke onrust. Daarnaast zal de Nederlandse vee- en vleessector zwaar worden getroffen met aanzienlijke onrust in die gevoelige sector.

Het scenario heeft geen directe knelpunten opgeleverd in het huidige beleid of de huidige capaciteiten. Wel is er een aantal onderwerpen naar voren gekomen dat in de toekomst aandacht vraagt. Daarbij is een onderscheid te maken naar enerzijds alternatieve versturende invloeden op de voedselvoorziening van de Nederlandse burger en anderzijds ontwikkelingen in het complex van schaarse grondstoffen, waarbij het meer gaat om indirecte effecten op de nationale veiligheid.

Alternatieve versturende invloeden op de voedselvoorziening aan de consument

Het gaat hier om andere ontwikkelingen die een groter effect kunnen hebben op de voedselvoorziening voor de consument. Daarbij moet worden gedacht aan grote problemen in de logistiek. Het logistieke netwerk/distributie netwerk is op basis van het 'just in time delivery' principe ingericht. Omdat er in de hele productieketen bijna nergens voorraden van voeding(sgrondstoffen) worden aangehouden is het systeem kwetsbaar. Ook zijn de risico's in de afgelopen decennia veranderd. Waar het na de WOII vooral ging over dreigingen als oorlog en watersnood is nu vooral sprake van dreigingen op het terrein van techniek/ICT en transport. Risico's als bijvoorbeeld ICT-uitval en kwetsbaarheden rondom de logistieke kant zouden daarom interessant zijn om nader uit te werken in scenario's. Daarbij gaat het dan om bredere scenario's, waarin de voedselvoorziening (de beschikbaarheid van voedsel voor de consumenten) een onderdeel is. Immers verstoringen in de logistiek, ICT en energietoevoer treffen ook andere vitale functies.

Ontwikkelingen in het hele complex van schaarse grondstoffen

Hierbij gaat het om grote fluctuaties in de prijsontwikkeling, negatieve effecten van beleid gericht op de aanpak van één schaarste voor de andere schaarsten en de geopolitieke ontwikkelingen m.b.t. de schaarste aan grondstoffen (sluiten van grenzen, handelsrestricties, heffingen). Voor deze groep van ontwikkelingen is het van belang om te beseffen dat deze de nationale schaal ontstijgen. Aanpak daarvan

¹⁴ *Resilience of the European food system to calamities (2008), Wageningen University & Research Center in opdracht van het ministerie van LNV.*

vraagt Europese of mondiale actie. Deze bevindingen komen ook terug in de onderwerpen die in de capaciteitenanalyse zijn geïdentificeerd.

Te versterken capaciteiten

Tijdens de capaciteitenanalyse zijn de volgende belangrijke te versterken capaciteiten benoemd:

1. Monitoring en analyse capaciteit
2. Afhankelijkheden verminderen
3. Wereldvoedselsysteem en transitie (bewustwording)

Monitoring en analyse capaciteit

Het is van belang dat Nederland als exporterend land een goede observatiefunctie heeft. Monitoring en analyse van grondstofprijzen, (geo)politieke ontwikkelingen en (wijzigende) belangen van andere landen en spelers is nodig om crisissituaties aan te zien komen. Nederland moet met name zicht hebben op interferenties met andere vormen van schaarste (bijvoorbeeld energieprijzen). Een integrale analyse op deze verschillende monitors is noodzakelijk om de interactie tussen prijzen, internationale en geopolitieke ontwikkelingen en de interferenties goed te kunnen duiden. Dit vereist samenwerking op Europees en mondiaal niveau.

Afhankelijkheden verminderen

Nederland en Europa zijn geheel afhankelijk van landen buiten de Europese Unie voor soja import. Het is van belang inzicht te hebben in welke partijen Nederland van soja kunnen voorzien, met welke partijen samengewerkt moet worden, wat de relatie met deze partijen is en waar eventuele coalities voorbereid of gesloten kunnen worden.

Wereldvoedselsysteem en transitie (bewustwording)

Met een toenemende wereldbevolking wordt het in de toekomst steeds moeilijker om iedereen van voedsel te voorzien. De wereldwijde voedselproductie moet, in vergelijking met het niveau van 2005-2007, tot 2030 met meer dan 40% toenemen, en tot 2050 met 70%. Voedselproductie is sterk afhankelijk van water. Van het watergebruik in OESO-landen gaat 44% naar landbouw. Veranderende consumptiepatronen in opkomende economieën als China en India (meer melk en vlees) leiden tot een nog groter waterverbruik.¹⁵

Mogelijke toekomstige watertekorten kunnen tot problemen leiden in de wereldvoedselproductie. Ook vanuit het oogpunt van duurzaamheid is bewustwording van de kwetsbaarheid van het wereldvoedselsysteem nodig. Dit maakt dat aan de aanbodkant dient te worden nagedacht over transitie naar een efficiëntere en meer verantwoorde manier van voedselproductie. Tevens dient aandacht te worden besteed aan bewustwording bij consumenten.

Huidig beleid

¹⁵TK 2009-1010 31 793, 39 *Schaarste en Transitie, Kennisvragen voor toekomstig beleid*, p. 28

Het ministerie van ELenI is momenteel bezig met een aanpassing van het crisisdraaiboek voedselvoorziening. Hierin worden de uitkomsten van dit scenario en capaciteitanalyse meegenomen.

Daarnaast heeft het ministerie van ELenI namens de Nederlandse regering in het najaar de Global Conference on Agriculture, FoodSecurity and Climate Change georganiseerd in samenwerking met de FAO, de Wereldbank en regeringen van verschillende landen. Een initiatief dat voortvloeide uit het Nederlandse voorzitterschap van de Commission on Sustainable Development in 2009. Aan de conferentie namen regeringen, internationale organisaties, de private sector, non-gouvernementele organisaties, liefdadigheidsinstellingen, lokale producenten en de wetenschappelijke wereld deel. Tijdens de conferentie is een *roadmap* met concrete acties ontwikkeld, waarin investeringen, beleid en maatregelen in de landbouw worden gekoppeld aan een transitie naar een klimaatbestendige, emissiearme groei. Dit vanuit de overtuiging dat landbouw de oplossing kan zijn voor veel van de wereldproblemen. De conferentie werd voorgezeten door de Nederlandse staatssecretaris van Economische Zaken, Landbouw en Innovatie.

Het interdepartementale programma Duurzame Voedselsystemen draagt zorg voor de uitvoering van de beleidsagenda Duurzame Voedselsystemen. Deze agenda is een specifiek onderdeel van het voedselbeleid dat beschreven is in de nota Duurzaam Voedsel (juni 2009). De agenda richt zich op een optimale Nederlandse bijdrage aan de verduurzaming van het mondiale voedselsysteem, met een focus op het eiwitvraagstuk als één van de centrale uitdagingen voor het systeem. Ook de interdepartementale programma's *Biodiversiteit* en *Biobased economy* hebben in die zin een relatie met dit onderwerp daar in beiden de relatie naar voedselschaarste zijn meegenomen. Voor het programma *Biodiversiteit* betekent dit dat er een onderzoek is gedaan naar de relatie tussen biodiversiteit, voedsel en klimaatverandering. Het programma *Biobased economy* werkt vanuit de voorwaarde dat de ontwikkeling naar een *biobased economy* niet ten koste mag gaan van de wereldvoedselzekerheid.

Tot slot wordt gewezen op de interdepartementale verkenning 'Schaarste & Transitie'¹⁶. Kennisvragen voor toekomstig beleid'. De te agenderen capaciteiten monitoring en analyse, verminderen afhankelijkheden en transities in het wereldvoedselsysteem sluiten hier nauw bij aan.

In de brief aan de Eerste en Tweede Kamer over de verkenning Schaarste & Transitie is aangegeven dat één van de vervolgtacties zich richt op de vraag welke interdependenties (EU in relatie tot andere landen) en samenwerkingrelaties wederzijds profijtelijk zijn en hoe vooraf internationale coalities kunnen worden gevormd¹⁷.

Mineraal geopolitiek

¹⁶ TK 2009-1010 31 793, 39 *Schaarste en Transitie, Kennisvragen voor toekomstig beleid*

¹⁷ TK 2009-2010 31 793 nr.39

Mineralen zijn belangrijk voor de productie van bijvoorbeeld auto's, mobieltjes en tv's. Ook zijn mineralen vaak een essentiële schakel in producten die de transitie naar een duurzame energievoorziening bevorderen, zoals zonnepanelen. De OECD¹⁸ verwacht dat mede hierdoor de wereldvraag naar mineralen in 2030 2,5 keer zo groot is ten opzichte van 2005. De huidige geschatte hoeveelheden metalen en mineralen in de aardbodem zijn weliswaar ruim voldoende om tot na 2030 aan de (stijgende)vraag te voldoen. De vraag is echter of de noodzakelijke grondstoffen tijdig beschikbaar en voldoende betaalbaar blijven om aan de groeiende vraag van onder meer de opkomende economieën te voldoen, ook rekeninghoudend met een breder beleidskader waarin duurzaamheidsaspecten een steeds grotere rol spelen. Zeker is in ieder geval dat de markt voor metalen en mineralen gekenmerkt wordt door sterke prijscycli; er kunnen zich op kortere termijn situaties voordoen waarbij het aanbod achter blijft bij de vraag en de prijzen sterk kunnen stijgen. Ook neemt de concentratie van de voorraden in een beperkt aantal - soms instabiele - landen toe. Hierdoor stijgt het risico dat niet altijd onder gunstige voorwaarden toegang tot de voorraden kan worden verkregen. Dit kan nadelige gevolgen hebben voor de concurrentiepositie van de (duurzame) industrie in Nederland, omdat de EU in sterke mate importafhankelijk is, met name voor *hightech* metalen. Gezien het hiervoor geschreven belang van mineralen voor Nederland is het van groot belang om adequaat met dit onderwerp om te gaan onder meer om op termijn problemen voor de nationale veiligheid te voorkomen.

Te versterken capaciteiten

Tijdens de capaciteitanalyse zijn de volgende belangrijkste (categoriegroepen) capaciteiten benoemd:

1. Maatregelen gericht op het vervangen, efficiënter gebruiken en hergebruiken van mineralen.
2. Maatregelen om de toevoer van mineralen veilig te stellen.

Momenteel is het Nederlandse beleid ten aanzien van het vraagstuk schaarste aan mineralen in ontwikkeling. Uit de capaciteitanalyse komt een aantal zaken naar voren dat in ieder geval zou moeten worden opgepakt.

- Allereerst is er behoefte aan meer informatie over de mineralen die voor Nederland en haar industrie van strategisch belang zijn. Uitgezocht moet worden om welke bedrijven en sectoren het precies gaat en waar schaarste welk effect heeft.
- Verder is van belang om de kennisinfrastructuur ten aanzien van het vinden van substituten, recycling en efficiënter materiaalgebruik te versterken.
- Daarnaast moet de regie op het beleid verder versterkt worden, onder meer door in het interdepartementale visietraject 'Duurzaam Materialenbeheer' een integrale visie te formuleren die recht doet aan de economische-, milieu- en geopolitieke dimensies van het grondstoffenvraagstuk.
- Naast de noodzaak van interdepartementale versterking van beleid, is het ook van essentieel belang om het Europese beleid met betrekking tot dit

¹⁸ *Organisatie voor Economische Samenwerking en Ontwikkeling (OESO), "OECD Environmental Outlook to 2030", (2008)*

vraagstuk te versterken¹⁹. Alleen in Europees verband kan deze problematiek effectief worden aangepakt.

Huidig beleid

Het importeren van grondstoffen en het inspelen op mogelijke schaarste, door bijvoorbeeld te zoeken naar substituten, is in eerste instantie de verantwoordelijkheid van bedrijven zelf. Vaak is er echter geen sprake van een vrije internationale markt, waardoor er ook een rol voor de Nederlandse overheid, en breder de EU, is weggelegd.

Het kabinet heeft onlangs een integrale verkenning uitgevoerd naar ontwikkeling van schaarste aan voedsel, water, energie en mineralen in de context van klimaatverandering, biodiversiteit en veranderende geopolitieke verhoudingen in het kennistraject 'schaarste en transitie'²⁰. Naar aanleiding hiervan is een aantal kennisvragen neergelegd bij strategische adviesraden, planbureaus en kennisinstellingen²¹. In aanvulling hierop is bij het Ministerie van Economische Zaken, Landbouw en Innovatie gestart naar het belang van kritische grondstoffen voor de Nederlandse economie (afroning is gepland eind 2010). Organisaties van ondernemers (VNO-NCW en FME-CWM) zijn hierbij betrokken. De Nederlandse inzet op het gebied van grondstoffen in bijvoorbeeld het industriebeleid, onderzoek en innovatie, handelspolitiek en duurzaamheid zal op basis van de antwoorden op de genoemde kennisvragen nader worden ingevuld. Gezien de grote belangen die hiermee gediend zijn, is één gezamenlijke strategie met betrokkenheid van overheid, bedrijven en kennisinstellingen van belang. Verder is er een belangrijke link met het Raw Materials Initiative van de EU, waarvan eind 2010 een update wordt verwacht en waarvoor de antwoorden van genoemde kennisvragen tevens belangrijke input voor Nederland zijn. Hoewel het bovengenoemde scenario aanwijzingen geeft dat toekomstige grondstoffenschaarste risico's kan inhouden voor nationale veiligheid (o.a. sociale onrust die optreedt als gevolg van negatieve economische effecten) is de economische insteek dominant in dit dossier. Regie voor nadere uitwerking van de genoemde trajecten ligt daarom bij het ministerie van Economische Zaken, Landbouw en Innovatie.

Conclusie schaarste

De komende decennia wordt het probleem van schaarste meer veroorzaakt door politiek gedreven distributieschaarste dan door absolute schaarste (beperking van de fysieke omgeving). Geopolitiek gedreven schaarste vraagstukken kunnen in potentie leiden tot politieke en economische instabiliteit en kunnen daarmee indirect gevolgen hebben voor de nationale veiligheid (vergelijk de gasdistributie via de Oekraïne). Het is daarom van belang om nationale veiligheidsbelangen goed te bezien vanuit de internationale context. Een goede koppeling tussen nationale veiligheid met het Nederlandse buitenlandbeleid is hierbij noodzakelijk.

¹⁹ *Het EU Raw Material Initiative geeft aan dat de EU een geïntegreerd grondstoffenbeleid heeft.*

²⁰ TK 2009-1010 31 793, 39 *Schaarste en Transitie, Kennisvragen voor toekomstig beleid*

²¹ TK, 2009-2010, 31 793 nr. 39.

Tevens is het van belang goed inzicht te hebben op hoe de verschillende schaarsten en gevolgen daarvan op elkaar in kunnen werken. Te denken valt aan de relatie tussen voedsel en water, mineralen en energie. Een beter zicht hierop maakt dat gefundeerde keuzes kunnen worden gemaakt waar overheidsmaatregelen nuttig kunnen zijn en waar niet.

3.5 Conclusie

In paragraaf 3.2 tot en met 3.5 zijn voor alle nieuw ontwikkelde scenario's de uitkomsten van de capaciteitsanalyses samengevat. Samenvoeging van deze capaciteitsanalyses leidt, mede afgezet tegen eerdere capaciteitsanalyses, tot identificatie van een aantal gemeenschappelijkheden.

Ten eerste blijkt uit de meeste capaciteitsanalyses weer eens de grote afhankelijkheid die Nederland kent van haar internationale omgeving. Voor voedselproducten betreft dat vooral de import van voedselgrondstoffen. Nederland moet ook veel mineralen (maar ook energiebronnen) importeren, met name voor de ontwikkeling en productie van duurzame goederen. Bovendien is Nederland in velerlei opzichten een transitieland: veel transport loopt via de Rotterdamse Haven, Schiphol of het treinverkeer. Ook voor het digitale domein en energievoorziening fungeert Nederland als transitieland. Naast het feit dat Nederland sterk profiteert van de toegevoegde waarde van deze relaties, dragen deze afhankelijkheden ook risico's in zich. De effecten die een cyberconflict op Nederland kan hebben of die verstoring van aanvoer van grond- en voedingstoffen kan hebben kunnen zeer grote gevolgen hebben. Het beïnvloeden van deze potentiële risico's en afhankelijkheden is voor Nederland alléén lastig. De vraagstukken vragen vaak om een meer internationale insteek, waarbij Nederland nauw moet samenwerken met andere landen en internationale organen. Het is dan ook van groot belang om bij het internationaal opereren van Nederland de nationale (veiligheids)belangen terdege mee te nemen.

Ten tweede komt uit de meeste capaciteitsanalyses het grote belang van goede informatiewinning, -analyse en -deling naar boven. In alle capaciteitsanalyses komt naar voren dat het tijdig beschikken over voldoende juiste informatie(analyse) een randvoorwaarde is voor het ontwikkelen van het meest effectieve beleid. Weten welke mineralen voor de Nederlandse industrie essentieel zijn, maakt het mogelijk maatregelen te nemen om de effecten van schaarste aan mineralen te beperken. Tijdige informatiedeling versterkt het effect van preventieve en responsieve maatregelen. Afspraken over ondersteuning en overname van uitgevallen of beschadigde systemen verhogen bijvoorbeeld de weerstand van ICT netwerken. Het tijdig delen van informatie kan de preparatie en respons op een incident verbeteren en versnellen. Monitoring maakt het mogelijk afwijkende ontwikkelingen vroegtijdig te signaleren. De opmerking over afhankelijkheid van het buitenland geldt ook hier: kennis over het gebruik van voedselproducten (biobrandstoffen) voor duurzame energie maakt het mogelijk het initiatief te nemen

om in internationaal verband de dialoog aan te gaan over afspraken ten aanzien van de 'wereldvoedselzekerheid'.

Ten derde wordt in de meeste nieuwe scenario's duidelijk gemaakt dat de overheid niet de enige speler is die invloed uitoefent op het ontstaan en verloop van een incident. Ook het bedrijfsleven en de samenleving zullen bij moeten dragen aan het voorkomen en/of beperken van de gevolgen van een incident. Uit de capaciteitanalyses komt de vraag naar voren of het bestaande beleidsinstrumentarium van de overheid in de publiek-private verhoudingen zoals Nederland die nu kent, het maatschappelijke belang in de context van de nationale veiligheid voldoende bescherming kan bieden. Zo is het continuïteitsvraagstuk binnen het netwerk van (internationale) internet exchanges de verantwoordelijkheid van deze partijen zelf. Of en hoe dit geregeld is, is wel van groot belang voor de maatschappij en verlangt daarmee de mogelijkheid voor de overheid om afwegingen te kunnen maken op dat terrein.

Ten slotte is een vernieuwend element ten opzichte van eerdere scenario's de introductie van dreigende situaties die (nog) niet hebben geleid tot een daadwerkelijk incident. Een voorbeeld hiervan zijn de scenario's met betrekking tot schaarste. De manier waarop met deze situatie wordt omgegaan is cruciaal ten aanzien van het wel of niet uitgroeien tot een daadwerkelijke crisis. Voor dit type dreigingen zijn vooral preventieve en preparatieve maatregelen van belang; maatregelen die de waarschijnlijkheid moeten beperken dat zich een incident gaat voordoen. Uit de analyses komt hierbij overigens duidelijk naar voren dat de manier waarop gecommuniceerd wordt en/of publieksinformatie wordt uitgewisseld van grote invloed kan zijn op de ontwikkeling van een situatie. Bijkomende uitdaging is dat soms al op korte termijn maatregelen genomen moeten worden om op lange termijn een incident te voorkomen of de gevolgen ervan te beperken. Fysieke schaarste aan mineralen is bijvoorbeeld de eerstkomende jaren naar verwachting geen grote dreiging, maar het kabinet onderzoekt nu alvast of actie nodig is om te voorkomen dat er zich op langere termijn wel een situatie voordoet die onder meer de nationale veiligheid kan aantasten.

Deze hierboven beschreven observaties hebben geleid tot een viertal breed inzetbare capaciteiten die mogelijk ontwikkeld of versterkt zouden moeten worden. In hoofdstuk 4 wordt nader ingegaan op deze vier mogelijk te versterken breed inzetbare capaciteiten en op een aantal specifieke capaciteiten voor individuele dreigingen.

4. Agenderingsadvies

4.1 Inleiding

In hoofdstuk 3 is per thema weergegeven welke capaciteiten volgens de experts versterkt zouden kunnen worden om de waarschijnlijkheid van een dreiging en de mogelijke gevolgen ervan te beperken. In de volgende paragrafen wordt een voorstel gedaan om een aantal capaciteiten daadwerkelijk te ontwikkelen en/of te versterken. Daarbij wordt onderscheid gemaakt tussen capaciteiten die op meerdere incidentscenario's effect hebben en capaciteiten die een bijdrage leveren aan het terugbrengen van het risico op een specifiek incidentscenario.

De keuze voor de te ontwikkelen en/of te versterken capaciteiten, zowel breed inzetbaar als specifiek, hangt af van een aantal factoren:

- Wat is de plaats van het incidentscenario in het risicodiagram? (de 'score' op waarschijnlijkheid en impact);
- Heeft versterking van een capaciteit een vermindering van de waarschijnlijkheid of van de impact voor één of meer van de impactcriteria tot gevolg? (effectiviteit van de capaciteit)
- Kan met een relatief kleine investering een grote versterking worden gerealiseerd? ('quick-win' / kosten-batenanalyse);
- Raakt het scenario aan een onderwerp dat als politieke prioriteit is benoemd? (politieke urgentie / haalbaarheid);

In paragraaf 4.2 en 4.3 wordt de agendering voor 2009-2010 weergegeven voor de breed inzetbare (4.2) en specifieke (4.3) capaciteiten. De ontwikkeling/versterking van breed inzetbare en/of specifieke capaciteiten vereist inspanning van zowel de overheid, de burger als het bedrijfsleven.

4.2 Aanbeveling 2010: breed inzetbare capaciteiten

De uitkomsten van de derde cyclus van de Nationale Risicobeoordeling en de bijbehorende capaciteitenanalyse hebben de volgende aandachtspunten opgeleverd:

- Nederland is in belangrijke mate afhankelijk van het buitenland. Dit geldt zowel waar het gaat om incidenten of ontwikkelingen die in het buitenland plaatsvinden en die gevolgen kunnen hebben voor de Nederlandse nationale veiligheid. Als ook daar waar het gaat om in Nederland genomen maatregelen ter voorkoming van- of voorbereiding en respons op risico's die van invloed kunnen zijn op het buitenland.
- In een snel veranderende wereld kunnen nieuwe dreigingen zich razendsnel ontwikkelen en aan waarschijnlijkheid of impact winnen. Het is daarom van groot belang om in een vroeg stadium zicht te krijgen op mogelijke dreigingen en om interferenties tussen dreigingen in beeld te brengen. De internationale context en de tijdsduur zijn daarbij belangrijke factoren. Om

in staat te zijn tot een vroegtijdige (h)erkenning van dreigingen is een goede informatiewinning, -analyse en -deling cruciaal.

- Op een aantal terreinen is sprake van een publiek-private verantwoordelijkheidsverdeling. Deze verantwoordelijkheidsverdeling is veelal niet vanuit het nationale veiligheidsbelang gegroeid en het is de vraag of het huidige beleidsinstrumentarium dat de overheid ter beschikking staat afdoende is om de nationale veiligheidsbelangen te behartigen.
- In bijna alle scenario's is sprake van een grote sociaal-psychologische impact. Crisiscommunicatie door de overheid is cruciaal om onnodige escalatie en sociaal-psychologische onrust te voorkomen. Meer inzicht in de sociaal-psychologische aspecten van dreigingsituaties, de invloed die communicatie als instrument hierop kan hebben en de rol die de nieuwe media hierbij kan spelen is gewenst.

Deze aandachtspunten hebben geleid tot een viertal breed inzetbare capaciteiten die mogelijk ontwikkeld of versterkt zouden moeten worden.

4.2.1 *Integratie nationale veiligheidsbelangen in internationaal beleid*

Voor een groot aantal dreigingen geldt dat zij transnationaal van aard zijn. Bij een significant aantal van deze dreigingen is de aard, omvang, complexiteit en dynamiek van dien aard dat deze de autonome Nederlandse capaciteiten om hier effectief weerstand tegen te bieden te boven gaan. De Nederlandse samenleving is in toenemende mate geïntegreerd in een mondiaal sociaaleconomisch systeem. Dit levert Nederland als internationaal georiënteerde handelsnatie grote sociale en economische voordelen op. De keerzijde van de medaille is echter dat Nederland door haar bereikbaarheid (fysiek en virtueel), allianties (VN, NAVO, EU), economische specialisatie, welvaart en technologische ontwikkeling en het daarmee samenhangende consumptiepatroon ook kwetsbaarder is voor transnationale dreigingen. De activiteiten van transnationale terroristische en criminele netwerken, het uitbreken van een pandemie, de aantasting of uitval van essentiële diensten (ICT, Telecom, financieel) of ernstige schaarste van essentiële producten (energiebronnen, voedsel, water en mineralen) kunnen in Nederland tot maatschappelijke ontwrichting leiden. De mogelijkheden van Nederland om de onderliggende processen van dreigingen als een mondiale economische crisis of schaarste te beïnvloeden zijn zeer beperkt. Een internationale aanpak in coalitieverband is voor Nederland daarom noodzakelijk om Nederlandse beleidsmakers handelingsperspectief te bieden bij de aanpak van dergelijke crisis. De uitkomsten uit de derde cyclus van de Nationale Risicobeoordeling en de bijbehorende capaciteitenanalyse geven aanleiding om het aspect van nationale veiligheid nadrukkelijk(er) mee te nemen in het internationale opereren van Nederland. Dit kan gedaan worden door nationale veiligheidsthema's internationaal te agenderen, door het zoeken naar samenwerking met één of meerdere landen en het aansluiten bij initiatieven van internationale organisaties als EU, NAVO, VN, enz.

Advies:

Concreet wordt daarom geadviseerd om bij invulling van het internationale beleid waar nodig nationale veiligheid nadrukkelijk(er) mee te nemen. Hierbij draait het zowel om de preventie van risico's als de voorbereiding en respons op mogelijke risico's. Lange termijn risico's zoals schaarste van grondstoffen en primaire levensbehoeften dienen hierbij prominent aandacht te krijgen.

4.2.2 *informatiewinning, analyse en deling*

Sinds de totstandkoming van de strategie Nationale Veiligheid is de afgelopen drie jaar een groot aantal dreigingen volgens de bijbehorende werkwijze uitgewerkt. Met de totstandkoming van deze bevindingenrapportage zijn drie cycli van Nationale Risicobeoordeling en capaciteitanalyse doorlopen. Eén van de belangrijkste lessen die geleerd kan worden is dat de effectiviteit van de strategie en met name ook de mate waarin Nederland zich kan voorbereiden op allerlei dreigingen valt of staat met de kwaliteit van de informatie die wordt gebruikt en die wordt gedeeld.

Het vroegtijdig in beeld krijgen welke dreigingen kunnen ontstaan leidt er toe dat eerder en mogelijk beter gereageerd kan worden op potentiële bedreigingen voor de maatschappij.

Dit gegeven komt uit veel capaciteitanalyses naar voren. Hierbij is een belangrijk aandachtspunt de (mogelijke) interferentie die kan bestaan tussen verschillende terreinen cq. dreigingen en ontwikkelingen.

Binnen de werkwijze van de strategie is in het onderdeel rijksbrede analyse een aantal instrumenten benoemd die bij moeten dragen aan het zo goed mogelijk identificeren van potentiële dreigingen die nadere aandacht behoeven. Dit kan in de vorm van acuut te ondernemen acties, maar ook in de vorm van nadere uitwerking in een Nationale Risicobeoordeling en capaciteitanalyse. Hierbij kan het gaan om vraagstukken die op korte termijn opspelen (0 tot 6 maanden) en waar direct (politieke) sturing en actie op nodig is. Te denken valt aan consequenties van (internationaal) politiek en maatschappelijk gevoelige kwesties (zoals bijvoorbeeld de voorgenomen bijbel verbranding in de VS) of plotseling opspelende (potentieel) dreigende situaties zoals de 'as-wolk' van begin 2010. Het kan echter ook gaan om zaken die op langere termijn zouden kunnen gaan spelen (10 tot 20 jaar) en die vaak een meer sluipend karakter hebben. Hierbij valt te denken aan bijvoorbeeld prijsontwikkelingen, (geo)politieke ontwikkelingen en (wijzigende) belangen van andere landen en de interferenties daartussen. Beide analyses kunnen informatie opleveren op basis waarvan de nationale risicobeoordeling kan worden uitgevoerd. Op versterking van beide moet dan ook worden ingezet.

Advies:

Om meer directe en samenhangende (politieke) sturing mogelijk te maken op actuele dreigingen moet een actueel dreigingsbeeld structureel worden opgesteld en behandeld. Bij de vormgeving hiervan kan worden aangesloten bij bestaande initiatieven op dit vlak vanuit het traject Crisisstructuur op Rijksniveau (CoR) (NCC en DCC's). Voor de lange termijn analyses wordt op basis van ervaringen met de

werkwijze van de strategische verkenningen nationale veiligheid 2008 onderzocht hoe de lange termijn analyses in de toekomst tot stand kunnen komen. Bij de versterking zijn belangrijke aandachtspunten 'de internationale context', 'sector overstijgende interferentie (voedselgrondstoffen die ook als biobrandstof gebruikt kunnen worden)', 'publieke versus private belangen' en sluipende ontwikkelingen. Hierbij zouden ontwikkelingen die zich hebben voorgedaan ten aanzien van de informatiepositie op terreinen als olie en voedsel in ogenschouw kunnen worden genomen. Bij het versterken van de lange termijn verkenningen zal onder meer gekeken moeten worden hoe bestaande kennisdragers binnen de overheid (o.a. planbureau's), maar mogelijk ook daar buiten kunnen worden benut om de informatiepositie met betrekking tot nationale veiligheidsvraagstukken te versterken.

4.2.3 *Nationale veiligheidsbelangen in publiek private verhoudingen (Governance)*

Samenwerking tussen overheden en private partijen is de laatste jaren steeds belangrijker geworden wanneer het gaat om nationale veiligheidsvraagstukken. De intensieve samenwerking die op het terrein van de bescherming van de vitale infrastructuur in de afgelopen jaren tot stand is gekomen is hier een goed voorbeeld van. Het belang van goede samenwerking komt voor een belangrijk deel voort uit de gedeelde betrokkenheid, maar ook gedeelde verantwoordelijkheid van overheid en private organisaties op veel terreinen. In de afgelopen decennia hebben liberalisering, globalisering, maar ook technologische ontwikkelingen voor sommige terreinen geleid tot een complexe verdeling van verantwoordelijkheden en afhankelijkheden. De nationale veiligheid is echter niet altijd een aandachtspunt geweest in de gegroeide verantwoordelijkheidsverdeling en met name het daarbij gerealiseerde beleidsinstrumentarium.

De capaciteitanalyses t.b.v. de diverse scenario's voor ICT uitval zijn mede aanleiding voor het stellen van de vraag of de overheid, uitgaande van de huidige verantwoordelijkheidsverdeling binnen het Telecom/IT-domein over afdoende (beleids-)instrumenten beschikt om het maatschappelijke belang vanuit de context van nationale veiligheid te beschermen.

Aangezien er mogelijk meer domeinen zijn waarvoor dit vraagstuk zou kunnen gelden kan dit capaciteitsvraagstuk als een breed inzetbare worden opgevat. Ondersteunend aan deze constatering zijn o.a. de discussies over de verkoop van elektriciteitsproducenten aan buitenlandse bedrijven in 2009 en de groeiende rol van nationale investeringsfondsen van landen als China en Saoedi-Arabië. In de beantwoording van deze vraag dient de balans te worden gezocht die past binnen onze staatsrechtelijke verhoudingen, onze open handelseconomie en onze cultuur waarin samenwerking centraal staat. Een belangrijke bijkomende factor is het internationale perspectief.

Advies:

Om antwoord te kunnen geven op de vraag of het bestaande beleidsinstrumentarium voldoende toepasbaar is kan een evaluatie van aan de overheid ter beschikking staande instrumenten op een aantal relevante domeinen worden uitgevoerd. De analyse moet ingaan op de doelbereiking, de effectiviteit en de bedoelde en onbedoelde effecten tussen de verschillende instrumenten in onderlinge samenhang.

Om structuur in de evaluatie aan te kunnen brengen wordt geadviseerd om te beginnen met de (telecom/)IT sector. Dit omdat deze sector een zeer internationaal karakter kent en een van oudsher terughoudende overheidsbetrokkenheid kent. Verder geldt dat binnen deze sector op dit moment internationaal de discussie over het governance vraagstuk in bredere zin loopt en zoveel mogelijk op deze discussie aangesloten kan worden. Aan de hand van het verloop van de evaluatie kunnen vervolgens andere sectoren betrokken worden om te bepalen of ook voor die domeinen een nadere evaluatie op dit vlak nodig is.

4.2.4 Communicatie bij dreiging en crisissituaties

De rol van communicatie op het terrein van nationale veiligheid is al meerdere malen als belangrijk aandachtspunt benoemd. Hierbij is in de afgelopen jaren de focus gelegd op:

- Eenduidige communicatie: 'één boodschap' vanuit de overheid, afstemming met private partijen.
- Geven van helderheid over wat burgers en organisaties wel en niet kunnen verwachten van de overheid en andere partijen en
- Schetsen van handelingsperspectief om de zelfredzaamheid van mensen en organisaties te bevorderen;
- Bijdragen in de beeldvorming aan het beeld van een betrokken overheid, door in de communicatie nadrukkelijk aandacht te besteden aan duiding en betekenisgeving.

Deze zaken blijven van groot belang en hebben in de afgelopen tijd al veel opgeleverd zoals de interdepartementale coördinerende rol van het NCC op het gebied van crisiscommunicatie en de Denk Vooruit-campagne.

Uit de huidige Nationale risicobeoordeling (2009-2010) en capaciteitanalyses is naar voren gekomen, dat bij een dreigende of daadwerkelijke aanslag of crisis de manier waarop de overheid communiceert van groot belang kan zijn voor de wijze waarop de maatschappij reageert. Het is van belang dat bestuurders, communicatieadviseurs en crisismanagers zich ervan bewust zijn dat het hoe, wanneer en door wie in de media brengen van onderwerpen en het reageren van de overheid op signalen uit de maatschappij van directe invloed kan zijn op hoe de maatschappij reageert. Hierbij spelen nieuwe, 'social media' als You Tube, Facebook en Twitter een belangrijke rol.

Advies:

Concreet wordt geadviseerd om:

1. Crisiscommunicatie nog meer als een volwaardig instrument in te zetten om het ontstaan van een crisis tegen te gaan, dan wel de impact van een crisis te beperken. Om dit te bewerkstelligen zal onderzoek worden gedaan naar de sociaal-psychologische aspecten van (langer durende) dreigings- en/of crisissituaties en de toegevoegde waarde van crisiscommunicatie als beleidsinstrument. Tevens zal hier in evaluaties van crisissituaties structureel aandacht voor worden gevraagd. Het bestaande evaluatieformat van het Nationaal Crisiscentrum wordt hierop aangepast. Het overdragen van deze kennis zal door het Nationaal Crisiscentrum via het bestaande netwerk van communicatieadviseurs, crisismanagers en bestuurders actief worden uitgedragen bij opleidingen, advisering bij oefeningen en crisis en publicaties over dit onderwerp
2. De rol van de nieuwe media (social media) te erkennen als een kans (sneller en breder inzicht in zorgen en vragen en geruchten) en als een uitdaging: doordat informatie zich steeds sneller en zichtbaar voor iedereen verspreidt en de overheid - voorafgaand aan en tijdens crises - niet meer de enige informatiebron en autoriteit is, wordt de urgentie nog groter om als overheid snel en adequaat te communiceren met de samenleving. Dit vraagt enerzijds om bewustwording bij bestuurders, crisismanagers en communicatieprofessionals en anderzijds om meer capaciteit en een andere werkwijze en organisatie van communicatie door de overheid. Op basis van onderzoek²² naar de mogelijkheden van nieuwe media (social media) bij crises en ervaringen die ELenI heeft opgedaan met gebruik van nieuwe media in de bestrijding van de Q-koorts crisis²³ wordt nader verkend hoe de overheid hiermee om kan gaan.

4.3 Aanbevelingen 2010: specifieke capaciteiten

In de vorige paragraaf is een aantal breed inzetbare capaciteiten benoemd dat nadere uitwerking zou moeten krijgen. Naast deze breed inzetbare capaciteiten zijn er uit de uitgevoerde analyses zoals beschreven in hoofdstuk 4 ook enkele specifieke capaciteiten gekomen die nadere aandacht vergen. In deze paragraaf wordt hier nader op in gegaan.

4.3.1 ICT-uitval

Cyberconflict

Cyber security krijgt bij private en publieke partijen al enkele jaren de aandacht. Een brede maatschappelijke aanpak in relatie gebracht tot internationale

²² *Twitter in Crisiscommunicatie, een onderzoek naar de mogelijkheden van het gebruik van Twitter tijdens crises, COT Instituut voor Veiligheids- en Crisismanagement – an AON Company, Den Haag, mei 2010*

²³ *De directie communicatie bij ELenI heeft tijdens de Q-koorts crisis in 2010 voor de eerste keer gebruik gemaakt van twitter voor het informeren van doelgroepen. Deze ervaring zal interdepartementaal gedeeld worden om zodoende het gebruik van social media bij crises verder te optimaliseren.*

machtsverhoudingen is echter van recente aard. Deze aanpak wordt uitgewerkt in de Nationale Cyber Security Strategie (NCSS). Uit de capaciteitenanalyse komt een aantal zaken naar voren dat in ieder geval zou moeten worden opgepakt.

Uit de capaciteitenanalyse 'cyber conflict' komen een aantal zaken naar boven die aansluiten bij de capaciteiten die ook voor andere scenario's zijn geïdentificeerd.

1. Het sterk internationale karakter van de dreiging dat er toe noodzaakt dat de hier aan verbonden nationale veiligheidsbelangen in sterke mate geïntegreerd moeten worden in het Nederlandse internationale beleid.
2. Het gegeven dat gedegen vergaring, analyse en deling van informatie nodig is om dit soort dreigingen te identificeren is in brede context geïdentificeerd.
3. Het belang van duidelijkheid ten aanzien van regie en aansturing op dit terrein waar private partijen een zeer grote rol spelen. De geïdentificeerde aandacht voor het governance vraagstuk op ICT terrein sluit hier op aan.

Naast deze capaciteiten van generieke aard worden ook twee belangrijke constatering gedaan die primair voor dit type dreigingsscenario van belang zijn. Het gaat hierbij om:

1. Het versterken van de mogelijkheid om de beschikbare publieke en private responscapaciteit gezamenlijk en gericht in te zetten om de ICT dreiging aan te pakken.
2. Nederland moet over de kennis en middelen beschikken om meer pro-actief te reageren op 'aanvallen' op de samenleving via elektronische weg.

Advies:

Al de bovenstaande punten zouden de komende tijd moeten worden opgepakt. Veel publieke en private partijen ontplooi activiteiten op het terrein van cyber security. Echter, een veilig gebruik van ICT vergt een brede maatschappelijke aanpak. Momenteel wordt samen met private partijen gewerkt aan een Nationale Cyber Security Strategie (NCSS) en een bijbehorend actieplan. Bovenstaande capaciteiten kunnen de basis vormen voor het actieplan.

"Uitval Nederlandse Internet Exchanges"

Uit de analyse van het internet exchange (IX) scenario is gebleken dat de manier waarop het netwerk van IX'en is opgebouwd, leidt tot een relatief zeker systeem. De impact van een verstoring van een individuele IX lijkt minder groot dan tot nu toe vaak gedacht. De meerwaarde van deze analyse is dan ook onder meer dat een dreiging die eerder als mogelijk groot werd gezien nu als relatief klein kan worden betiteld.

Er is echter in meer algemene termen wel gebleken dat uitgaande van de bestaande verantwoordelijkheidsverdeling, zoals bijvoorbeeld blijkt bij de analyse van de ICT uitval scenario's, het ter beschikking staande overheidsinstrumentarium vanuit het perspectief van nationale veiligheidsbelangen tegen het licht moet worden gehouden. In deze context zal worden onderzocht of er omstandigheden bestaan waaronder het transport van het dataverkeer problemen kan ondervinden als gevolg van uitval van meerdere grote buitenlandse internet exchanges. Aangezien dit vraagstuk breder dan alleen voor de ICT sector geldt is dit vraagstuk in paragraaf 4.2.3 als breed inzetbare capaciteit opgevoerd.

4.3.2 *Grootschalig ongeval*

Crisiscommunicatie is ook bij een grootschalig ongeval een voorwaardelijk instrument om de gevolgen in te perken. Een eensluidende en snelle communicatieboodschap is hierbij essentieel. Aangezien crisiscommunicatie bij meerdere scenario's is benoemd als te versterken capaciteit is dit onderwerp in paragraaf 5.2.4 als breed inzetbare capaciteit opgevoerd.

4.3.3 *Schaarste*

Schaarste van grondstoffen kan leiden tot gevolgen voor de nationale veiligheid wanneer hier niet adequaat mee omgegaan wordt. Nederland moet hierbij opereren in een internationaal speelveld. Het vraagstuk of Nederland effectief kan optreden in deze internationale context is bij de breed inzetbare capaciteiten reeds geagendeerd (4.2.1).

Naast de internationale context kent Nederland ook beleid dat zich met name richt op Nederland zelf. Rond het vraagstuk mineraal geopolitiek lopen verschillende initiatieven (project Schaarste en Transitie, Initiatief Duurzame handel en het Platform Materiaalschaarste) volgens betrokken experts is er echter onvoldoende sprake van duidelijke regie op hoe deze initiatieven elkaar beïnvloeden laat staan versterken.

Het wordt dan ook van belang geacht dat ter voorkoming van mogelijke gevolgen in de toekomst voor de nationale veiligheid de regie op het terrein van omgang met schaarse mineralen versterkt wordt. Het interdepartementaal visietraject 'Duurzaam materialenbeheer' zal hier aan bijdrage. Hierin worden de geo-politieke, milieu- en economische dimensie van grondstoffenschaarste meegenomen.

Een belangrijk vraagstuk ten behoeven van deze versterkte regie is het inzicht in welke mineralen voor welke partijen in Nederland van groot belang zijn en hoe zich dit verhoudt tot de behoeftes in het buitenland. Monitoring van zaken als vraag en aanbod en afhankelijkheidsrelaties op het terrein van deze schaarste mineralen is dan ook van groot belang.

Concreet wordt geadviseerd om:

1. De regie op het beleid ten aanzien van de omgang met schaarse mineralen te versterken. Lopende initiatieven op dit vlak zoals het interdepartementale visietraject 'Duurzaam materialenbeheer' geven hier al gedeeltelijk invulling aan.
2. De Nederlandse informatie positie ten aanzien van schaarse mineralen nationaal en in internationaal perspectief te vergroten. Het lopende onderzoek naar kritieke grondstoffen voor de Nederlandse economie draagt hier in belangrijke mate aan bij.

4.4 Tot slot

Met de totstandkoming van de derde bevindingenrapportage nationale veiligheid is weer een stap gezet in de groei van de Strategie Nationale Veiligheid. Zo is met deze cyclus zoals eerder gezegd de nationale risicobeoordeling door uitwerkingen van scenario's op het terrein van schaarste bijna 'all hazard' op het niveau van benoemde dreigingstypen. De groei voor wat betreft de benoemde capaciteiten zit in het feit, dat in deze cyclus de breed inzetbare capaciteiten van meer strategische en preventieve aard zijn. In de eerdere bevindingenrapportages waren deze breed inzetbare capaciteiten vaak van meer responsieve en/of tactisch-operationele aard.

Inhoudelijk gaat het hierbij om:

- het versterken van de samenhang tussen nationale veiligheidsbelangen en de internationale beleidsinzet.
- het meer in samenhang monitoren van (internationale) ontwikkelingen met als doel het vroegtijdig kunnen identificeren van dreigen.
- het evalueren van de ter beschikkingstaande instrumenten voor de rijksoverheid om haar verantwoordelijkheid voor nationale veiligheid waar te kunnen maken.
- En het meer als daadwerkelijk (beleids)instrument inzetten van communicatie om crisis te voorkomen.

Voor wat betreft de toekomst zit de groei van de strategie onder meer in:

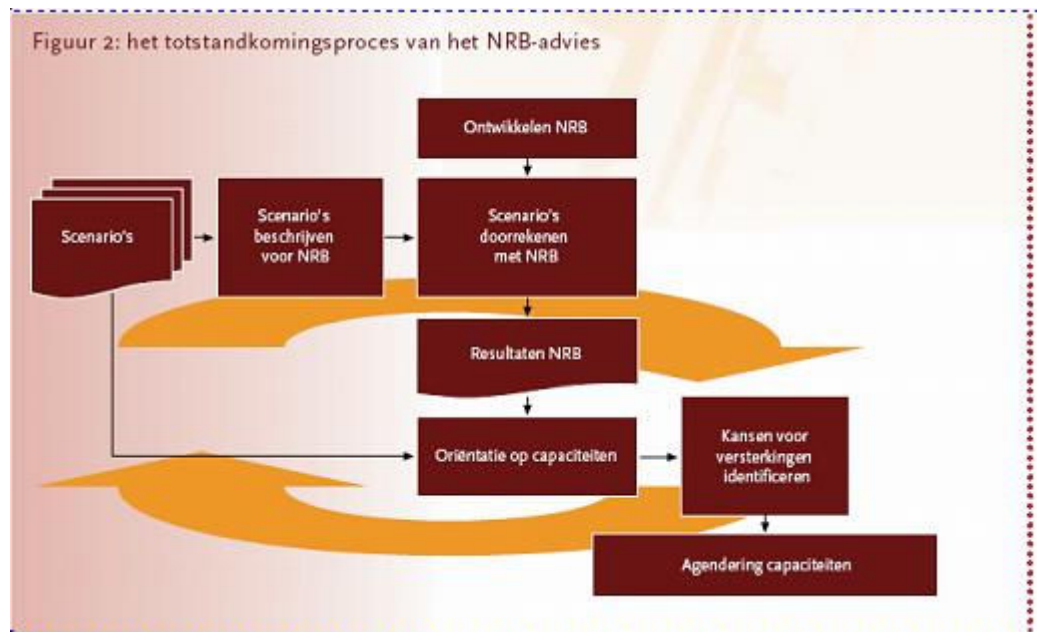
- Het versterken van de informatie- en kennisbasis over zich mogelijk ontwikkelende dreigingen, onder meer om meer direct (politiek) sturing te kunnen geven op basis van actuele dreigingsbeelden.
- Het doorontwikkelen van de capaciteitenanalyse. Aandachtspunten hierbij zijn de compleetheid van het huidige palet aan benoemde capaciteiten, de manier waarop het inzicht in het niveau van benodigde capaciteiten actueel gehouden kan worden en de aansluiting tussen het nationale beeld, de uitkomsten van regionale capaciteitenanalyses van de veiligheidsregio's en mogelijke internationale ontwikkelingen op dit vlak. Hierbij is het streven om op basis van de capaciteitenanalyses waar mogelijk en nodig concrete handelingsperspectieven te ontwikkelen op (inter)nationaal en regionaal niveau.
- En het vergroten van de effectiviteit van de implementatie van geagendeerde capaciteiten, waarbij de samenwerking tussen overheidspartijen, bedrijfsleven en andere mogelijk betrokkenen een belangrijk aandachtspunt is.

Bijlage 1 Methodiek: van scenario's tot capaciteiten

B1.1 Inleiding

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

- Scenario's (B1.2);
- Nationale RisicoBeoordeling (NRB) (B1.3)
- Oriëntatie op capaciteiten (B1.4)



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.

B1.2 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.

B1.3 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 wereld²⁴. 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)
Sociale en politieke stabiliteit	5.1 Verstoring van het dagelijkse leven 5.2 Aantasting van de democratische rechtstaat 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.

²⁴ Technische Universiteit Delft, het Sociaal en Cultureel Planbureau, TNO Defensie en Veiligheid, AON Global Risk Consulting, het Rijksinstituut voor Volksgezondheid en Milieu, het Milieu en Natuur Planbureau (nu Planbureau voor de Leefomgeving (PBL)), de AIVD en het ministerie van VenJ.

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 capaciteiten²⁵ 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.

B1.4 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 versterken capaciteiten. De capaciteitenanalyses zijn uitgewerkt door thematische expertgroepen.

²⁵ 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.

Bijlage 2 Uitgebreide leeswijzer risicodiagram

B2.1 Leeswijzer risicodiagram

Op de verticale as is de impact uitgezet. De maximale waarde van de as komt overeen met een (fictief) scenario dat op alle tien criteria de maximale score (catastrofaal) oplevert (100%). De indeling van de verticale as in categorieën is logaritmisch van aard en zo gekozen dat iedere volgende categorie een drie keer hogere impact aangeeft dan de vorige.

Op de horizontale as is de waarschijnlijkheid van het scenario weergegeven. De indeling van deze as is zo dat iedere volgende categorie een tien keer hogere waarschijnlijkheid aangeeft dan de vorige categorie.

Het kleurverloop in het diagram geeft aan dat scenario's van de linker benedenhoek naar rechts en naar boven steeds ernstiger worden (in impact en in waarschijnlijkheid).

B2.2 Kwadranten

De scenario's kunnen globaal in vier kwadranten van zwaarte of ernst worden ingedeeld:

Hoge waarschijnlijkheid en hoge impact

In deze categorie vallen alle scenario's waarvan de impact 'zeer ernstig tot catastrofaal' en de waarschijnlijkheid 'mogelijk tot zeer waarschijnlijk' wordt geacht. De scenario's die hieronder vallen zijn o.a. ernstige en milde griepvloed; enclavevorming, beïnvloeding openbaar bestuur en mineraal geopolitiek.

Lage waarschijnlijkheid en hoge impact

Deze groep bestaat uit de scenario's met een 'zeer ernstige tot catastrofale impact en een lage waarschijnlijkheid (onwaarschijnlijk tot zeer onwaarschijnlijk). In deze categorie vallen de overstromingsscenario's; moedwillige elektriciteitsverstoring; confrontaties tussen extreemrechts en allochtone groepen en een nucleair incident.

Hoge waarschijnlijkheid en (relatief) lage impact

Een derde groep wordt gevormd door scenario's die minder hoog scoren op impact (aanzienlijk tot ernstig) dan de scenario's in categorie I. De waarschijnlijkheid van deze scenario's is echter vergelijkbaar met die van de eerste groep. De scenario's in deze categorie zijn sneeuwstormen, dierenrechtenextremisme, politiek salafisme, natuurbranden en ijzel.

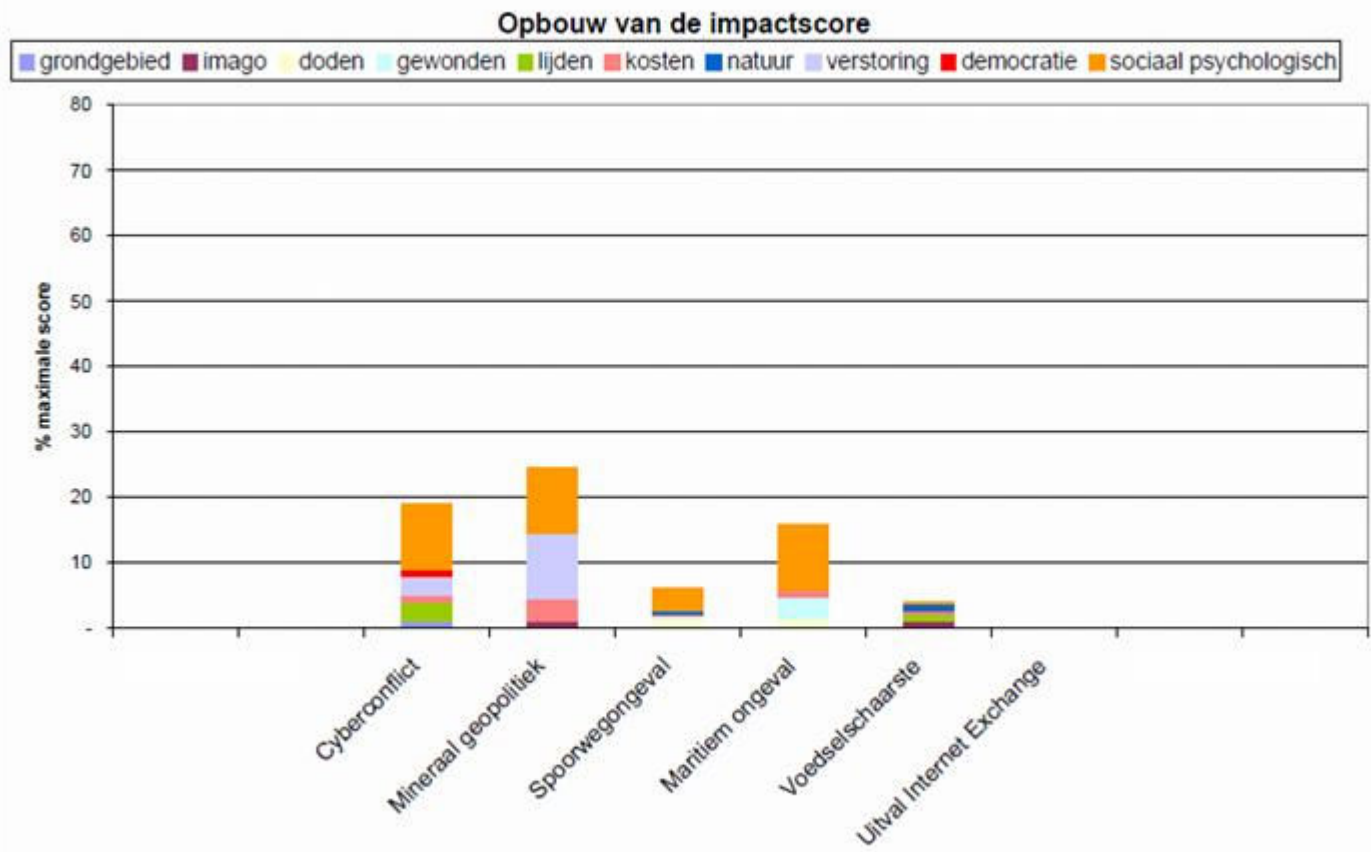
Lage waarschijnlijkheid en/of beperkte impact

De scenario's met relatief beperkte impact, ongeacht de waarschijnlijkheid en de scenario's die als 'onwaarschijnlijk' zijn betiteld, met beperkte tot ernstige impact vallen buiten de drie categorieën. Dit zijn o.a. de scenario's scheepvaartongeval, spoorwegongeval en uitval van één Internet Exchange.

Bijlage 3 Opbouw impactscores scenario's

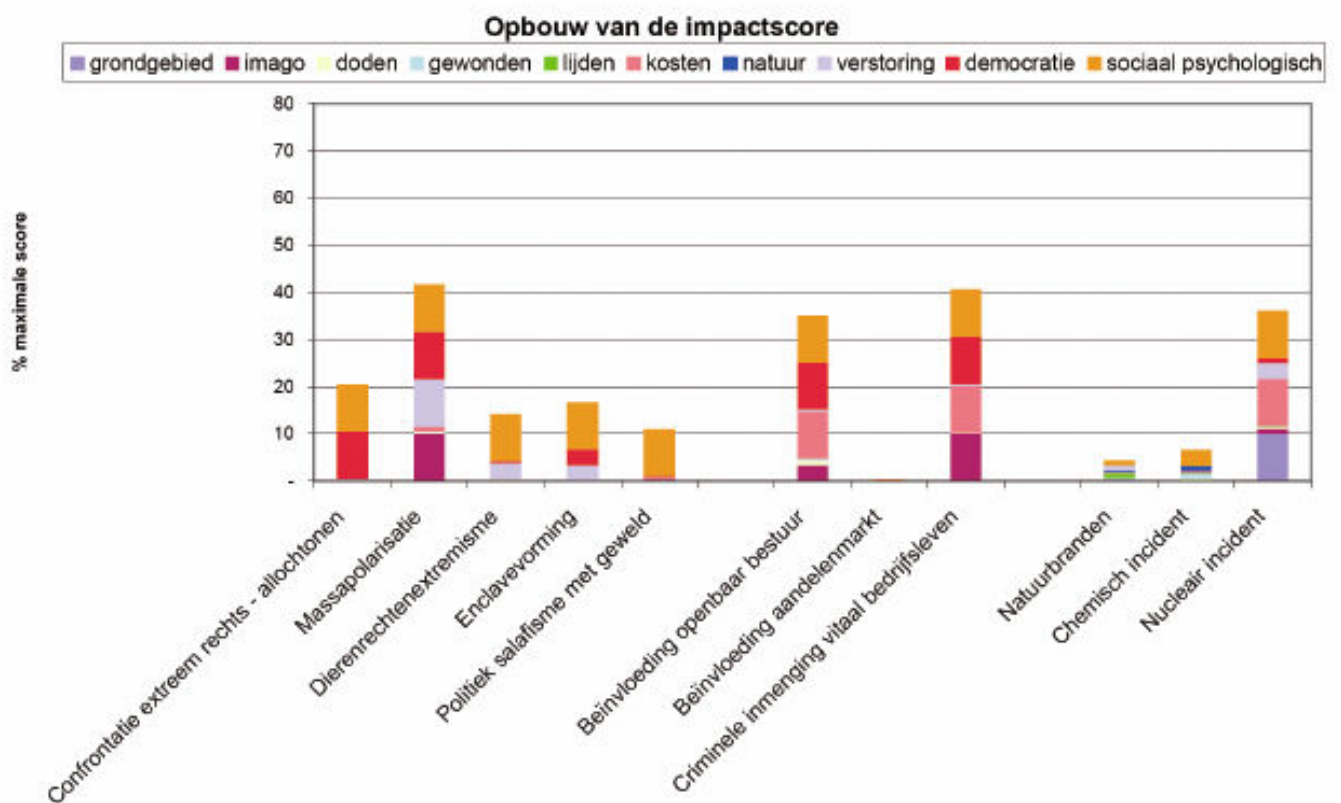
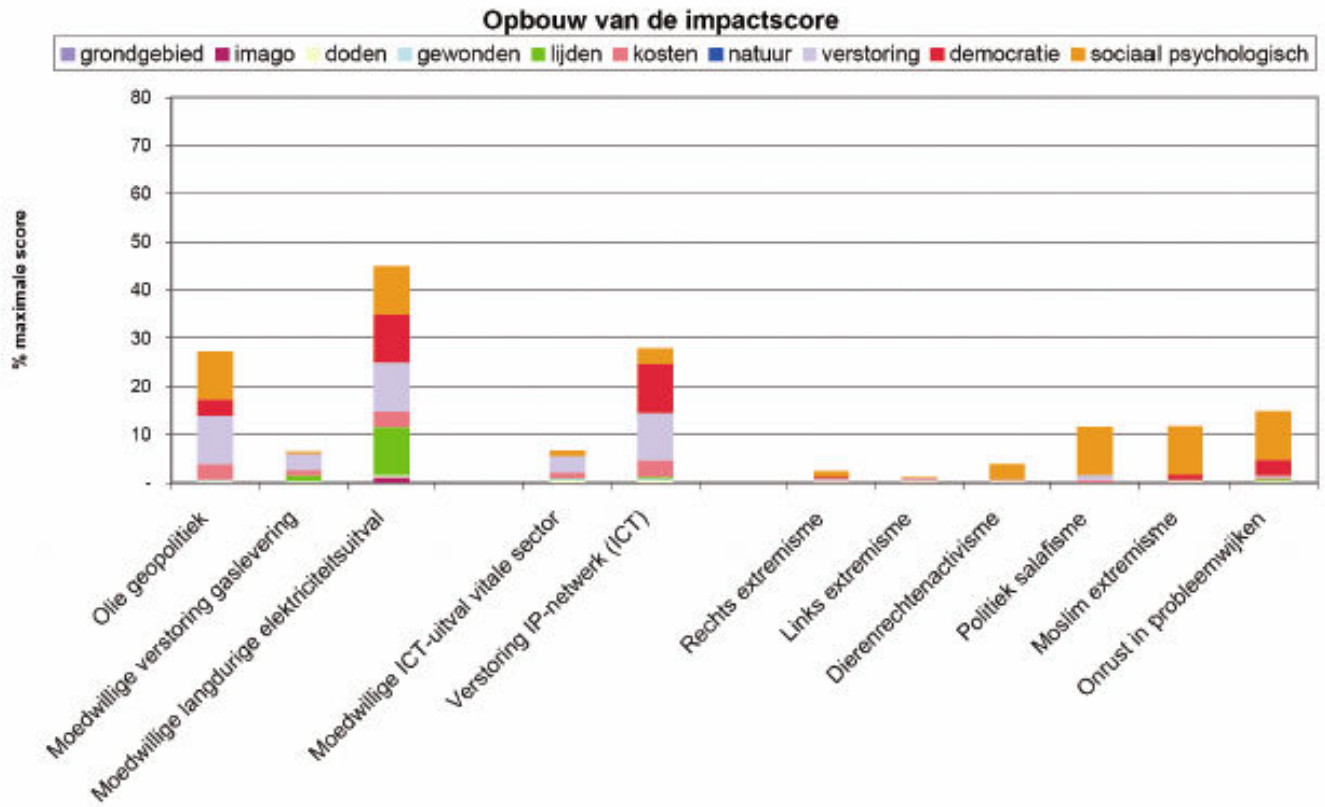
B3.1 Nieuwe scenario's

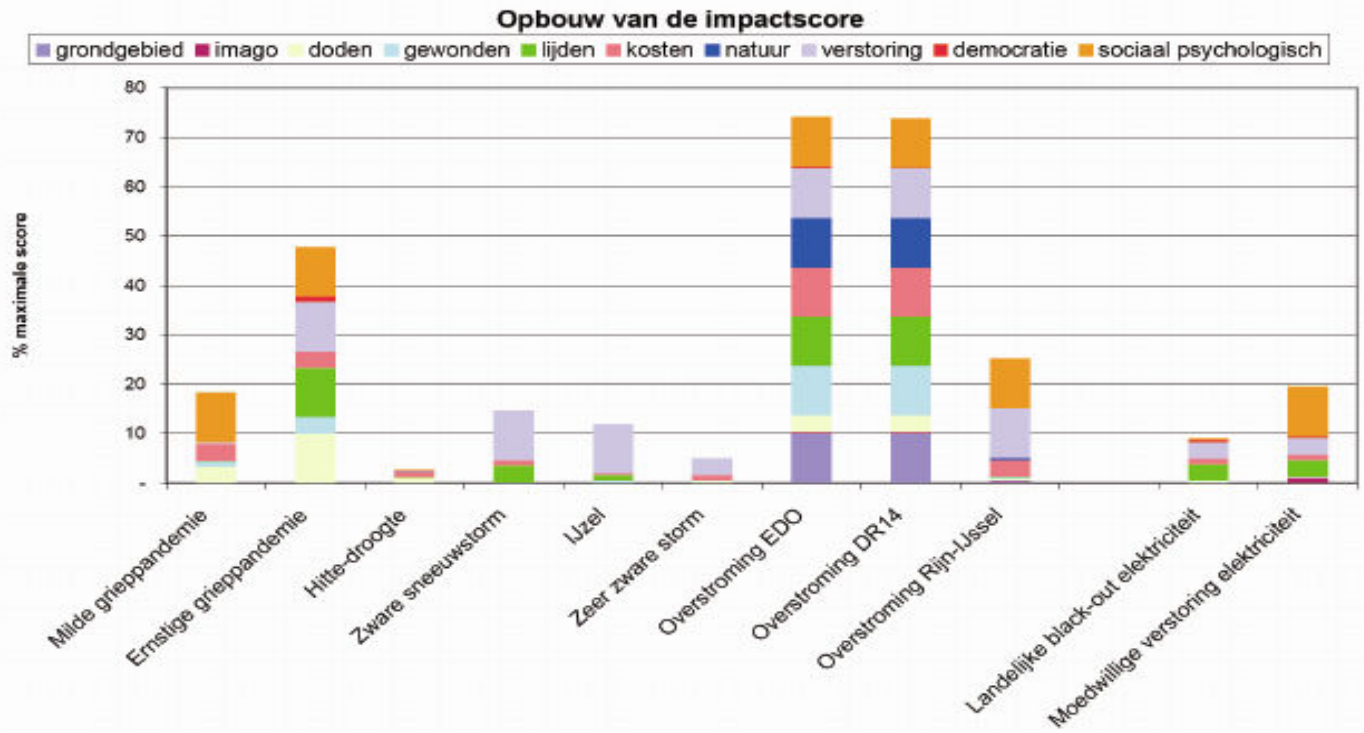
In figuur 4 is aangegeven hoe de impact van de scenario's in deze NRB cyclus is opgebouwd. In bijlage 1 zijn de impactscores van de 33 eerder uitgewerkte scenario's opgenomen. Dit inzicht biedt aanknopingspunten voor de versterking van capaciteiten.



Figuur 4: de opbouw van de impact per scenario van de NRB 2010

B3.2 Impactscores scenario's vorige NRB cycli





Bijlage 4 overzicht waarschijnlijkheid en impactscores van de scenario's

Scenario	Waarschijnlijkheid ²⁷	Impactscores [²⁶]									
		Integriteit grondgebied	Integriteit internationale positie	Doden	Gewonden en chronische ziekten	Gebrek primaire levensbehoeften	Kosten	Milieu en natuur	Verstoring dagelijks leven	Democratische rechtstaat	Sociaalpsychologisch
Griep пандemie mild	D	-	-	D	C	A	D	-	B	-	E
Griep пандemie ernstig	D	-	-	E	D	E	D	-	E	C	E
Hitte-droogte	D	-	-	C	-	A	C	A	A	-	A
Zware sneeuwstorm	E	-	-	A	A	D	C	-	E	-	-
IJzel	D	-	-	A	B	C	B	-	E	-	-
Zeer zware storm	D	-	-	B	A	-	C	-	D	-	-
Overstroming Westelijke kust (EDO)	A	E	B	D	E	E	E	E	E	B	E
Overstroming Dijkkring 14	A	E	B	D	E	E	E	E	E	A	E
Overstroming Rijn-IJssel	A	B	A	B	B	A	D	B	E	A	E
Landelijke black-out elektriciteit	D	-	-	B	A	D	C	-	D	B	B
Moedwillige verstoring elektriciteit	B	-	C	A	A	D	C	-	D	B	E
Oliegeopolitiek	C	-	A	A	B	-	D	-	E	D	E
Moedwillige verstoring gaslevering	A	-	A	A	A	C	C	-	D	A	B
Moedwillige langdurige elektriciteitsuitval	C	-	C	B	A	E	D	-	E	E	E
Moedwillige verstoring ICT vitale sector	C	A	-	B	B	A	C	-	D	A	C
Verstoring IP-netwerk	C	A	-	B	B	B	D	-	E	E	D

²⁶ A: beperkt gevolg; B: aanzienlijk gevolg; C: ernstig gevolg; D: zeer ernstig gevolg; E: catastrofaal gevolg.

²⁷ A: zeer onwaarschijnlijk; B: onwaarschijnlijk; C: mogelijk; D: waarschijnlijk; E: zeer waarschijnlijk.

Rechts-extremisme	D	-	A	A	A	-	A	-	B	B	C
Links-extremisme	C	-	A	A	A	-	B	-	A	A	A
Dierenrechtenactivisme	C	-	A	A	A	-	A	-	A	-	D
Politiek salafisme	E	-	A	-	-	-	B	-	C	-	E
Moslimextremisme	B	-	A	A	A	-	A	-	A	C	E
Onrust in probleemwijken	C	A	-	A	A	B	B	-	B	D	E
Confrontaties allochtonen – extreem rechts	B	-	-	A	A	-	A	-	A	E	E
Massapolarisatie	C	-	E	B	A	-	C	-	E	E	E
Dierenrechtenextremisme	C	-	A	A	A	-	A	-	D	B	E
Enclavevorming	D	-	-	-	-	-	-	-	D	D	E
Politiek salafisme met geweld	C	-	B	A	-	-	B	-	-	A	E
Beïnvloeding openbaar bestuur	D	-	D	C	B	-	E	-	B	E	E
Beïnvloeding aandelenmarkt	E	-	A	-	-	-	A	-	-	-	A
Criminele inmenging in vitaal bedrijfsleven	C	-	E	A	A	-	E	-	B	E	E
Natuurbranden	D	B	-	A	A	C	A	B	C	-	C
Chemisch incident	A	A	-	B	C	A	B	C	-	-	D
Nucleair incident	A	E	C	B	A	A	E	-	D	C	E
Cyberconflict	D	C	A	A	A	D	C	-	D	C	E
Mineraal geopolitiek	D	-	C	-	-	-	D	A	E	-	E
Spoorwegongeval	A	B	-	C	B	-	B	B	A	-	D
Maritiemongeval	A	A	A	C	D	-	C	-	A	-	E
Voedselschaarste (sojabonen)	C	-	C	-	-	C	B	C	-	-	B
Uitval Internet Exchange	A	-	-	-	-	-	A	-	-	-	-

ⁱ <http://www.thing.net/~rdom/ecd/ecd.html>

ⁱⁱ http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

ⁱⁱⁱ <http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf>

^{iv} <http://www.secureworks.com/research/blog/index.php/2009/01/28/kyrgyzstan-under-ddos-attack-from-russia/>